Delivering constituent services with the network of the future

AT&T Public Sector

AT&T | government technology

The COVID-19 pandemic forever changed the public sector in the United States. It redefined the nature of work for public employees. It broadened governments' understanding of the digital divide and the critical role they play in working to close that gap. It accelerated agencies' digital transformation efforts by years or even decades.

And it fundamentally altered the relationship between government agencies and the communities they serve. Throughout the pandemic, the general public relied on federal, state, tribal and local governments to provide them with critical information and vital services. Whether it was for reliable news on vaccines or school openings, or access to programs such as unemployment insurance, rental assistance or SNAP benefits, the systems of government proved crucial in residents' daily lives.

Now, as government leaders look to the future, they are only beginning to understand this seismic shift in delivering constituent services—and the ways in which technology, tools and infrastructure must adapt.

Improving the experience for constituent service delivery is a central part of any post-pandemic planning conversation in the public sector. State and local government technology leaders ranked "digital government/digital services" as their second-highest priority for 2022, behind cybersecurity and risk management.[1] It's a top priority at the federal level as well. In December 2021, President Biden signed an executive order on "transforming the federal customer experience and service delivery." Among other mandates, the order calls for redesigning the USA.gov website to make it more user-friendly and intuitive, and it includes a commitment to improve 36 "customer service experiences" across 17 federal agencies.[2]

As governments at all levels redouble their commitment to customer service and transforming constituent service delivery, they will need a network that can accommodate these new demands. In planning for the future, four critical priorities are top of mind: the decentralization of employees and constituents; the flexibility of the network itself; the need for new approaches to cybersecurity; and the ability to optimize funding for the technologies that will power the public sector for years to come. This handbook provides valuable insights on how state and local leaders can leverage technology to help achieve those goals, and how organizations across the public sector are working to make government more agile, resilient and secure.

Decentralized Work, Dispersed Communities

In March 2020, most government workers were told to work from home for what they thought might be a few weeks. Years later, many are still camping out in home offices, at kitchen tables or in basements, trying to fulfill their agency's mission and provide the level of government service their constituents have come to expect.

The good news is that, for the most part, it has worked. State, local and tribal governments had long lagged private companies when it came to telework policies and flexible schedules. Indeed, most public sector organizations prohibited any work arrangement other than in-person, in the office, five days a week. But almost overnight, they pivoted to the new, decentralized reality forced by the pandemic. Many agencies not only survived in the new environment; they thrived.

"The biggest shift in thinking was the realization that remote workers in many types of jobs can be just as productive—if not more productive—than onsite workers, when they have the right tools, organizational framework and leadership support," says AT&T Sales Center Vice President George Spencer. While "there is no substitute for face-to-face interactions on some type of regularly scheduled basis," he says, modern network collaboration solutions let employees collaborate and engage anytime, anywhere.

"We've learned that remote work is sustainable," agrees Chris Lusey, an AT&T public sector sales manager. "Our technologies and capabilities have helped us

> “We’ve always been trying to deliver services the way residents want them delivered. It’s just that the pandemic changed how many of them want to interact with us.”
>
> - Jonathan Askins, Chief Technology Officer, Arkansas

close the productivity gap in a virtual environment.”

For that reason, many public sector organizations are envisioning a hybrid work future, in which employees are expected to regularly come together in a physical space but have the flexibility to work remotely when it makes sense.

Indeed, even in jurisdictions where all employees returned to the office, there’s a recognition that the workforce of the future must include telework flexibility. In Arkansas, for example, every state employee was required to return to the office full time by summer 2021. But even there, says Arkansas Chief Technology Officer Jonathan Askins, the pandemic has shifted employee expectations.

“Some things are going to change permanently,” he says. “From a workforce standpoint, if we’re not going to allow people to work remotely—even if it’s from Nome, Alaska—recruitment and retention is going to become an issue. We don’t have an answer on that yet. But I feel like that’s something permanent we’re going to have to learn and adapt to.”

As public sector organizations wrestle with hybrid work policies, they also must stay focused on the technology that enables remote work. While the workplace may have changed, the need for employees to effectively communicate with each other did not. Communicating and collaborating as a team is even more important in today’s decentralized environment. As governments transition from the remote work landscape of the pandemic to the hybrid world of the future, IT leaders must collaborate with agencies to give employees the tools and capabilities they need to stay connected. That means answering some important questions, including:

- What is your plan for the laptops, home printers, webcams and other devices procured for employees’ home office setups?
- How will you incorporate tools such as video-conferencing and team chats once most employees are back in the office?
- How can you ensure your collaboration tools continue to be upgraded, updated and secure?
- What tools will enable even greater mobility for the workforce of the future?
- How can strategic partners help plan, execute and maintain your technology needs?

Public organizations are increasingly turning to the cloud to help answer those questions. Cloud platforms offer the flexibility and scalability agencies need to meet the evolving needs of the modern, decentralized workforce. Cloud-based document management systems and other applications help streamline workflows and ensure efficient processes with a dispersed team. And software-as-a-service (SaaS) models, in which agencies contract with private partners for technology, talent and other resources, ensure government networks and tools stay up to date without costly new investments or system relaunches.

With the right technologies and policies, and with strategic partners in the private sector, governments can be confident that employees will have the tools they need to stay connected and engaged in the agency’s mission—no matter where they may be.

