E-BOOK

DESIGNING MODERN GOVERNMENT NETWORKS

Guidance for evaluating and implementing new network and connectivity capabilities

Spectrum ENTERPRISE

It's a new era in government. Citizens want easy access to online services and high-quality digital experiences.

At the same time, new developments in smart city infrastructure are transforming city, state and county management. Networked sensors and controllers can reduce costs and improve efficiencies by enabling officials to remotely monitor and manage the delivery of utilities and other services from a central location.

Meeting stakeholders' rising expectations calls for modern networks that can handle additional bandwidth and security requirements. These new realities place huge demands on government IT leaders, who must design networks that can replace legacy systems with modern capabilities, without disrupting essential services.

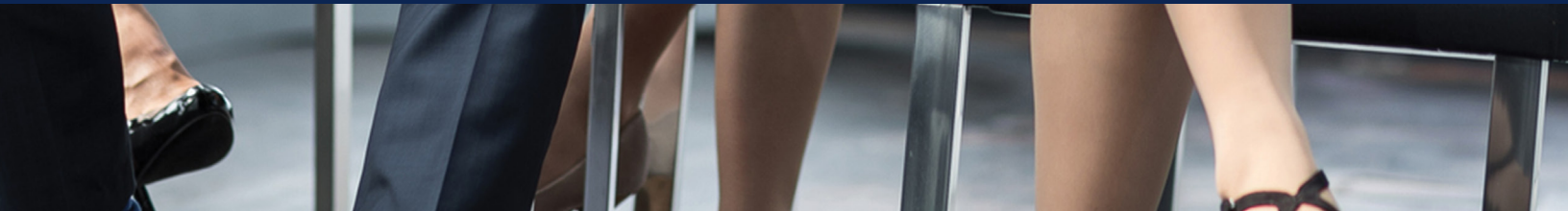
This e-book will help you understand:

- The critical importance of having a modern network infrastructure.
- How to identify your WAN, WiFi and security needs.
- How to form a plan for upgrading that ensures seamless continuity.
- Strategies for choosing the right partner for success.

Inside this e-book

Section 1

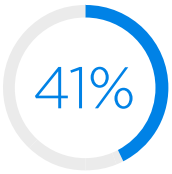
The case for innovation



1 2 3 4 5

Section 1: The case for innovation

Technology is rapidly evolving and government agencies must keep up to take advantage of new capabilities and meet rising citizen expectations. Here are four key factors that are driving the need to take stock of your network infrastructure and make plans for enhancements:



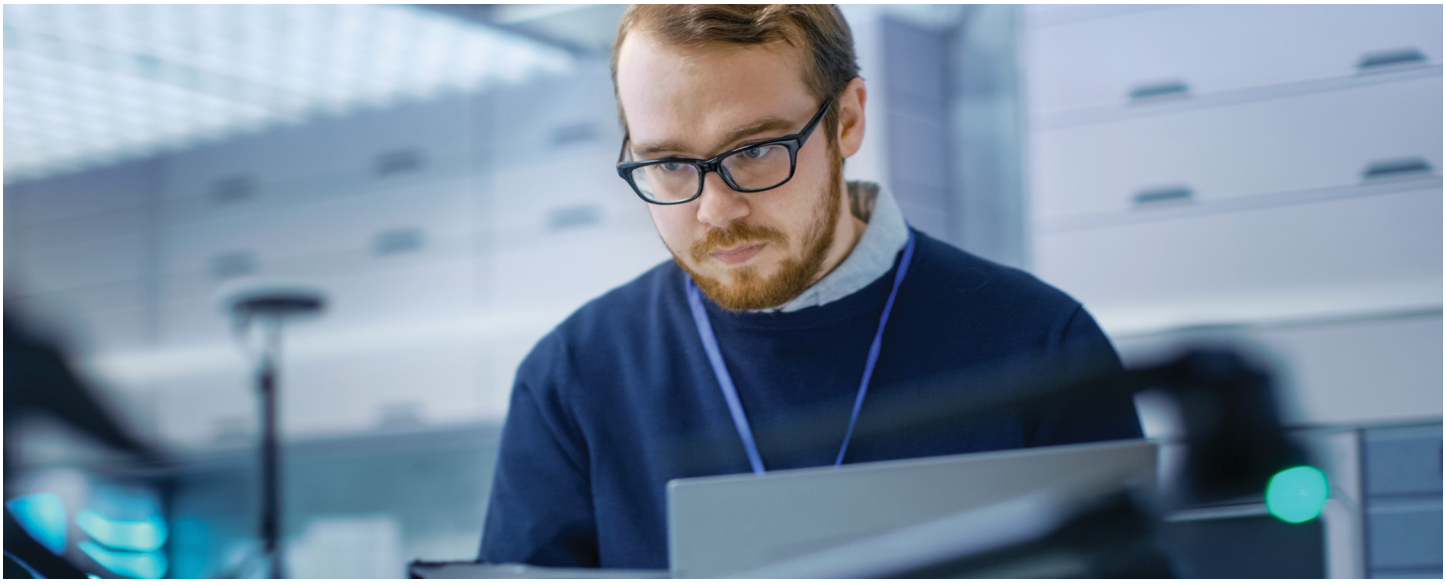
of state and local government CIOs listed migrating their infrastructure to the cloud as a top priority.[1]

