



A GOVERNMENT TECHNOLOGY THOUGHT LEADERSHIP PAPER



State and Local Network Modernization:

Building a Resilient and Future-Ready System

SPONSORED BY

LUMEN®

State and local governments are modernizing critical services as budgets grow tighter, risk tolerance shrinks and internal capacity remains limited.

In a 2025 survey of 300 state and local government respondents, 47% of IT decision-makers said their agencies are focused on modernizing legacy systems, while more than half said their organizations are prioritizing improved cybersecurity (54%) and reduced costs (56%).¹ Typically, agencies have taken an incremental approach to modernization, onboarding new solutions from different vendors over time. However, this approach leads to more fragmentation, less visibility, increased complexity, cost unpredictability and operational risks.

Successful modernization now demands a shift from infrastructure as a collection of assets to the network as a managed operating model. Only then can agencies become more efficient, resilient and financially secure.

Why Modernization Is Difficult

➔ **Budget uncertainty and the need to justify spend in planning and forecasting cycles.** About 7 in 10 surveyed state and local IT decision makers said the cost to modernize and transition from legacy systems is still too high, which slows down innovation.²

➔ **Rising security and resilience expectations alongside expanding threats.** CISOs now contend with more sophisticated cyberattacks and AI as a threat vector. According to a recent National Association of State Chief Information Officers (NASCIO) study, state CISOs listed legacy infrastructure, advanced cyber threats and limited funding as their top cybersecurity challenges.³

➔ **Legacy infrastructure that limits flexibility and slows modernization.** State and local governments will spend a projected \$160 billion on IT in 2026.⁴ However, they continue to grapple with technical debt. Maintaining legacy systems is both cost- and resource-intensive, consuming valuable dollars and staff time that could be devoted to modernization initiatives.

➔ **Lean teams expected to support more services with fewer resources.** Workforce shortages continue to hinder modernization. This challenge may only get worse as longstanding employees with

deep institutional knowledge retire. Many agencies also face skills gaps, as the private sector continues to scoop up security, cloud, networking and AI talent that could help governments modernize faster.

➔ **Procurement complexity, long contract cycles and multi-vendor environments.** Government procurement cycles do not move at the speed of innovation. It can take several months, and sometimes longer, to onboard new solutions. By this time, operational challenges may have changed significantly.

Project-by-project network upgrades and traditional network procurement only compound these pressures, producing fragmented networks that are difficult to manage, expensive to evolve and risky to change.

“If you look at a classic tech networking procurement cycle, the technology team and the procurement team had to budget for the worst-case scenario, so the network was static,” says Nate Smith, a digital sales specialist at Lumen, a leading provider of network-as-a-service (NaaS) solutions for governments. “It couldn’t change.”

AI, software, applications and data are advancing faster each year, making it critical for agencies to be more nimble and reimagine how they approach network infrastructure management.



Shifting to a Network Operating Model

Governments have typically managed their network like a utility. “It’s been set-it-and-forget-it,” Smith says. “But if you look at a network as an operational model, it can help you and your technology stack serve residents better.”

A network operating model approach centers on four key pillars:

Pillar 1: Predictable Budgeting and Forecasting

Traditional network procurement often leads to cost variability driven by overages, penalties, capacity mismatches and reactive upgrades.

In contrast, an operating-model approach can:

- ➔ **Align spend to actual usage and demand**
- ➔ **Reduce surprise costs tied to growth or change**
- ➔ **Improve planning confidence for finance and procurement teams**

“Agencies probably had to over-buy services when they started their contract, and they might have been running short on services at the end of the contract,” Smith says. “In a modern network operating model, they’re now able to manage their bandwidth and manage their capacity as needed.”

This model can serve agencies well in several ways.

When a city is hosting a major public event or dealing with a natural disaster, it can scale network resources to meet increased demand, even segmenting network traffic to increase reliability. It can also better prepare for upcoming usage surges during property tax season, elections and benefit enrollment periods.