New ways to serve constituents

The pandemic didn’t just transform government’s relationship to its employees; it completely reoriented agencies’ relationship to the communities they serve. Overnight, constituents needed to access government services in new ways. Agencies needed new methods to communicate, and to accommodate the unprecedented surge of requests from residents seeking benefits or information. Chatbots, virtual agents and other scalable solutions helped meet the new demand. Countless functions that had always been done in person—city council meetings, court hearings, license renewals—all went virtual.

Of course, even prior to COVID, governments had been engaged in digital transformation efforts for years, quietly adding new online services and digitizing certain processes here and there. But the pandemic accelerated those efforts into warp speed, moving agencies closer to a full virtualization of the government experience.

Now, public sector leaders are focused on honing and

Staying connected to the mission

State and local agencies can have life-changing impacts on the communities they serve. But government technology employees don’t always get to see how their work connects with residents in a meaningful way. That changed in the pandemic, says Allie Larman, the communications technologies manager for the Oklahoma Office of Management and Enterprise Services.

“In 2020, IT technical staff saw a picture of the citizens they hadn’t seen before,” she says. “They really got close with the agencies and got to see how their work affected the agencies and how that affected the citizens themselves.”

Keeping that perspective is critical, she says. “Maintain those close relationships you’ve developed with agencies. Keep the lines of communication open. We as IT people now have a much clearer view of what agencies need in order to fulfill their core mission and take care of their constituents.”

improving the government experience, ensuring constituents can access the information and services they need in the most efficient, effective and empathetic way possible. Residents today expect the same ease of transaction and level of customer service from state and local government that they experience with global retailers, banks and other online companies. And they expect the flexibility to engage with government in any number of ways.

"Technology today needs to meet citizens where they want to be," says AT&T's Lusey. That means letting constituents engage via chat, texting, video and social media—in addition to mail, email, phone and in-person visits. "And citizens want to be able to transition from chat to phone to in-person. Agencies need to support that entire seamless constituent journey."

But if some of the specific technologies have evolved, says Arkansas' Askins, the underlying goals of government service delivery remain the same.

"The key is listening to our customers about how they want different services delivered, and then trying our best to meet that model," he says. "Is that a change from the past? Gosh, I hope not. I hope it's just the way we've been doing business. We've always been listening. We've always been trying to deliver services the way residents want them delivered. It's just that the pandemic changed how many of them want to interact with us."

> "Technology today needs to meet citizens where they want to be."
>
> - Chris Lusey, Public Sector Sales Manager, AT&T

Modernizing the contact center

Since the onset of the pandemic, governments have made incredible strides to enable a decentralized workforce and engage with their constituents in safer, more convenient ways. There is perhaps no better example of that transformation than the rapid evolution of the government call center.

Just ask Allie Larman, the communications technologies manager for the state of Oklahoma's Office of Management and Enterprise Services. In her role, Larman oversees contact center operations for the entire state. Prior to the pandemic, she says, Oklahoma's call center looked like a lot of other states': Agents came to the office, answered phones, and provided information to callers or routed them to the appropriate agency.

The underlying technology was a patchwork of solutions. "There were various contact center platforms across the state, a mix of on-premises systems and hosted," Larman says. "There was a lot of variety. We'd been working toward a centralized platform for some time. But 2020 really sped up that unification of our contact center solutions."

When the pandemic hit, Larman's team had to figure out how to let agents handle calls remotely. "We had to turn every agent into a teleworker," she says. "We quickly had to give them the tools they need, but also train them on how to use them."

At the same time, they had to confront a deluge of constituent service requests.

"We saw an unprecedented increase in our call volumes. Our queues became huge, and it was very important that we were able to grow and expand with the citizens' needs," Larman says. That meant rapidly launching chatbots and live agent chat interfaces. And it meant staffing up to meet demand. One agency, for example, averaged 12 agents on duty during a typical day prior to the pandemic. At the peak of the COVID crisis, Larman says, the same agency had 1,200 agents a day. By fall 2021, that number had settled back down to about 300—still a 2,400% increase from the previous norm.

The key to accommodating fluctuations like that, says Larman, was moving to a unified contact center platform that could rapidly scale to meet changing needs.

Just as important as the unified platform itself was the fact that it was built on an agile, flexible network. "AT&T provided contact center solutions to the state of Oklahoma by connecting it to our enterprise voice platform and delivering it over our network," Lusey says. "That enabled them to scale to meet the needs of the pandemic."

Deeper relationships with private partners will continue to serve the state in the future, according to Larman.

"I think we'll continue to need strategic partners that can help us scale up services and meet new requirements," she says. "I think that's a permanent shift. We need partnerships that allow us to bring in new resources or solutions or headcount—whatever we may need. We've got to make sure we keep those partnerships strong."

The Oklahoma state contact center today represents a vast improvement over March 2020. It's agile enough to instantaneously roll out new initiatives statewide. It's flexible enough to scale as demand changes. The unified platform enabled Larman's team to implement workforce management and quality management throughout the environment. And the platform produces valuable web-based performance management wallboards, which are linked to every agency so executive leaders can respond to changes in real time.

