A GOVERNMENT TECHNOLOGY HANDBOOK FOR verizon

The New Realities Driving Government Network Transformation

Contents

3 Introduction

4 What is Network Transformation?

6 **Core Technologies:** Driving Automation & Legacy System Modernization

8 **Workforce:** Delivering a Better Employee Experience

10 **Public Safety:** Protecting Communities & Improving Emergency Response

12 **Connectivity & Access:** Closing the Digital Divide

15 **Cybersecurity:** Securing the New Edge

16 **Budget & Cost Control:** Optimizing Funding & Improving Financial Sustainability

18 Best Practices for Network Transformation

19 Conclusion

Introduction

Every day, millions of people in states, cities and rural areas throughout the country rely on network connectivity to execute critical tasks in their lives.

A business owner relies on it to process customer transactions or to apply for a new local government permit. A first responder needs it to get timely information about what awaits her at the scene of a massive accident. A state health and human services employee depends on it as he wades through information to make an eligibility determination that could make all the difference for a family in need. And for a student whose school is using technology to enhance learning outside the classroom, strong network connectivity could determine whether she can participate in the day's lesson plan or fall behind.

Though we often don't fully realize it, network connectivity serves as a critical lifeline for so many communities. It's not just about downloading the latest viral video or being able to send a text that arrives in milliseconds. As the COVID-19 pandemic made all too evident, network connectivity enables so many aspects of government service delivery that when networks falter or don't function optimally, the consequences could be significantly disruptive and potentially catastrophic.

The lessons from the last two years have taught state and local governments they are long past due for modernization.

As governments work to become more technology-enabled, they'll not only need to enact digital transformation but also network transformation.

Network transformation can drive better government in six key areas:

1. **Core technologies:** Automating and modernizing legacy systems
2. **Workforce:** Delivering a better employee experience
3. **Cybersecurity:** Securing the new edge
4. **Public safety:** Protecting communities and improving emergency response
5. **Connectivity and access:** Closing the digital divide
6. **Budget and cost control:** Optimizing various funding streams and improving financial sustainability

With network transformation, state and local governments can deliver a better constituent experience, make meaningful progress toward achieving their mission and finally realize the vision of digital government. This handbook provides a roadmap for how they can start and successfully navigate this journey. ■

What is Network Transformation?

Network transformation means modernizing an organization's or municipality's network architecture to accelerate the delivery of information and improve application and system performance.

In terms of government service delivery, "network transformation is about strategically re-evaluating your network architecture and then implementing new technologies and new processes to enable more effective and efficient constituent services," says David Grady, chief security evangelist at Verizon. "This means putting your organization and its infrastructure under a microscope and making decisions about what you want it to be able to do in the future."

This kind of transformation forces governments to focus on the outcomes they want to achieve. But at a more granular level, it drives them to carefully think about their approach to network design. In a digital world, network design must be more hyperdynamic and interconnected, with the ability to assign roles based on defined business criteria rather than just an IP address.

"From my perspective, network transformation encompasses moving away from a diverse array of point products and services and applications with little common oversight to an ecosystem of more synergistic applications and capabilities," says Tony Dolezal, public sector marketing manager for national public safety at Verizon Business Group.

To achieve network transformation, governments first need a deeper understanding of the constituent experience and how residents interact with various agencies and departments across the ecosystem. Constituents now judge their interactions with government agencies based on the customer experience they receive in the private sector. They expect real-time, responsive, personalized service, but governments historically haven't been well equipped or well resourced enough to meet these expectations.

In some respects, the pandemic illuminated these issues but also accelerated progress toward resolving them. In the first months of COVID, there were stories about long lines, waits and hold times to collect unemployment benefits, apply for a permit or schedule a court hearing. Months later, many municipalities implemented virtual services, with the help of a variety of cloud-based software-as-a-service applications, to streamline service delivery and bolster their resilience.

Public sector organizations scrambled to implement videoconferencing, digital workspaces and distance learning platforms, but they often failed to

consider efforts to strengthen network connectivity in the long term.