What Is a Network Operating Model?

A network operating model treats the network as a strategic service rather than a static asset. It combines connectivity, security, visibility and governance into a unified framework that can adapt as agency needs change.

The result is a network designed to be easier to manage, more resilient to disruption, and better equipped to support modernization initiatives, cloud adoption and technologies such as AI.



Pillar 2: Governed Flexibility

Agencies must change — adding locations, enabling new services and responding to policy shifts — without compromising existing operations.

Governed flexibility can mean:

- ➔ **Policy-driven controls rather than ad hoc changes**
- ➔ **Clear accountability for how and when changes occur**
- ➔ **The ability to adapt without introducing chaos or downtime**

Governed flexibility — which requires team collaboration rather than a single decision-maker — can give governments an operational advantage when they roll out new digital services and must provision network resources to strengthen the performance, reliability and security of applications.

Flexibility also helps agencies respond to policy changes or new federal mandates that require them to quickly deploy new services or modify existing infrastructure. The recent Medicaid redetermination changes, which now require program participants to recertify every six months, are just one example of this.

Governed flexibility can ensure agency networks are primed to handle increased application volumes, resident questions coming into call centers and self-service portals designed to provide 24/7 access.

Pillar 3: Simplified Operations

Operational complexity is one of the fastest-growing hidden costs in state and local IT environments.

Technical debt, along with technology and vendor sprawl, drives this complexity. In the NASCIO study, CISOs expressed concern about the growing number of third parties that interact with their networks, which “may introduce risks to transparency, access and credentials, and other vulnerabilities.”⁵

A simplified operating model combats these challenges by enabling:

- ➔ **Fewer platform hand-offs and vendors**
- ➔ **Less need for manual intervention**
- ➔ **Centralized visibility and day-to-day management**

“If you have a single pane of glass, where your team can now have visibility into your networking platform and application servers so they can see what the performance and health is, it allows them to manage that much more efficiently,” Smith says.

With centralized visibility, agencies can understand utilization in real time, assess network performance, and increase bandwidth to support new applications and services. AI can also help agencies optimize their networks, facilitating automation that improves network health and performance.

Research shows large organizations lose millions annually to digital inefficiencies, while employees lose 36 workdays a year to IT bottlenecks driven by fragmented tools.⁶ This may be why vendor consolidation became a top priority for CIOs last year, with 68% saying they planned to streamline their vendor landscape and, by extension, their IT infrastructure.⁷



Pillar 4: Resilience and Risk Management

Cyber resilience and networking are now two sides of the same coin.

Resilience is essential in modern government. Resident services, public safety systems and internal operations all depend on continuous availability.

A network operating model embeds resilience into governments' IT foundation by:

- **Designing for continuity, not just uptime**
- **Supporting security and compliance requirements without stacking point solutions**
- **Enabling quicker response and recovery when incidents occur**

A network operating model becomes an integral part of cyber resilience by protecting governments against internet-based attacks, intercepting threats at the network edge and delivering real-time intelligence for a more proactive security posture.

"When the network can participate actively in that type of security posture enhancement, the other portions of the security stack don't have to work as hard," Smith says.