And constituents can engage via voice, texting, chat or email. In the future, that will expand to include video, social media, conversational artificial intelligence (AI) and more. "We don't have 'call centers' anymore," says Larman. "No one should. We have 'contact centers,' because that's what our citizens need."

A New Network for a New Era

The Choctaw Nation is a vast American Indian territory in the southeast corner of Oklahoma. The tribe includes some 225,000 members across the country. But the territory itself has roughly 40,000 residents spread across an area larger than Massachusetts. It's a decidedly rural place, with plenty of wide open spaces.

But like the rest of the world, the Choctaw government sent its employees to work from home when the pandemic hit in March 2020.

"The pandemic made us realize we've got a large percentage of our workforce that can successfully work from home," says Choctaw Nation Director of Enterprise Systems Mark Ross.

Dustin Stark, IT director for the Choctaw Nation, agrees, referring to the early days of the pandemic as "a forced large-scale telework pilot." Remote work, he says, "really wasn't on the organization's near-term roadmap. Now we had to understand how to build it out at scale."

But the government faced one very big challenge in making that work: poor network connectivity.

"The biggest problem of remote work for us was connectivity at the home," says Ross. Many government employees lacked reliable high-speed home internet; in many places, it's not even an option. "We don't have enough middle-mile fiber, which constrains the last-mile in getting access to households," he says. "We just don't have enough broadband to the home. And in a remote environment, we've got limited work-around options. Service is simply not available in some of these areas."

"In a lot of the areas of our jurisdiction, the connectivity options are fairly limited," agrees Stark. "The digital divide is something that's real in Oklahoma."

The Choctaw Nation is hardly alone. As governments everywhere shifted to telework, online services and remote education, digital equity has become a paramount concern—in rural counties, suburbs and dense urban neighborhoods. The pandemic changed the way we work, the way we communicate, and the way we access goods and services. And that has fundamentally altered the way we think about the network.

Connectivity has become an essential lifeline. But for IT leaders, responding to the needs of the pandemic and planning for the future isn't just about expanding the network. It's about reimagining the network itself—what it looks like, how it functions, and how it lives and breathes.

> "In a lot of the areas of our jurisdiction, the connectivity options are fairly limited. The digital divide is something that's real in Oklahoma."
>
> - Dustin Stark, IT Director, Choctaw Nation

A model turned inside-out

"Digital transformation, increased virtualization and the move to cloud generally has turned the entire network model inside out," says Thomas Steegmann, an AT&T principal architect supporting the public sector. "Being 'inside the network' used to mean people sitting in a government building on local area network [LAN]. Now they could be anywhere, and we have to reorient the network to account for that."

Before, when employees were sitting in their offices, they were likely accessing applications—for email, file sharing and all other job-related tasks— that were housed in a nearby government-run data center.

"When those apps were sitting in a data center that was proximate to where the employees were, it was really your LAN infrastructure that was going to make the difference," says Steegmann. As those applications have migrated to the cloud—first before the pandemic and then in response to it—the needs of the network changed. Connectivity between remote locations and headquarters became less important;

instead, the network had to connect remote users directly to the internet or hosted cloud services, Steegmann says. “You need to get those remote locations directly out to the cloud providers rather than hair-pinning back through HQ.”

That shift is a permanent one, he notes. “Now, even if everyone is back sitting at their desk in the headquarters building, and they want to access Office 365 or Amazon Web Services or Azure or whatever—that’s traffic that’s going out to the internet and then coming back in. That’s a traffic pattern that didn’t exist before. That’s a huge change for the network.”

This difference is what enabled some governments to transition more seamlessly than others in the earliest days of the pandemic, says Erik Lindborg, an AT&T assistant vice president for sales to state and local government and education. And it’s what will help them flex, scale and adapt to meet the demands of the future.

> “Digital transformation, increased virtualization and the move to cloud generally has turned the entire network model inside out.”
>
> - Thomas Steegmann, Principal Architect for Public Sector, AT&T

“You had some governments with hub-and-spoke, centralized ethernet networks,” Lindborg says. “Those networks had fixed speeds, fixed throughputs and they were designed from a capacity standpoint to meet yesterday’s needs. They may have been highly functional, but they were not robust or resilient enough to respond in a crisis.”

At the other end of the spectrum, Lindborg says, were organizations that had incorporated software-defined wide area networks (SD-WANs), which allow speeds to increase or decrease as demand grows and contracts. “That way, you have this basic infrastructure with the ability to increase your throughputs as needed.”

Even more important for building network resilience, he says, is for governments to work with a private sector partner to provide much-needed expertise and an agile architecture that can easily scale up as needs change. “As the network flexes, those governments are ideally positioned to manage increased demands, because of those managed services at the edge and working together with their carrier.”

Architecting for the future

As governments work to implement more flexible, adaptable, breathable networks, they’re also rethinking the components that make up that network.

“For some time now, we’ve had sort of a two-sizes-fits-all approach,” says AT&T’s Steegmann. “Either you have a carrier-based Layer 2 network or a carrier-based Layer 3 network, or maybe you lay your own fiber and put your own Layer 2 and 3 stuff on it. But basically, that’s how networks have looked.”

Going forward, he says, IT planners will need to think about creating a more comprehensive network ecosystem.