Many municipalities face ongoing connectivity challenges that boil down to affordability, accessibility and infrastructure issues. Though federal stimulus funding has paved the way for state and local governments to invest in broadband connectivity, they still must go through the process of installing conduits and cables to increase the bandwidth and performance of next-generation networking technologies like 5G. This process — though critically necessary — is both capital-intensive and time-consuming. But municipalities have pressing connectivity needs they must solve for today.

Additionally, governments continue to grapple with legacy technologies and on-premises environments that aren't always compatible with modern connectivity solutions. Accessibility is another pressing challenge. Recent studies show 72 percent of U.S. households in urban areas have access to the internet while only 37 percent of rural households do.[1] According to the Federal Communications Commission (FCC), despite significant progress in expanding high-speed internet across the country, 19 million Americans lack access to fixed broadband. In rural areas, the problem is even more pronounced, as 14.5 million people don't have this service. Even in areas with broadband service, 100 million people don't subscribe,[2] perhaps because they cannot afford to.

As these figures make clear, network transformation is crucial for enabling governments and the constituents they serve to access modern digital applications for activities such as hybrid work, distance learning and digital service delivery. Network transformation is also critical to advance key goals such as digital equity, increased public safety, and economic growth and development.

This transformation can be a crucial catalyst for state and local governments as they try to achieve these strategic objectives. To kickstart both their digital and network transformations, government organizations can begin by focusing on modernizing their core technologies.

19 M
Americans lack access to fixed broadband, with 14.5M of them living in rural areas.

1/ Core Technologies: Driving Automation & Legacy System Modernization

Network transformation is inextricably linked to digital transformation. For governments to become more agile and deliver better and faster service, they need to modernize legacy networks and redesign their network architecture.

The traditional approach to networking in the public sector typically has relied on a hub-and-spoke model with branch sites connected to a centralized data center via a router over public or private fiber, Ethernet or multiprotocol label switching (MPLS) connections. Within this network architecture, traffic is routed based on IP address rather than business priorities, which means data from mission-critical applications often isn't routed as quickly as it should be.

Traditional government networks weren't built to handle the massive bandwidth requirements associated with thousands of employees working remotely or multiple agencies using cloud, IoT-based and AI-driven applications. But the world has changed, and government networks must change along with it to support these use cases and other emerging needs within government operations. To accelerate network transformation, governments must transition from legacy networks to software-defined networks that are better able to meet the bandwidth and performance demands, low latency and high availability requirements necessary to run a digitally driven organization.

Allen Moore, managing partner for connected health at Verizon, says software-defined wide area networking (SD-WAN), multi-access edge computing (MEC) and 5G are some of the foundational technologies governments need to enact network transformation.

SD-WAN is a virtualized networking technology that overlays MPLS and/or internet circuits, routing low-priority network traffic over less expensive circuits and prioritizing the delivery of data from mission-critical applications to ensure lower latency, better performance and high availability. Government organizations can implement this technology on their own or use SD-WAN managed

services to drive more value from this investment. With MEC, data is stored and processed as close to its intended destination as possible, while 5G is fifth-generation wireless technology that uses low-, mid- and high-band radio frequencies to increase network capacity. 5G also enables the network to better support latency-sensitive, high-bandwidth applications.

"If you have SD-WAN with network function virtualization [or software-based, rather than hardware-based network services], then you really have the best of both worlds," Moore says.

Moore adds that MEC takes an organization's compute environment and moves it closer to its user community, which is critical for the optimal delivery of voice and video data transmissions. He says one of the capabilities that makes 5G so valuable is that it enables network slicing, a network architecture that allows multiple software-defined networks to use the same physical network infrastructure. With network slicing, government organizations can create isolated and defined networks designed to meet a specific use case or application requirement, whether it's powering an unemployment claims system, business permitting application or video surveillance system for police investigations.

"The application always gets the bandwidth. It always knows that it has a transmission path because it is that impactful to the organization," Moore says.

By redesigning their network architecture around software rather than hardware-based connectivity solutions, state and local governments can position themselves to integrate cloud and AI-driven technologies that automate their processes and increase data visibility and accessibility throughout their organizations.