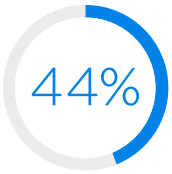
Services are moving to the cloud

When we want to check our bank balance or make a transfer, there's an app for that. When we want to order takeout, shop for a last-minute gift or schedule a ride to the airport, we can do it all from the palm of our hand. Citizens increasingly expect the same level of convenience when they interact with government agencies. Moving services to the cloud helps satisfy this demand.

A growing number of government agencies are also learning that moving to the cloud can lower costs and improve efficiencies. In a recent survey conducted by the Center for Digital Government (CDG), 37 percent of state and local governments say the biggest benefit of cloud services as been lowering total operating costs.[2] Nearly one-third say increasing the speed and agility of application development has been their biggest benefit, and one-quarter say it's improving mission-critical service delivery.

While cloud-based services allow state and local governments to reduce costs and increase efficiencies, moving to the cloud puts additional strain on government networks. Agencies must have a secure and reliable network infrastructure that can handle this additional load.





of wireless users say poor indoor connectivity is noticeable.[5]

The Internet of Things is changing service management

Networked cameras and controllers, smart sensors and other Internet of Things (IoT) devices are transforming the way services are delivered, monitored and managed. But IoT adoption also places more pressure on government networks.

In a CDG Smart Network Infrastructure survey, the majority of respondents (63 percent) are either actively discussing or considering implementing IoT technologies. But 59 percent say their network can't handle the expected demands of IoT over the next 12 to 18 months.[3]

A proliferation of connected devices will vastly increase data traffic and create many more data entry points on government networks. To prepare for these eventualities, government networks must have secure fiber connections, easily scalable bandwidth and strong endpoint security.

Employees expect reliable WiFi to do their jobs effectively

In 2020, many state and local government employees switched to remote work as a result of COVID-19 restrictions. Now that they're back, and there are more demands on the network, employees may not have the wireless coverage or WiFi needed to do their jobs effectively. Consider:[4]

- 44 percent of employees notice poor wireless coverage indoors.
- 84 percent of employees are more productive when they have reliable internet connections.

Fast and reliable WiFi is essential for enhancing staff productivity and reducing the workload on government IT departments.

278%

increase in leaked government records — just in Q1 2020.[5]

Keeping citizen data secure is non-negotiable

Perhaps most importantly, network upgrades are critical if government agencies are to keep their citizen information secure. Government agencies are expanding access to remote work and work-from-home arrangements, with 61 percent of local municipalities allowing their employees to work from home.[6] This opens up networks to cybersecurity breaches, including ransomware, data theft and malware.

The security of citizen information isn't the only thing at stake. Network breaches can cripple essential government services and cost millions of dollars to fix. In 2018, Atlanta was victimized by a ransomware attack that took many of the city's services offline for nearly a week, and Baltimore's 911 dispatch system was paralyzed for more than 17 hours by a cyberattack. The most serious issue faced by state and local governments are phishing attacks, which can disclose sensitive information, followed by data-related attacks and cloud networking attacks. The majority of respondents (84 percent) to a January CyberRisk Alliance Survey reported that they experienced cloud networking attacks. One in four respondents encountered malicious internal attacks.[7] A strong network security strategy and solution are critical in preventing these kinds of attacks.