“Building the network of the future means looking more at technologies like SD-WAN that can stitch together different modes of communication and different transport mediums to create high-uptime, high-efficiency, high-performance networks,” he says. That means reimagining the network as a web of different technologies including WAN, LAN, 5G, residential broadband, cellular hotspots and anything else that helps employees and constituents stay connected to government. “As part of this network re-architecture we’re seeing—partly in response to what happened during COVID—networks are really going to look different a few years from now,” Steegman says.

Sustaining the network of the future also requires IT leaders to evolve and modernize their approach. As network connectivity grows more vital, tech leaders must constantly make sure it serves the needs of government and the community, says Askins, the Arkansas CTO.

“Throughput is something we think about every day now,” he says. “Pre-pandemic, if we saw a small blip in service or a minor network disruption, we might have thought, ‘Well, let’s see what happens. This’ll probably work itself out.’ Now, even the tiniest blip sets off alarms. We take it very, very seriously, because we know the bandwidth has got to be there.”

> “Every minute of every day, you have to be prepared for your network to fail. That’s how you build the network of the future.”
>
> - Erik Lindborg, Assistant Vice President for SLED Sales, AT&T

More than anything, says Lindborg, the key to ensuring a reliable, resilient network is understanding that it won’t always work, and having a plan in place for when problems arise. That means thinking about network diversity and layers of redundancy. It means optimizing a mix of traditional ethernet and software-defined networks. It means transitioning to cloud platforms and managed service agreements with trusted, established partners.

“Inevitably, there will be elements of your network that fail. It’s incumbent upon IT leaders to work with that design theory in mind,” he says. “Every minute of every day, you have to be prepared for your network to fail. That’s how you build the network of the future.”

A Modern Security Paradigm

The shift to digital service delivery and the decentralization of the workforce created massive new challenges for cybersecurity professionals. As agencies embraced hybrid telework, a completely amorphous and unfamiliar perimeter added complexity to the already monumental task of safeguarding government networks and constituent data.

Cybercrime is thriving in this disrupted environment. State and local governments were already prime targets for hackers and bad actors before 2020; documented cyberattacks on states and localities rose nearly 50% from 2017 to 2019.[3] The pandemic saw the number of attacks skyrocket. At least 2,354 governments, health care facilities and schools in the United States were the victims of ransomware attacks in 2020, according to experts, a number that continues to grow.[4] Those are merely publicly reported attacks—the actual incidence rate is certainly far higher.

Along with growing in sheer number, hacking and phishing attacks have become more sophisticated. And as events such as the May 2021 Colonial Pipeline breach make clear, bad actors aren't just targeting sensitive data and government communication networks. They're threatening critical pieces of physical infrastructure as well.

In this new era of constant threats and decentralized users, cybersecurity leaders need to adopt an entirely new paradigm. A legacy approach based on fortifying government networks with firewalls and other protections simply cannot stand up to today's threat landscape, says AT&T Cybersecurity Director Bindu Sundaresan.

"If we go back to how we've traditionally thought of cybersecurity, it's in the form of the C.I.A. triad: confidentiality, integrity and availability of information," Sundaresan says. "But all that was set from the point of view of perimeter-centric security: Whoever is on the outside should not be able to access things, but once you're in, you have access."

As the perimeter itself has dissolved, that approach is no longer viable.

"For digital government to evolve, we can't have this cybersecurity philosophy of just putting up all these walls and focusing on preventing a threat," she says. "The center of cybersecurity today is really all about trust, privacy, risk and resilience. Constituents want to be able to access services from anywhere, at any time, on any device. And we expect the security model to support that."

An effective cyber strategy—one based on resilience and adaptability rather than fortification—is built on effectively protecting digital assets but having a plan in place to manage risks and mitigate attacks and breaches when they inevitably occur.

"In a modern cybersecurity approach, we have to assume that the network is always hostile," Sundaresan says. "We have to assume that internal and external threats will always be on our network. We have to think about authenticating every device, every user, every network flow."

Embracing zero trust

At the heart of the new security paradigm are the core components of improved identity and access management (IAM) tools and a Zero-Trust model for security. Zero Trust is a strategic approach that eliminates implicit trust for network users and continuously validates them based on their identity, behavior, and the workflows and level of data they are attempting to access.

"Think of drawing concentric circles around your protect surface," says Sundaresan. "Your innermost circle includes the data you most have to protect, and then you work out from there. "The rings will change depending on your identity, where you're accessing the data from, and whether you're

using a legacy technology or a cloud-native one."

State and local organizations are eager to embrace Zero Trust, but there is still a lack of understanding about what it means, she says.

"A lot of people have the misconception that they can just go buy a product, flip a switch and they'll be in Zero-Trust mode. But it's a philosophy and a principle. It's an underlying shift in how we provide access to information and how information is used."

Laying the right foundation for Zero Trust involves painstaking processes that can be challenging for any organization:

Conduct a thorough assessment of your entire network, and inventory every server, every printer, every internet-enabled thermostat and any other endpoint device. "Document down to every nut, bolt and screw," says Shannon Brewster, an AT&T cybersecurity consulting director. "I don't think a lot of customers are accustomed to the level of granularity this requires. But it enables you to start setting up that Zero-Trust environment."

Employ network segmentation and micro-segmentation techniques to partition your IT ecosystem, protect vulnerable devices and limit the impact of a breach. Instead of traditional firewalls or access control lists, modern software-defined access technology simplifies segmentation by grouping and tagging network traffic.