Once they lay this foundation, governments can put their network to work for a variety of mission-critical use cases, such as initiatives that improve the employee experience and lead to workforce transformation.

With network slicing, government organizations can create isolated and defined networks that are designed to meet a specific use case.

2 / Workforce:

Delivering a Better Employee Experience

Even before the pandemic, government agencies were gradually moving to the cloud. However, the public health crisis accelerated cloud migration and the need for these organizations to modernize their networks as employees' homes become the new perimeter. Brett Barganz, manager of product development at Verizon, says network transformation can help governments increase their agility in several ways.

"Governments, in many cases, have a need to add a branch office. That may be a new courthouse to serve constituents in other parts of the county so they don't have to travel as far, or a health and human services department opening a new health center," he says. "Then there are temporary sites. In the past, election sites haven't needed permanent or even significant connectivity, but as election security becomes a larger issue, election sites may require more advanced thinking when it comes to connectivity."

In addition to use cases like those, one of the most urgent factors driving network transformation is today's hybrid work environment. Municipalities may have to redesign their network architecture to support a new remote work infrastructure that encompasses solutions such as videoconferencing systems, digital collaboration platforms, cloud-based document management systems and IT asset management tools. They'll also need to enact network transformation to expand connectivity for residents throughout their local area, says Sunil Rajan, a managing client partner for the public sector at Verizon.

"Cities are now concerned about employers closing offices and having people work from home. Employees don't want to go back into the city anymore, so how do you start driving the whole-return-to-work aspects from an economic perspective as cities look to keep those revenue streams going?" Rajan says. "5G can enable things like internet connectivity for employees on mass transit systems, so they can be productive while going into the office."

Both Barganz and Rajan say that although governments must focus on the technological aspects of network transformation, effective change management is just as critical. They say leaders need to start with a clear vision and goals, revamp their business processes to reflect behavioral changes that often come with remote work, and develop digital skills training to effectively use the tools they've implemented.

"For organizational change management, I usually think of three big things: communications, behavior change and training," Barganz says. "You need to have leadership support for it and communicate to employees why it's important for your organization to enable everyone to work from home — the goals behind it and the vision behind it. You also need immediate managers communicating out the message about how this is going to impact their specific employees."

Network transformation will pave the way for workforce transformation in government. As governments prepare for the future of work, they can bring their people, processes and technology together to empower employees, streamline and automate routine and repetitive tasks, and better align their work with their organization's overall mission.

Municipalities may have to redesign their network architecture to support a new remote work infrastructure that encompasses solutions such as videoconferencing systems, digital collaboration platforms, cloud-based document management systems and IT asset management tools.

3 / Public Safety:

Protecting Communities & Improving Emergency Response

Public safety agencies rely on technology to keep their communities safe, from GIS spatial information tools, drones and radio communications technologies to data management and evidence collection systems.

However, reliable connectivity continues to be a challenge for these agencies. With crime rising in several parts of the country[3] and increased calls for transparency within law enforcement, network transformation can help first responders and law enforcement professionals improve public safety and their interactions with the public.

Sam Kroack, senior manager of government solution architects at Verizon, says robust network connectivity has several applications in public safety. It can make it easier to safely collect, store and analyze data from body-worn cameras, crime tips and evidence generated from the public via social media. It can also accelerate information delivery from a 911 dispatch center to officers in the field to improve situational awareness when they respond to a crime scene.

A large water utility leveraged 4G LTE networks, a dedicated mobile app with real-time connectivity and smartphone devices purpose-built for hazardous environments to maintain communications with firefighters in remote areas as they battled wildfires.

"For public safety agencies, it's become really important to have an open dialogue with the constituents they support. That will only increase trust, reliability and relationships as we go forward. Technology is at the forefront of making that happen," Kroack says.

Network transformation can also support purpose-built applications that are specifically designed for public safety and law enforcement agencies, such as heart monitoring technologies that will be able to allow EMS workers to share information in near real-time with hospitals as they transport patients. Or smart, IoT-enabled helmets that increase firefighters' field of vision in zero- or low-visibility situations.