Meeting the connectivity needs of citizens and government employees requires a solid network infrastructure — one that is secure, reliable, flexible and adaptable. Is your network ready?

Section 2

Identify your needs

Section 2: Identify your needs

Wide-area network

The wide-area network (WAN) of the future is highly agile, scalable and adaptable, capable of expanding to meet your government's needs. It should be customizable with features to optimize performance and the intelligence to identify problems. As you evaluate your WAN's readiness for the future, here are some key questions to help guide you.

Capacity: *Does your network have the capacity to meet users' needs now and into the future?*
Consider how many total users you'll have (including staff and citizens), what applications they'll be using and how many IoT devices will be connected to your network over the next several years. Do you have enough bandwidth to support the demand? What is the latency between network end points? You need a network that can handle the load without becoming congested during peak usage times.

Resiliency: *Is your WAN designed to withstand a cut cable or other outage to a critical network connection? Do you have failover protections in place?*
Loss of a network connection can be extremely disruptive to daily operations. Building a resilient network involves planning for the worst and having alternate routes available for your network traffic in case something goes wrong.

Flexibility: *Can your network easily accommodate changing needs?*
Does your network infrastructure give you the flexibility you need to easily make adjustments, such as adding new locations or modifying bandwidth? An agile network gives you more control, allowing you to respond quickly to changing needs.

Visibility: *Are you able to see data traffic patterns and application usage across your network?*
To make smart policy decisions based on how your network is performing, you need to be able to see what's going on with your network at any given time. Having both real-time and historical insight into your network operation allows you to monitor performance and set or adjust policies as needed.

Efficiency: *Does your network include features designed to maximize the efficiency of data flow?*
Features such as traffic shaping allow you to prioritize certain types of network traffic (like communication and citizen applications) over other types (such as video streaming), resulting in faster and more reliable network performance.

Having real-time and historical insight into your network performance lets you make smart policy decisions.

Action items

- Understand your network capacity needs for at least the next few years, how much traffic your network can currently handle and where you might need to upgrade. Conduct capacity testing to measure network speeds and throughput and to identify current (or potential) bottlenecks. If necessary, add bandwidth or upgrade your network infrastructure to meet future demands.
- Work with your service providers to design highly resilient networks that can maintain connectivity in the event of an outage. Make sure lines with the highest volume of traffic have alternate routes available. Request service level agreements that guarantee sufficient uptime.
- If your network isn't easily customizable, consider a software-defined WAN (SD-WAN) solution or other technologies to create a more flexible, agile network.
- Make sure you have visibility into how your network is performing, including traffic flow and application usage data arranged by user, type and specific application.
- If you don't currently have traffic shaping capabilities, invest in a solution that allows you to prioritize certain types of network traffic in order to maximize the efficiency of data flow.

WiFi

Adequate wireless coverage throughout your buildings is essential for employee productivity. To support your vision for the future, your WiFi infrastructure should connect users in the most efficient way possible, reducing congestion and optimizing network performance. Here are some questions to ask as you evaluate your WiFi needs.

Self-optimization: *Does your WiFi infrastructure contain built-in intelligence that continuously looks for ways to optimize performance, so users receive the best experience possible?*
The latest generation of WiFi technology can improve network performance in congested, high-density environments by dynamically setting and changing the channel selection, channel width, and transmission power of radio frequency (RF) antennas to match the needs of users in that environment. What's more, this happens without the need for manual intervention. Automating this process reduces signal interference and results in a better wireless experience for staff and other stakeholders.

Load balancing: *Does your WiFi infrastructure automatically distribute users evenly across controllers and access points to prevent network congestion?*
The latest WiFi technology can transfer users to controllers and access points with less of a load automatically, which eases congestion in high-density areas. This process happens dynamically in real time as citizens and government workers are roaming with their devices. The result is better signal throughput for each user.