Classify data based on sensitivity. "Think about what your most sensitive data is and what workflows need the greatest protection," says Sundaresan. "Require multifactor authentication to limit access only to those who truly need it."

Develop a comprehensive cybersecurity plan. Too many organizations still approach security on an ad hoc basis. "You need an orchestrated, cohesive strategy," says Sundaresan, one that's flexible and iterative enough to meet future threats. "You have to have the right policies that are dynamic and adaptive to as many data sources as possible—which is very different from how we've always treated security."

Leverage the expertise of strategic partners. Few public sector organizations have the resources, staff and in-house skills necessary to move toward Zero Trust on their own. The rapidly changing nature of cyber threats and the expanding threat landscape make it more important than ever for state and local organizations to establish ongoing relationships with valued partners in the private sector, says Gene Moore, an AT&T client solutions executive. "With all the changes of remote work and digital services and the need to protect the network, how do you as an agency keep up with that? You can't. You have to find a third-party partner you can trust that you work with consistently."

Stop the shame

A modern approach to cyber resilience means collaborating with peers about new and emerging threats—and sharing information openly and honestly when you're the victim of a breach.

"When cyberattacks occur, there can at times be feelings of embarrassment or shame or vulnerability," says Contra Costa County, California, CIO Nathan Wiebe. "I'm a very strong champion of the idea Brené Brown speaks of in her book *Dare to Lead*. We have to be vulnerable in order to lead. We have to accept that we're not perfect. If someone is the victim of a cyberattack by a sophisticated group, that's not something to be ashamed of. It's something that we need to collectively respond to, and not just point fingers at someone who clicked on the wrong link."

AT&T Cybersecurity Director Bindu Sundaresan agrees: "We have to get away from the gotcha."

Secure from the start

As governments have embraced digital service delivery, their relationship with technology—and securing that technology—has shifted dramatically, says Nathan Wiebe, the chief information security officer (CISO) for Contra Costa County, California.

"IT has traditionally been thought of as support services for other government agencies. But now it's how we actually deliver government services to the public," he says. "So the security needs around these services have become much more significant."

Cybersecurity has evolved from a technological imperative to a business imperative and can no longer be treated as an afterthought. As agencies look to expand their digital offerings and improve how they serve constituents, security must be a part of the conversation at every stage. In many government organizations, CISOs and other cybersecurity directors have gone from back-office support staff to working alongside executive leaders and key decision-makers. That helps ensure security remains

top-of-mind, and that stringent cybersecurity protocols and IAM tools are "baked in" to any new solution an agency considers.

Nonetheless, it's important to remember that governments' business needs come first, says Wiebe.

"I want a seat at the table, but it's merely to ask the right questions of the folks who are actually doing the work. I'm just there as a facilitator to help guide the conversation—not to be setting edicts from the CISO's office that people have to follow."

In fact, Wiebe sees his primary role as that of a convener, rather than a technician.

"I don't look at cybersecurity strictly as a technical engagement. My job is to be a guide, to get answers from people who are much smarter than me, and more involved in the business and governance and technology—not only within my organization but with the private sector and academia and other government organizations as well," he says.

Indeed, as governments focus on strengthening and securing the network of the future, they will need to collaborate even more closely with strategic partners to leverage emerging security technologies.

"Artificial intelligence and machine learning, for instance, are going to take on an increased role in cybersecurity," Wiebe says. "As a local government, I have no business hiring professionals to be doing ML algorithms. Let's leave that to the professionals and focus on being a government that can utilize those services from the private sector. Let government do what we do best."

For a more detailed look at evolving cybersecurity in the public sector, download the Security for the Network of the Future guide here: ps.att.com/SecurityNOF

A Sustainable Strategy for Funding

As governments turn their attention toward building—and securing—the network of the future, they have a rare opportunity: a massive influx of funding from the federal government. Since the onset of the pandemic, Congress has approved some $4.6 trillion in relief spending.[5] That includes hundreds of billions of dollars for businesses, government agencies, hospitals, K-12 schools, higher education institutions and direct payments to citizens.

It's an unprecedented amount of spending to meet unprecedented needs—including digitizing paper processes and other key technology upgrades, says AT&T Assistant Vice President for Public Sector Chris Congo.

"This is a unique moment in time, both from a funding perspective and from a network demand perspective," he says. "You have the ability to fix the gaps in your current network. And now is the time to act."