With better networks, first responders can take advantage of 5G-enabled unified communications platforms that ensure their communications are highly secure and prioritized for rapid delivery across the network. Advanced network technologies can also help ensure public safety agencies' communications infrastructure is highly available, reliable and resilient — as long as the network is built with redundancy in mind and incorporates battery and satellite backups to reduce the risk of network failures.

Some municipal departments have already implemented network modernization to improve emergency response operations. For example, a large water utility in the western U.S., which supplies water to firefighters, leveraged 4G LTE networks, a dedicated mobile app with real-time connectivity and smartphone devices purpose-built for hazardous environments to maintain communications with firefighters in remote areas as they battled wildfires.

Implementing these advanced network connectivity solutions has allowed the utility to improve the delivery of water resources, enhance interoperability across devices so the agency and firefighters can communicate across both phones and radios, and help ensure worker safety with communications that meet OSHA and union requirements.

Cory Davis, director of Verizon response and public safety operations, says network transformation will enable public safety departments to "communicate more effectively, not only with their agencies, but with all of those who are part of the response recovery efforts. It will also allow agencies to make quicker and smarter decisions."

As agencies modernize their networks, Kroack says it's important to remember there's no one-size-fits-all approach to network transformation. For example, agencies may still be able to make good use out of various public safety technologies with 4G connectivity, rather than 5G.

"You're only enhancing your network — you're not eliminating it," Kroack says. "With network transformation, it's about really understanding where you want to go and knowing that 5G may not be the answer for everything, but it might be the answer for a lot of things."

4 / Connectivity & Access: Closing the Digital Divide

Just as network transformation can look different within agencies, it can also take different forms depending on geography.

"Transformation looks different depending on whether you're in an urban or rural area," says Verizon's Davis.

In rural communities where there may be limited funding and not as many fiber lines or infrastructure to expand network capabilities, governments will need to devise a different plan for network modernization.

Still, some of this can be resolved by implementing a whole-of-state approach to network transformation, as some states have done with cybersecurity. Federal stimulus relief — including the American Rescue Plan Act — as well as other federal broadband funding streams have given states a prime opportunity to make these investments in rural areas. They've also lowered some of the cost barriers for network providers who have not yet expanded in these locations because they're difficult to reach or have rugged terrain.[4]

But it isn't just rural communities that will benefit from advanced connectivity. Over the last two years, children from low-income households or those who were displaced during the pandemic and other natural disasters have struggled to fully participate in distance learning because they didn't have the connectivity — or in some cases, the devices — to engage with their classmates and teachers.

Modern connectivity solutions have helped some school districts, like Fort Wayne Community Schools (FWCS) in Indiana, address this challenge. FWCS has focused on maximizing connectivity for its nearly 30,000 students. Before the pandemic, the district already had a goal to provide every student with a digital device. However, the pandemic accelerated the district's 1-to-1 device implementation and gave it a new goal to facilitate remote learning.

This was an uphill battle, considering only 60 percent of the district's students had connectivity at home. FWCS partnered with Verizon and provided mobile hotspot (MiFi) devices to qualifying students. The solution allowed FWCS to deliver cost-effective, reliable and strong connectivity that could travel with students. This was crucial because many students temporarily moved or were displaced during the pandemic. Each mobile hotspot was also configured with an enterprise mobile device management solution, which also strengthened network security.[5]

In rural communities where there may be limited funding and not as many fiber lines or infrastructure to expand network capabilities, governments will need to devise a different plan for network modernization.

Along with MiFi devices, Verizon's Dolezal says a host of other technologies are emerging that can address the digital divide, such as 5G fixed wireless access, an alternative to wireline access to a single location that is provided on a public network. This technology particularly benefits suburban and rural areas and allows them to access broadband services.

"The will to address this issue is much stronger than before. The government must take a hard look at current infrastructure and assess what must change to address these inequities," he says. "That's really where governments are going to have to focus: How do they enable this wireless coverage and how do they make it accessible to their constituents?"