Multi-tenancy: *Does your WiFi infrastructure allow you to create separate, secure wireless networks from shared access points?*
A key challenge in creating wireless environments is how to establish separate networks for employees, visitors and the IoT using the same WiFi access points. The latest WiFi technology lets you do this easily. As a result, government agencies can enjoy better network security and efficiency while also lowering the cost of WiFi deployment and creating less RF signal interference.

increase in cybersecurity attacks on state and local governments since 2017.[10]

Seamless failover: *Does your wireless network have the ability to switch users over to another controller or access point seamlessly (and automatically) in the event of a failure, so service continues uninterrupted?*
The latest WiFi technologies are built in such a way that when a controller or access point fails, another will automatically pick up the user session with no drop in service. If controllers and access points are configured in clusters, then standby paths are created in real time to alternate devices within the same cluster. During high-priority sessions (such as voice or video use), these sessions are synchronized between active and standby devices, so if a network device fails, switching the user to another network device is completely seamless. This means users won't experience any disruption in service — and IT staff aren't burdened with a user complaint or a request for help.

Action items

- Invest in smart infrastructure that can self-optimize WiFi performance in high-density locations.
- Take advantage of intelligent WiFi infrastructure that can balance the load evenly among various controllers and access points to improve network performance.
- Consider WiFi infrastructure with seamless failover capabilities to ensure uninterrupted service if a controller or access point fails.

Network security

Security is a critical aspect of building a modern network infrastructure. Cybersecurity attacks on state and local governments are up 50 percent since 2017, with average ransom demands rising from $30,000 to nearly half a million dollars.[9] As you assess your security needs, here are some key considerations:

A firewall with unified threat management (UTM): *Can you administer and manage multiple security functions from a single console?*
Choosing a firewall solution that combines features such as intrusion detection and prevention, antivirus software, deep packet inspection, application layer control and advanced security reporting within a single solution can simplify network security while saving time and money. There are fewer products to configure and maintain, and network administrators can achieve a single, holistic view of the threats to their network.

DDoS protection: *Do you have a way to protect your network from a distributed denial of service (DDoS) attack?*
In a DDoS attack, a hacker takes control of several computers and uses them to target a single server, overwhelming the server's network with traffic and taking it offline. DDoS attacks are fairly easy to carry out, and they can be very disruptive to day-to-day operations. Government networks have become increasingly popular targets for these kinds of assaults, and the best defense is to deploy a cloud-based security solution that can intercept the onslaught of traffic attacking your network before it even reaches its intended target.

Vulnerability testing: *Are you regularly scanning your network for potential weak spots that can be exploited by hackers?*
As a general rule, you should test your network at least on a quarterly basis to find and correct possible weaknesses in your security defenses. Ideally, this testing should be performed by a certified third party.

Other best practices: *Have you adopted other industry-recognized best practices for keeping your network secure, such as network segmentation?*
Segmenting your network involves separating groups of systems or applications from each other either physically or virtually. This limits communication between various systems, which limits how much damage a hacker can do on your network.

Action items

- Choose a firewall solution with UTM capabilities that makes network security simpler and more effective.
- Invest in a DDoS protection solution that shields your network from these increasingly common and highly disruptive types of attacks.
- Partner with a respected third party to conduct regular vulnerability testing on your network to identify and correct potential weak spots.
- Think about how you might segment your WAN to limit the damage in the event of an attack.

Section 3

Form a plan

Section 3: Form a plan

Upgrading your network should be done with as little impact on citizens and staff as possible. You need to replace outdated systems without disrupting your current network service. Creating a well thought-out migration plan can help you ensure success. Here are three steps to consider in this process:

Determine a rollout strategy

Will you upgrade all at once, or roll out new network infrastructure in phases? What is your timeline for upgrading? How you answer these questions depends on many factors, such as your budget and how ready you are to make significant changes.

Your rollout strategy should consider your capacity for change, including the resources you have available for change management, training and support. It should also balance the speed of deployment with the risk of making mistakes; your goal should be to upgrade in a reasonable amount of time without taking any major risks.

Read our guide to learn more strategies for tackling a modernization project.

Develop a business continuity plan

To ensure that service continues uninterrupted as you upgrade your network, you should identify your agency's key service areas and critical functions, determine how all of these are interrelated, then create a plan to maintain operations.