For states and localities—and especially public sector technology leaders—the biggest federal COVID relief funding came from three sources:

- **The 2020 CARES Act** included $150 billion in direct aid to state, local and tribal governments to help stabilize their initial COVID response measures.[6] That influx was crucial to support remote employees and students amid plummeting state and local tax revenues.
- **The FY 2021 Omnibus Appropriations Bill,** signed into law in December 2020, included $7 billion to expand broadband internet access for underserved

students, families and unemployed workers.[7]

- In March 2021, the **American Rescue Plan Act (ARPA)** provided another $350 billion in direct aid via the Coronavirus State and Local Fiscal Recovery Funds, which could be used broadly to support families and businesses hit hard by the pandemic, maintain vital public services, and make investments that would support a strong and resilient economic recovery. Of that $350 billion, Congress allocated $195 billion to states, $65 billion to counties, nearly $46 billion to cities and $20 billion to tribal governments. That funding was enhanced by an additional $10 billion Capital Project Fund for states and localities to enable work, education and health monitoring in response to the ongoing health crisis. While much of this funding has already been allocated, governments can still use it to cover eligible costs incurred by the end of 2024, and they have until the end of 2026 to spend the money.[8]

> "With every single investment you make now, think about how it is going to prepare you for the future."
>
> - Chris Congo, Assistant Vice President for Public Sector, AT&T

Importantly for IT leaders, state and local governments have broad discretion to use ARPA funds for technology investments, including network upgrades and cybersecurity enhancements, that help address challenges related to the pandemic. In January 2022, the Treasury Department significantly expanded governments' ability to use ARPA funds for broadband infrastructure projects. Originally, eligible uses were limited to connecting "unserved or underserved households or businesses." In its Final Rule issued in January, the Treasury entirely abandoned the "unserved or underserved" requirement, instead enabling ARPA recipients to invest in any new broadband projects or upgrades they deem necessary.[9]

Then came an even bigger infusion of funds for network connectivity. The $1.2 trillion Infrastructure Investment and Jobs Act (IIJA), signed into law in November 2021, includes 375 programs distributed by 12 agencies over the next 10 years. The spending package included $65 billion for broadband, the largest federal investment in broadband expansion in history. The bulk of that money—$42.45 billion—goes to states, territories and the District of Columbia to distribute through competitive grants. The broadband spending also includes $1.25 billion for a new competitive grant for broadband deployments around digital equity, and $1 billion toward "middle mile" competitive grants for broadband deployment. Collectively, the funds will finally enable the United States to achieve its goal of universal broadband, according to the White House, and "ensure that all Americans have access to affordable, reliable, high-speed internet service."[10]

Best practices for optimizing funding

As state, tribal and local governments consider how to best leverage these federal funds to build the network of the future, they have been given wide latitude in how they choose to prioritize spending. On ARPA funding, allowable uses include data and technology infrastructure improvements to digitize paper processes and enhance government service delivery, public health programs and economic relief programs. That can include everything from broadband and cybersecurity to videoconferencing and employee collaboration tools.

In considering how to optimize any new funds, it's important to keep in mind the following best practices:

What else is in the infrastructure bill?

The Infrastructure Investment and Jobs Act (IIJA) includes $65 billion for investments in broadband. But the spending package includes other important funds for government IT:

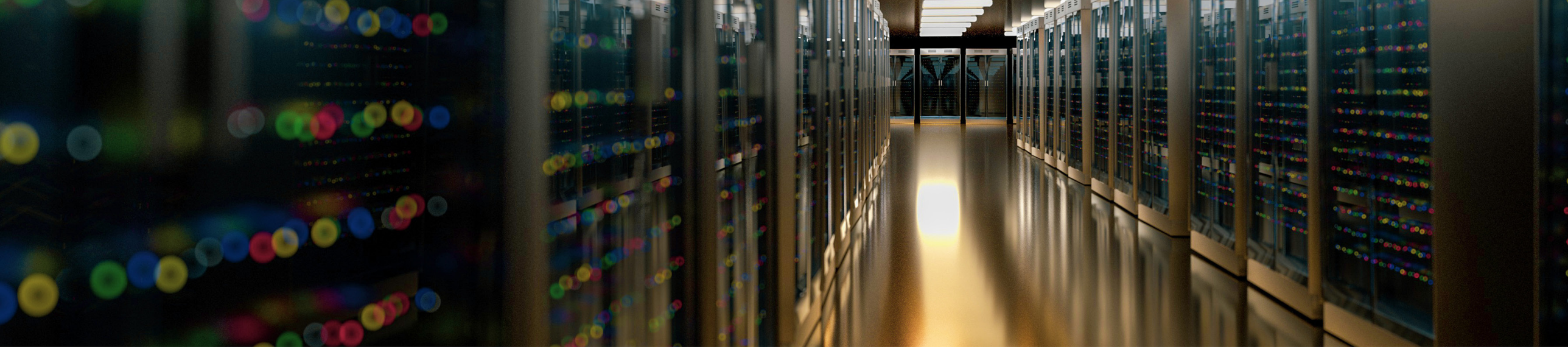
$284 billion for transit and transportation projects, which can include technologies that increase transportation efficiency, ease congestion and improve safety.

$6 billion for electric grid reliability and resilience funding, to be awarded in competitive grants to states and localities.

$1 billion in cybersecurity grants for state, local and tribal governments, to enhance the security of public networks and information systems. To receive these funds, governments will have to provide matching funds from their own budgets, and they must develop and submit a comprehensive cybersecurity plan.

$1 billion to fund the Building Resilient Infrastructure and Communities (BRIC) program, which has replaced the FEMA Pre-Disaster Mitigation Program to provide funding to states and localities to strengthen the resilience of critical infrastructure—including technology—for transportation, energy, water supply, communications systems and more.

$500 million for the new Strengthening Mobility and Revolutionizing Transportation (SMART) grant program, which will award competitive funding for smart city technologies including sensor-based architecture, commerce logistics, smart grid technologies, connected vehicles, systems integration, drones and more.