Confronting the digital divide will also help governments foster more equitable service delivery. This is critical as more agencies onboard cloud-based solutions and create additional digital services.

"The network is a tool and a means to an end to access these applications in a high-quality way," Dolezal says.

Dolezal adds that he believes wireless connectivity is key for the future because it is considerably more cost-effective for governments to implement than building out wireline connections. Research indicates better connectivity contributes to improving health and economic outcomes for residents and that it also coincides with greater economic and population growth,[6] so there are compelling reasons for governments to invest now.

"A government policy that promotes proliferation of wireless coverage, especially in traditionally poorly served areas, will potentially make a very large difference," Dolezal says.

Over the last two years, children from low-income households or those who were displaced during the pandemic and other natural disasters have struggled to fully participate in distance learning because they didn't have the connectivity — or in some cases, the devices — to engage with their classmates and teachers.

5 / Cybersecurity:
Securing the New Edge

Regardless of whether state and local governments improve network connectivity to transform their workforce, enhance public safety or advance digital equity, they need to make sure their networks are secure.

As public sector organizations introduce new applications and technologies into their IT environments, they expand their attack surface. In 2020, cybercriminals targeted nearly 2,400 governments, schools and health care facilities with ransomware attacks.[7] In addition, denial-of-service attacks, malware, phishing and other social engineering schemes continue to be persistent threats for governments.

In this threat environment, governments need to be laser-focused on endpoint and network security to ensure business continuity and to help avoid a massive security breach that could undermine the public's trust and increase their organization's regulatory risks. Grady, a Verizon security expert, says network transformation gives state and local governments the opportunity to strengthen their security posture.

"When you're stepping back and looking at your network infrastructure strategically, it gives you an opportunity to look broadly at all of the pieces of the puzzle. That includes your security operations and how well it's integrated into the network visibility," he says.

Grady says incorporating network detection and response (NDR) tools into their security strategy can help governments as they undergo network-driven digital transformation. These tools capture massive amounts of network traffic, identify security gaps and anomalies in an organization's IT environment, and enable proactive threat hunting. As a managed service, governments can leverage NDR technologies for security automation and orchestration, relieving some of the burden on their IT teams and redeploying these resources to other digital transformation initiatives beyond just network management.

If an organization is looking for a security framework to follow as it navigates network transformation, Grady suggests the secure access service edge (SASE) model, which integrates SD-WAN and other cloud security approaches.

"SASE extends security to network transformation. It's a great opportunity to bring together capabilities like SD-WAN, secure web gateway, software-defined perimeter and Zero Trust, which assumes that a device doesn't belong on the network and constantly validates that it does," he says.

As governments modernize both their networks and IT assets, they'll need to continually assess their security risks. No organization will ever have the resources to combat every threat. But by better understanding the specific threats they face, making security investments that are proportional to their organizations' unique risks and employing NDR tools for enhanced network security, state and local governments can significantly reduce their risk profile.

As public sector organizations introduce new applications and technologies into their IT environments, they expand their attack surface.

6/ Budget & Cost Control:

Optimizing Funding & Improving Financial Sustainability

Any transformation, whether digital or network-based, will come at a cost to government organizations.

But the funding environment has never been more favorable for state and local governments to strategically invest in network transformation. Though there are upfront costs with modernizing network architectures, the long-term return on investment is nearly immeasurable.

For one, network transformation makes it easier for governments to implement advanced security tools, like NDR technologies or AI-driven security automation platforms. Considering the average cost of a data breach now tops $4 million,[8] this cost avoidance alone can help state and local governments achieve better cost control.

"Immediate savings is going to come in the fact that you're less likely to be a target of a ransomware attack," Verizon's Moore says.

There's also the hard-to-quantify cost and time savings associated with automation and increased employee productivity, along with the more tangible costs associated with better IT asset management, such as reducing licensing fees and vendor lock-in. Moore says network transformation makes it easier for government organizations to right-size their IT environments, giving them the ability to implement best-of-breed solutions without a heavy IT lift and retire legacy applications that no longer serve their needs.