For instance, you might temporarily shift the performance of certain tasks to other departments while an upgrade is in progress. Or, you might build redundancy into your network so that you have alternate paths for transmitting data while part of your network is being replaced. However you approach establishing continuity of service, mapping out key business functions and how they are interconnected will help you make sure nothing is overlooked as you transition to a new network infrastructure.

Communicate with users

Frequent communication with employees and other network users is critical to the success of any network upgrade. Users should know in advance how the project might affect them and their ability to do their jobs, so there are no surprises. If you'll be making any changes to how employees will interact with your network, make sure you communicate these changes clearly. For instance, if a WiFi upgrade includes a new method for authenticating users, this needs to be communicated along with detailed instructions for how to use the new system.

Section 4

Owned vs. managed

Section 4: Owned vs. managed

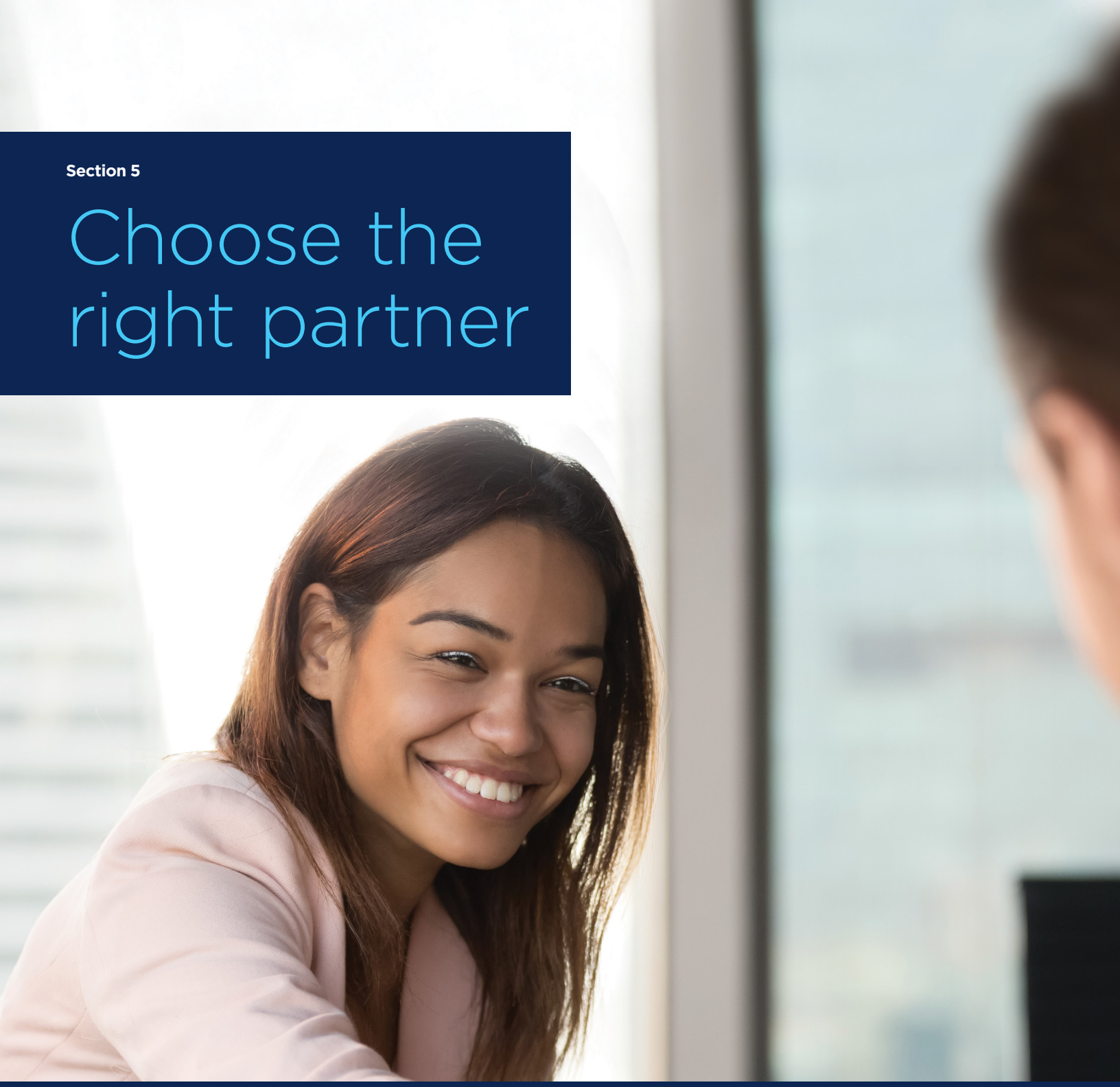
As you design your network strategy, one aspect to consider is whether you want to own and support all of it yourself. Municipalities no longer have to purchase and manage all their IT infrastructure. Instead, governments can choose solutions that are installed, owned and managed by a service provider. Here are some factors to think about when making this decision.