Start by looking back. "Look at what you built over the course of the pandemic," says Congo. "What measures did you put in place to enable work from home or to connect with constituents in new ways? What worked well and what didn't work? Did any of the stopgap solutions you stood up outperform the technology it replaced?" Take stock of those solutions and evaluate your existing equipment and infrastructure to establish a baseline.

Think long term. When considering use cases for IIJA funds, it's important to prioritize solutions that can accommodate future demands. Any new network solutions or applications should be flexible enough to handle your organization's current and future needs surrounding SD-WAN, cloud, mobile and other technologies.

Look for solutions with baked-in cybersecurity tools that support a modern approach to security and resilience—including Zero-Trust and Secure Access Service Edge (SASE) frameworks.[11] Consider how all applications and platforms can accommodate emerging innovations such as artificial intelligence, machine learning and data analytics. "With every single investment you make now," says Congo, "think about how it is going to prepare you for the future."

Lead with people, not technology. As with any new project, public leaders should think of technology not as an end, but as a means for enabling government to support public employees and improve constituent services. IT leaders should work closely with agencies to understand the end goals they want to achieve, and then how technology investments can help reach those goals. Tech officials, including cybersecurity leaders, should be involved in early-stage strategy conversations to ensure IT and security are considered throughout the planning process as crucial components for enabling public policy and service delivery.

Be mindful of one-time funds. State and local governments may be awash in federal funds, but it's crucial to remember these are one-time revenues. Spend them wisely. Consider how you'll sustain the investments you make now. Work diligently to assess the total cost of ownership (TCO) of any new solutions you procure, including maintenance, staffing and upgrade expenses down the road.

Bridging the digital divide isn't just about running broadband to every home, cautions Arkansas CTO Askins. "It's great that we're funding infrastructure," he says. "But there's a sustainability question we have to figure out." Universal broadband is important, but it's also important for government and providers to come together to help ensure affordable access to internet service. "Many rural Arkansans are at or below the poverty line. Can they truly afford to pay for broadband? Government can't be in the business of just giving people money, and then five years later the money has run out and they can't access that service anymore. That just can't be the model going forward."

Work with trusted private partners. As the needs of the network become increasingly complicated, and as it becomes even more crucial to build a scalable, adaptable IT ecosystem, it's more important than ever for public sector organizations to find reliable, strategic, long-term partners. Cloud and SaaS providers will play a critical role in helping governments achieve their goals for connectivity, mobility and security. And the resources and expertise of private partners will be increasingly important for helping governments overcome future budget constraints, staff shortfalls and skills gaps.

> "The public sector should not have any hesitation on inviting the private sector in and holding them accountable."
>
> - Chris Lusey, Public Sector Sales Manager, AT&T

"It's vitally important that the public and private sectors continue to collaborate on connectivity," says AT&T's Lusey. "The public sector should not have any hesitation on inviting the private sector in and holding them accountable for their subject matter expertise and their ability to bring thought leadership, investment and innovation."

For that reason, it's a good idea to bring private partners into strategy discussions early, says Congo.

"At the core of any good relationship is an understanding of mutual goals. It's important that any private sector company understands a government organization's core business and what they're trying to accomplish." Find partners who complement your efforts and involve them early, he says. "Ensure that everyone is aligned on the same goal."

How States Can Achieve the Infrastructure Bill's Broadband Goals

The federal government made states the key decisionmakers in distributing most of the $65 billion included for broadband in the IIJA. Executing the program will require many states to greatly enhance their grant administration efforts and deepen their understanding of telecom issues, including network architecture, broadband technologies, mapping and data analytics.

The Brookings Institution published nine steps every state should take in developing and implementing its broadband plan to achieve the goal of universal broadband access. Below is an excerpt from Brookings' report:[12]

Publicly establish a vision for using broadband to improve residents' lives. As an initial action, state political leaders should publicly establish broad—but clearly measurable and time-defined—goals to guide the broadband expansion process and build support for the effort. The vision should clarify that the goal is to not simply narrow the broadband network access gap, but to close it permanently; to establish long-term approaches for managing the overall digital divide, including improving adoption and utilization for essential services; to generate long-term impacts on economic development and societal health; and to assign responsibilities to specific actors in the state administrative bureaucracy and hold them accountable for explicit results.

Build institutional capacity to achieve the plan's goals. Unlike federal grants for roads, water, sewage and other traditional infrastructure, there are limited state administrative resources and little historic precedent for distributing broadband funds. Building the capacity to do so requires a surge of short-term resources without overcommitting to long-term administrative capacity.

Develop and publish a comprehensive timeline. The National Telecommunications and Information Administration, which will oversee state broadband programs, will have numerous deadlines that states cannot afford to miss. Considering the multifaceted and complicated set of requirements and opportunities, states should create a comprehensive timetable so that all stakeholders are aware of critical deadlines, analysis is completed to provide decisionmakers with the necessary information and applications are completed on a timely basis.

Engage communities and stakeholders in the development of the plan. States should gather input from all relevant stakeholders to enable inclusive and responsive decision-making and achieve optimal political buy-in for the broadband plan. This involves convening multiple interests, including local governments, internet service providers, educational institutions, health care providers and the nonprofit sector, among others.