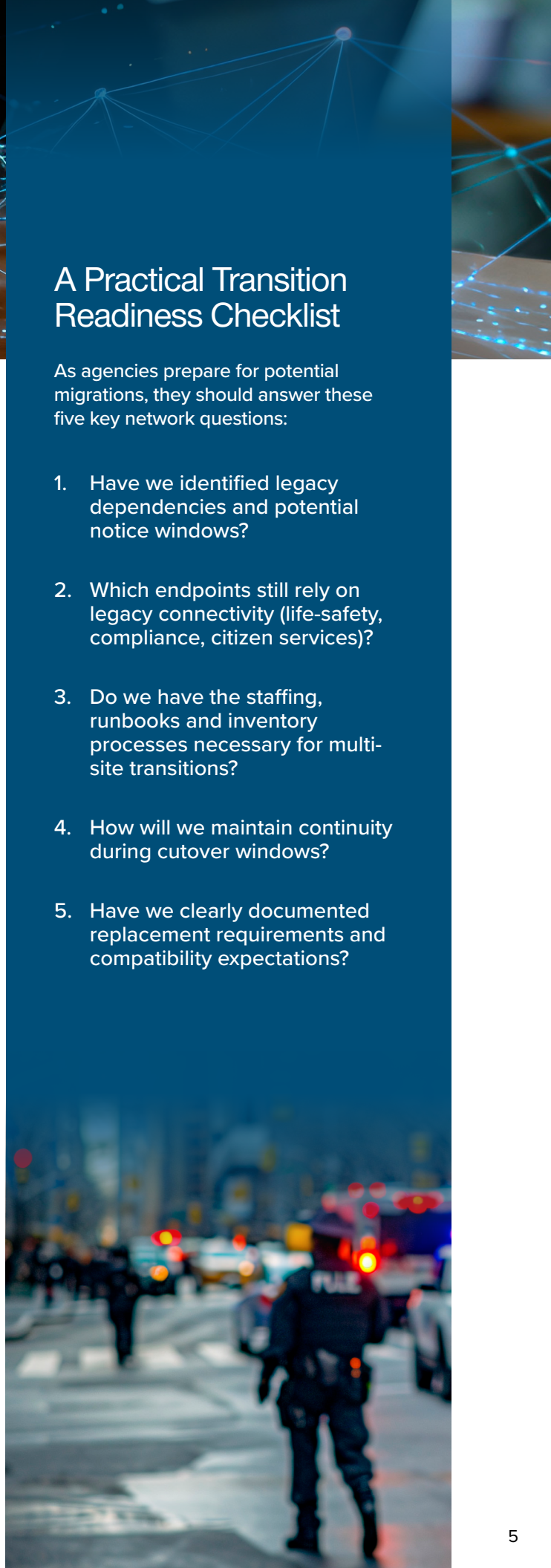
"If you look at a network as an operational model, it can help you and your technology stack serve residents better."

— **Nate Smith**, Digital Sales Specialist, Lumen

A Practical Transition Readiness Checklist

As agencies prepare for potential migrations, they should answer these five key network questions:

1. Have we identified legacy dependencies and potential notice windows?
2. Which endpoints still rely on legacy connectivity (life-safety, compliance, citizen services)?
3. Do we have the staffing, runbooks and inventory processes necessary for multi-site transitions?
4. How will we maintain continuity during cutover windows?
5. Have we clearly documented replacement requirements and compatibility expectations?





Transition Readiness: When Modernization Meets Deadlines

While many modernization efforts are strategic and long-term, others are triggered by external forcing functions, such as sunsetting legacy infrastructure, regulatory shifts or expiring vendor contracts.

Transition readiness focuses on maintaining control and continuity when timelines compress. Agencies should ask:

- **Do we understand our exposure to legacy dependencies?**
- **Which services and endpoints require special protection during transitions?**
- **Can we execute phased migrations rather than rushed cutovers?**
- **Who owns end-to-end accountability during the transition?**

“The devil is in the details, and planning is key,” Smith says. He cites the example of an agency modernizing old network infrastructure and assessing beforehand the network’s health, the services it supports, various interdependencies, and what network assets the agency must maintain.

“Most likely, you can’t afford any downtime, so you’re going to have to do a parallel operations and testing model to ensure the new solution provides the same level of service and reliability before you transition off the old network service,” he says.

How a network operating model drives transition readiness

In this example, and other migrations, a network operating model facilitates transition readiness in several ways:

- **Visibility:** Provides unified visibility of network assets and dependencies, giving agencies the necessary insight to help reduce migration risks.
- **Agility:** Enables flexibility to support parallel operations and phased migration.
- **Embedded security:** Integrates advanced security and compliance into the network foundation, closing critical security gaps to help agencies modernize safely.
- **Resilience:** Establishes a resilient foundation that maintains service continuity.
- **Ownership:** Supports clear accountability across services.