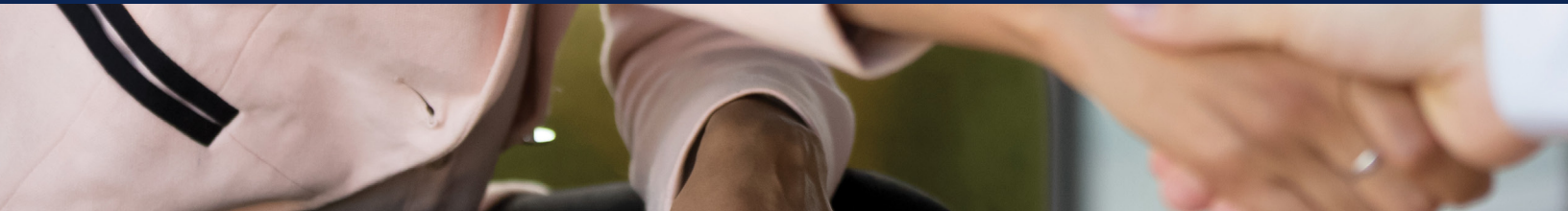
Consider the hidden costs that come with managing your own equipment.

- **Flexibility.** When you buy your own equipment, you're investing in a specific network infrastructure with a fixed capacity. If your needs change faster than you anticipated, or if you underestimated the demands on your network from the outset, you'll have to invest more money and time to upgrade. If flexibility is a priority, a managed solution lets you add more capacity as desired. It also gives you the assurance that as technology evolves, you'll always have access to the latest innovations.
- **Reliability.** When you own your network equipment, you're responsible for all maintenance and repairs. How might this affect the reliability of your network? With a managed solution, you have the peace of mind that comes from having a service level agreement (SLA) in place guaranteeing network uptime and issue resolution response times.
- **Budgeting.** Would you rather incur a large up-front expense or have monthly recurring charges? Some agencies would prefer the single capital outlay that comes from buying and installing their own equipment; for others, a fixed monthly rate for a managed service makes it easier to budget. Of course, if you invest in your own network infrastructure, you'll still have to set aside funding for maintenance and support — and these expenses can add up quickly.
- **Staff capacity.** Does your technology staff have the capacity to maintain and troubleshoot your network, while also leading innovation? Can you effectively support the network *and* meet other IT needs? If so, then owning your network infrastructure might make sense. But a growing number of IT leaders are finding that a managed solution that can deploy technicians 24/7/365 to address problems frees up staff from having to perform routine maintenance tasks, so they can spend more time on strategic initiatives that enhance their municipality's mission.

Section 5

Choose the right partner





1 2 3 4 5

Section 5: Choose the right partner

Your choice of service providers matters. You want a company that is not just a technology vendor, but a true partner who is fully invested in your success. The right partner can help you at every step in your project, ensuring the success of your network upgrade.

Here are four important qualities to look for in a network service provider:

- **Industry leadership.** Does the provider have the size, capacity and expertise to serve your needs effectively? Is the company stable and reliable, with a strong reputation in the industry?
- **Cutting-edge technology.** Does the provider employ the latest standards and technologies? Do the company's products reflect the latest industry developments?
- **Experience in the government market.** Does the provider understand the unique needs of government agencies? Does it have a proven track record of success in serving this market?
- **Top-notch service.** Does the provider value you as a customer? Will you receive prompt answers to your questions? Is someone available at all hours in the event of an emergency?