Improve mapping, data collection and modeling—and bookmark the funding to pay for it. A state will not succeed unless it facilitates intelligent decision-making. This requires each state to collect, analyze and disseminate the relevant information to stakeholders and decisionmakers on a timely basis. This includes data on the end-user structures that require a broadband connection; the type of networks available and performance characteristics; and socio-economic, demographic, adoption and usage data. Such mapping should be able to define geographies as served, unserved or underserved locations.

Develop a comprehensive plan for availability, adoption and utilization. The IIJA requires states to develop plans that detail how they will use broadband to improve performance in sectors that increasingly depend on it, such as health care, education, workforce development, public safety, emergency response and economic development. This means state plans should not only achieve the goal of assuring all residents have access to broadband networks, but also that broadband becomes affordable to all.

Coordinate state and local action to lower the cost of deployment. Once a state has its plan, it should establish processes that reduce construction costs. The idea is similar to the "dig once" concept—coordination in digging up rights of ways and upgrading other infrastructure can significantly reduce construction costs and disruption. Given the many infrastructure projects that could benefit from construction coordination—including roads, water and sewer networks, electric grids and broadband—states should develop plans that incentivize coordination. They should also incentivize permitting processes that accelerate decision-making and reduce costs.

Establish a competitive grant process. Once a state has identified where it wishes to deploy new or upgraded broadband networks, it must establish a competitive process for awarding the funding that rewards enterprises that can deliver the most valuable and cost-effective solutions.

Establish a process to enforce commitments. When states provide funding for private entities to deploy broadband networks, they must do so under contractual provisions that incentivize the winners to fulfill their commitments. States must take steps to oversee, audit and verify that those commitments have been met. This is not a unique problem, but it does raise significant complexities that are likely to be similar in many states.

Conclusion

Key Actions to Take for a More Agile, Flexible Future

The pandemic introduced abrupt changes to the way governments function, many of which will have a permanent impact on how the public sector delivers services to its constituents. As agencies hone their ability to support a decentralized workforce, enhance the digital government experience and strengthen their cybersecurity strategies, they're making crucial investments in the network of the future.

That works begins now. The pandemic put an unprecedented strain on governments. But many agencies used the challenges of COVID to make themselves into more modern, effective organizations.

"The pandemic forced us into some efficiencies, and it forced us to truly think about how we deliver services—both as an IT agency to our customers, who are other state agencies, as well as their customers, the citizens of the state," says Askins, the Arkansas CTO. "We're actually a better, more efficient agency now. We can stand up new solutions and new processes much more quickly."

As governments look to build and sustain the network of the future, there are certain steps that will help ensure their ability to meet demands for years to come:

☐ **Develop a comprehensive strategy.** Establish long-term organizational goals for a more adaptable, scalable and agile network, and then work backwards to determine which aspects of your current system need to be augmented or replaced.

☐ **Leverage federal funds now,** including from the IIJA and other sources, to build network capacity and agility. Optimize investments in new fiber and broadband that will improve connectivity and digital equity.

☐ **Keep your sights on cybersecurity.** To strengthen digital defenses and improve resilience in the face of evolving threats, organizations cannot treat cybersecurity as an afterthought. Look for network solutions with baked-in cybersecurity tools, and include security in every part of your network enhancement strategy.

☐ **Rely on outside expertise.** Look for partners in the private sector with longstanding experience working with governments. In addition to technology and talent, these private organizations can provide invaluable advice and expertise to help agencies navigate their journey to a more modern network.

Most impotantly, as governments have learned, the network of the future isn't a new piece of technology. It's a new paradigm.

"The biggest barrier to building the government of the future," says AT&T's Spencer, "is mindset. It's about seeing this moment not as a challenge, but as a great opportunity for improvement."

Endnotes:

1. https://www.nascio.org/wp-content/uploads/2021/12/NASCIO_CIOTopTenPriorities2022.pdf
2. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/12/13/executive-order-on-transforming-federal-customer-experience-and-service-delivery-to-rebuild-trust-in-government/
3. https://f.hubspotusercontent10.net/hubfs/4896063/BlueVoyant%20-%20State%20and%20Local%20Government%20Report%20-%2026th%20August%202020%20-%20FINAL.pdf
4. https://blog.emsisoft.com/en/37314/the-state-of-ransomware-in-the-us-report-and-statistics-2020/
5. https://www.usaspending.gov/disaster/covid-19?publicLaw=all
6. https://www.ncsl.org/research/fiscal-policy/state-uses-of-the-cares-act-coronavirus-relief-funds-magazine2020.aspx
7. https://www.ncsl.org/Portals/1/Documents/statefed/COVID-Econ_Relief_Bill.pdf
8. https://home.treasury.gov/system/files/136/SLFRF-Compliance-and-Reporting-Guidance.pdf
9. https://www.natlawreview.com/article/treasury-final-rule-significantly-expands-permitted-use-arpa-funds-broadband
10. https://www.whitehouse.gov/wp-content/uploads/2022/01/BUILDING-A-BETTER-AMERICA_FINAL.pdf
11. https://blogs.gartner.com/andrew-lerner/2019/12/23/say-hello-sase-secure-access-service-edge/
12. https://www.brookings.edu/2022/01/21/steps-the-states-should-take-to-achieve-the-infrastructure-bills-broadband-goals/