Most agencies can’t afford any downtime, so transition and testing need to happen in parallel.

The Power of a Network Operating Model: State and Local Government Examples

Driving Network Transformation for a Regional Transit Agency

The challenge: A large transit agency that operates a network of buses, light rails and commuter trains needed to securely connect its large regional operations and maintenance facilities to transit stations and other locations within its system. It also needed to expand internet service across various sites and support multiple diverse connections to Microsoft Azure.

The solution: The agency partnered with a leading provider of secure, AI-ready networking solutions to support these changes. Working with its provider, the agency implemented a network operating model, using the company's NaaS solution to stand up a point-to-point network, turn up connections to Azure, and set up additional future connections for on-demand internet service to meet transit riders' bandwidth needs.

The results: By implementing a network operating model, the agency has created a unified, resilient foundation that will drive its current and future network transformation.

Making Collaboration Easier for Local Law Enforcement Agencies

The challenge: A county sheriff's office needed a solution that securely connected several local law enforcement agencies to its law enforcement database, which would simplify collaboration and data sharing. The agency also needed to scale bandwidth during emergency and crisis situations. However, copper connections and legacy services stood in its way.

The solution: The county sheriff's office partnered with a leading provider of secure, AI-ready networking solutions to implement a NaaS and internet on-demand solution to address these challenges. Neighboring law enforcement agencies can now seamlessly and securely access the database. The sheriff's office also has the scale and flexibility to strengthen emergency response.

The results: The sheriff's office is now better positioned to future-proof its network, deploy internet on-demand services at other sites, and add connections to the cloud. Transitioning to a network operating model will allow the office to right-size network resources, reduce costs, and improve operational efficiency and flexibility — crucial capabilities that are non-negotiable for today's law enforcement agencies.

Conclusion

Modernizing the network is no longer just a technology decision. It also has critical implications for operations, finances and governance.

State and local agencies that adopt a network operating model — focused on predictability, simplicity, resilience and transition readiness — can modernize without disruption, respond to change with confidence and protect the services their communities rely on.

"Constituents are now used to everything on demand. They now expect the same level of responsiveness and immediacy for the government services they interact with," Smith says. "With a network operating model, your team can scale and right-size the network to meet your needs today. And as it grows, it can shift with changes in demand to meet new expectations for your organization."

1. https://www.ey.com/en_us/insights/government-public-sector/ey-government-state-and-local-2025-survey-findings
2. https://www.ey.com/en_us/insights/government-public-sector/ey-government-state-and-local-2025-survey-findings
3. <https://www.deloitte.com/us/en/insights/industry/government-public-sector-services/2026-nascio-deloitte-cybersecurity-study.html>
4. <https://www.govtech.com/budget-finance/what-will-state-and-local-government-spend-on-it-in-2026>
5. <https://www.nascio.org/wp-content/uploads/2026/04/2026-NASCIO-Deloitte-Cybersecurity-Study.pdf>
6. <https://www.cio.com/article/3841636/it-frustration-costs-companies-more-than-100-million-a-year-with-shadow-it-the-only-user-solution.html>
7. <https://news.sap.com/2025/08/cio-trends-2025-the-consolidation-imperative-takes-center-stage/>

*This piece was written and produced by the Government Technology Content Studio,
with information and input from Lumen.*



Produced by Government Technology

Government Technology is about solving problems in state and local government through the smart use of technology. Government Technology is a division of e.Republic, the nation's only media and research company focused exclusively on state and local government and education.

www.govtech.com



Sponsored by Lumen

Explore how the trusted Lumen network helps government agencies modernize infrastructure, strengthen cybersecurity, and build a resilient foundation for innovation and growth.

Learn more at **Lumen.com**