Though network transformation will be an ongoing process for many government organizations, Moore says employing a network-as-a-service approach is one of the best ways governments can cost-effectively modernize. Network providers like Verizon often work with government agencies to deploy technologies as an operating expense rather than a capital expense, so it becomes a monthly cost. This approach also allows agencies to benefit from unified network management, since a suite of interoperable network connectivity and security tools function together as part of this service.

Going forward, governments will need to increase their resilience. Network transformation will be a key part of this effort. Tapping into current federal funding streams, working collaboratively with network providers, and potentially adopting a service-based approach to network security and management can put governments on a sustainable path toward modernization.

The funding environment has never been more favorable for state and local governments to strategically invest in network transformation.

Best Practices for Network Transformation

At the "innovate state of ready," governments will move from a reactive stance to a proactive approach where they are more equipped to anticipate constituents' needs and that of their own workforce.

As state and local governments look to enact network transformation, they should consider using a framework called "The Five States of Ready"[9] to help them navigate their modernization journey.

The Five States of Ready

1 Start

An agency or government should begin by identifying their core business needs, align them to key strategic initiatives and then identify technology partners who can put them on the path to modernization.

Grady says when assessing technology partners, governments should "look for a provider that can start at the end and help the organization refine its vision, articulate what it wants to be, understand what the possibilities are, and not just look at the engagement as a technology implementation, but as a partnership."

"When you talk about digital transformation in government, you're essentially talking about changing society to a certain degree — whether it's smart cities, drones or driverless cars to improve public transportation," Grady adds. "The possibilities really are endless, especially with 5G, but they require vision and a partner who can help organizations get there."

2 Adapt

Once agencies identify their needs and choose a technology partner, they can begin to implement and test secure, interoperable network connectivity solutions that enable them to be more agile and efficient and drive better performance.

For state and local governments, these solutions may include some of the core technologies previously outlined, including SD-WAN and managed network services. Implementing these technologies can also help public sector organizations better understand and deploy their data for a range of use cases, whether it be hybrid work, emergency response communications or digital service delivery.

3 Elevate

At this stage, organizations will start making better use of the data flowing into their networks. They'll capture it at scale and begin to use it to inform their decision-making to drive better outcomes.

In government, this could mean uncovering insights that lead to the implementation of self-service tools to reduce call center wait times or pinpointing which intervention programs are most effective at reducing juvenile

interactions with the criminal justice system, and therefore doubling down on these efforts.

4 Innovate

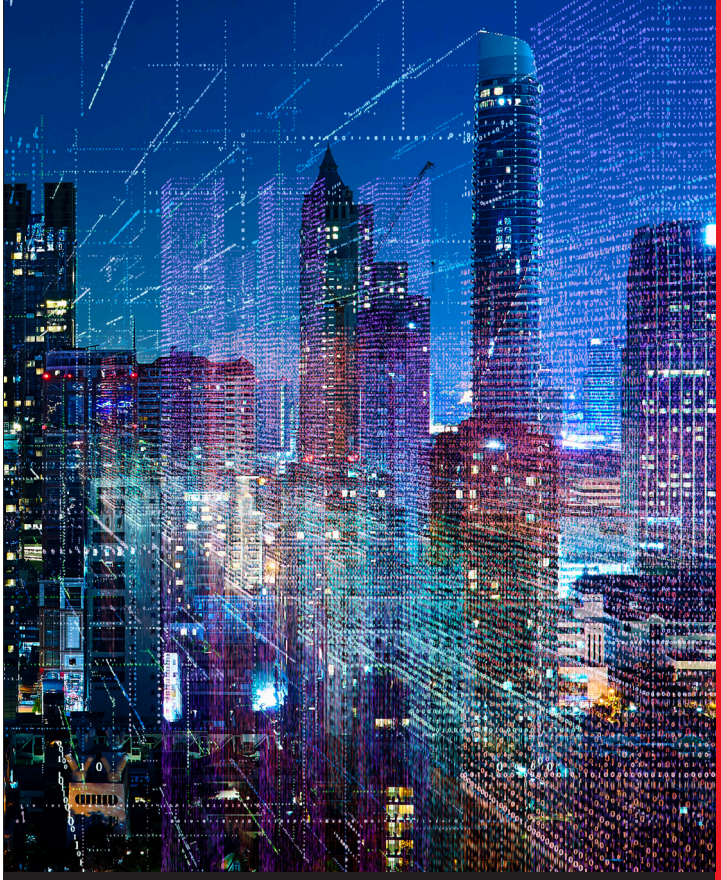
At this advanced stage, an agency will have evolved into a more data-driven organization and its network architecture will be optimized to deliver on its evolving business needs.