Spectrum Enterprise serves hundreds of government agencies nationwide.

Spectrum Enterprise — your partner of choice

Spectrum Enterprise meets all of these criteria and provides a complete range of network connectivity solutions for government agencies. Our dedicated public-sector IT experts serve hundreds of government agencies nationwide with a network engineered for exceptional performance, end-to-end accountability and support. Our services include:

Fiber Internet Access: Achieve dedicated internet connectivity with symmetrical upload and download speeds and bandwidth up to 100 Gbps.

Wireless Internet Backup: Experience automatic wireless internet failover and failback service that is managed for you.

Wireless Internet: Provide primary or secondary internet access over LTE Advanced technology with this all-inclusive wireless internet service.

Ethernet Services: Meet ever-growing data needs by connecting locations with a fast, reliable wide area network (WAN) solution backed by performance guarantees and built on a dedicated fiber infrastructure with bandwidth up to 100 Gbps.

Cloud Connect: Extend your network with fast, secure and dependable private cloud connections to cloud service providers.

Managed SD-WAN: Achieve greater visibility and insight with a managed WAN that allows for application-aware routing while reducing network complexity and cost.

Managed WiFi: Meet citizen and staff demands for reliable connections to the internet with ubiquitous coverage across your facilities and 24/7/365 support.

Managed Network Edge: Simplify the deployment and management of your network with this modular, all-in-one solution. Delivered over the Cisco Meraki platform, the solution offers security, routing, SD-WAN, WiFi, switching and cameras. Achieve flexibility and scalability with connectivity, equipment and network management from a single partner.

The nationwide private fiber network from Spectrum Enterprise provides reliable, hassle-free connectivity.

Managed Router Service: Efficiently route traffic and improve bandwidth use without investing in hardware or day-to-day management.

Managed Security Service: Protect your network with a fully managed solution that offers a firewall and unified threat management (UTM), intrusion detection and prevention, anti-malware, antivirus, event log management and more.

DDoS Protection: Guard against malicious volumetric attacks designed to overload your network with world-class distributed denial of service (DDoS) threat identification and mitigation.

Voice and unifed communications: Increase productivity with feature-rich, easy-to-scale PRI and SIP trunking solutions for on-premises phone systems. Alternatively, answer communication and collaboration needs for your teams with a fully managed, cloud-based unified communications solution that includes voice or video calling, availability status, instant messaging and desktop sharing available on any device from anywhere.

TV: Help government employees stay plugged in to events and to the community through a large variety of channel lineups, premium packages, on-demand content and customized content such as government services updates, agency news, how-to information and details about special events.

As technology continues to evolve, you'll need a high-performance network infrastructure capable of supporting the needs of citizens and employees. Let the government IT experts at Spectrum Enterprise help you get there.

Learn more

1. John Aldecoa, "IT Modernization Survey," Center for Digital Government, July 8, 2020.
2. "Gaining Steam: Cloud Platform Adoption and Emerging Technologies," Center for Digital Government, 2019.
3. "Smart Network Infrastructure: The Backbone of Sustainable IoT Initiatives," Center for Digital Government and Spectrum Enterprise, 2020.
4. Ed Wyatt Jr., "Is your agency's wireless network ready for returning workers?" GCN, June 5, 2020.
5. Ibid.
6. "Local, State and Federal Agencies Gear up to Fight Cloud Network Attacks and Data Breaches," January 2021.
7. Ibid.
8. James Coker, "278% Rise in Leaked Government Records During Q1 of 2020," InfoSecurity, April 15, 2020.
9. Stephanie Kanowitz, "Cyberattacks on state, local government up 50%," GCN, Sept. 4, 2020.
10. Ibid.

About Spectrum Enterprise

Spectrum Enterprise, a part of Charter Communications, Inc., is a national provider of scalable, fiber technology solutions serving America's largest businesses and communications service providers. The broad Spectrum Enterprise portfolio includes networking and managed services solutions: Internet access, Ethernet access and networks, Voice and TV solutions. Spectrum Enterprise's industry-leading team of experts works closely with clients to achieve greater business success by providing solutions designed to meet their evolving needs. More information about Spectrum Enterprise can be found at enterprise.spectrum.com.

Spectrum ENTERPRISE