At the "innovate state of ready," governments will also move from a reactive stance to a proactive approach where they are more equipped to anticipate constituents' needs and that of their own workforce. What does this look like in the real world? IoT-enabled communications on public transit, digital kiosks that deliver timely alerts in public spaces, and real-time response systems that increase situational awareness for first responders minutes before they arrive on scene — just to name a few.

5 Adapt

This end state isn't just aspirational — it's achievable.

At this stage, governments will be well equipped to adopt the latest technologies to create a more responsive and agile operating model. They'll be better positioned to make changes that truly improve residents' quality of life and drive business and economic growth, and 5G and MEC will be a core part of their network design. Modern connectivity will bring to life smart city initiatives and digital interfaces and applications largely will be the first touchpoint through which constituents interact with government — ultimately making real the promise of digital government.



Conclusion

Network transformation is the backbone of digital transformation, but to start on this journey, governments must be intentional in their approach.

Over the last two years, governments have had to rapidly adapt. They haven't had sufficient time to assess what a future-ready network architecture really looks like. Though governments have made gradual improvements to their network and IT infrastructure in recent years, now is the time — with a huge influx of federal aid — for them to make lasting and impactful strategic investments.

With the rapid shift to the cloud, increased calls for digital equity and a relentless threat environment that makes holistic cybersecurity more vital, governments must establish a strong foundation for reliable, high-performing network connectivity. There's never been a more critical time to do this, because, as Dolezal says, "what we've learned during the pandemic is that quality connectivity is no longer 'nice to have' — it's essential."

This handbook was created by the Government Technology Content Studio, with information and input from Verizon.

Endnotes:

1. https://datasmart.ash.harvard.edu/news/article/how-local-authorities-and-communities-are-working-better-connectivity-bridge-digital
2. https://www.fcc.gov/reports-research/reports/broadband-progress-reports/eighth-broadband-progress-report
3. https://www.npr.org/2021/09/27/1040904770/fbi-data-murder-increase-2020
4. https://www.brookings.edu/blog/up-front/2021/08/18/the-benefits-and-costs-of-broadband-expansion/
5. Verizon Case Study: "Fort Wayne Delivers Remote Learning During a Pandemic in Record Time"
6. https://www.brookings.edu/blog/up-front/2021/08/18/the-benefits-and-costs-of-broadband-expansion/#:~:text=Increasing%20access%20and%20usage%20of,formation%2C%20and%20lower%20unemployment%20rates%2C
7. https://www.washingtonpost.com/local/local-government-ransomware-dc/2021/08/05/048051cc-efc6-11eb-81d2-ffae0f931b8f_story.html#:~:text=In%202019%2C%20cybersecurity%20experts%20noticed,threat%20remains%20consistent%2C%20experts%20say
8. https://www.ibm.com/security/data-breach
9. https://enterprise.verizon.com/resources/whitepapers/digital-transformation-strategy-for-public-sector/

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.**

For: verizon

Verizon Communications Inc. was formed on June 30, 2000 and is celebrating its 20th year as one of the world's leading providers of technology, communications, information and entertainment products and services. The company offers voice, data and video services and solutions on its award winning networks and platforms, delivering on customers' demand for mobility, reliable network connectivity, security and control. For more information, visit **verizon.com/publicsector**

PHOTOS PROVIDED BY WWW.SHUTTERSTOCK.COM

© 2022 e.Republic. All rights reserved.