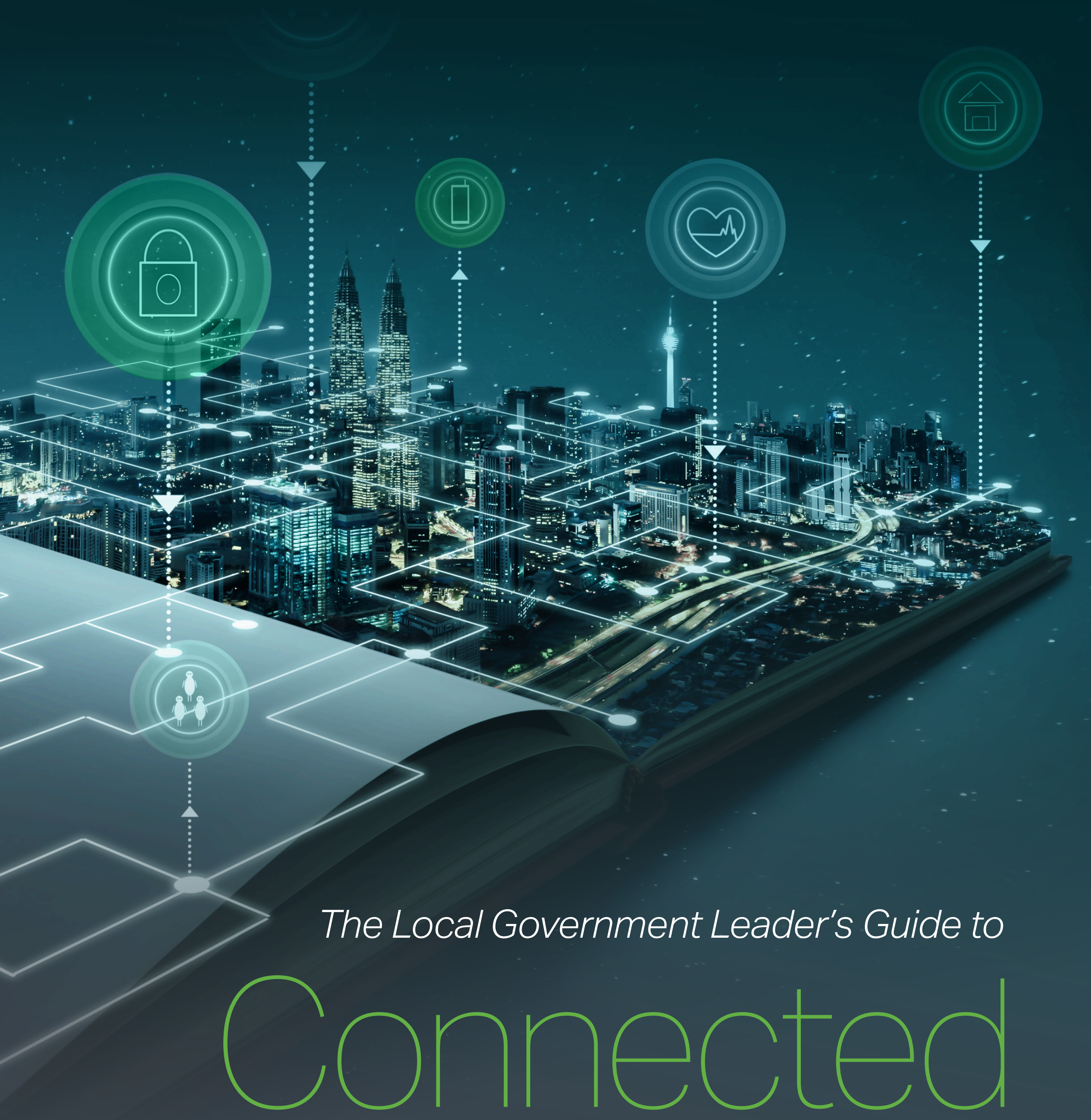
A GOVERNMENT TECHNOLOGY HANDBOOK FOR Cisco Meraki



The Local Government Leader's Guide to

Connected Communities

Table of Contents

03 Introduction

04 Connected Communities: A Status Report

06 Managing the Internet of Things (IoT)

09 Bridging the Digital Divide

12 Preparing for the Future of Work

15 Securing It All

18 Conclusion

Introduction

Longstanding shifts in work and education that accelerated dramatically during the pandemic have changed how communities think about connectivity. One of the most profound changes for government leaders involves the notion of edgeless government — where constituent services mesh seamlessly into a world of decentralized work, hybrid learning and digital interactions in the other areas of residents' lives.

Governments have much work to do to meet these evolving expectations. A Center for Digital Government (CDG) survey shows that 42% of respondents don't have a roadmap for the connected communities their constituents increasingly expect. Too many governments, says CDG Senior Fellow Bob Bennett, "are living in a 21st-century whirlwind and still dealing with 20th-century procedures."

As governments look to rapidly address these unmet needs within their operations and their broader communities, they must leverage and apply the right approaches, tactics and partners. Drawing from a survey of government leaders and expert interviews, this handbook examines how governments can manage expectations in hyper-connected environments, bridge the digital divide, prepare for the future of work, and ensure these growing community connections remain safe and secure.

"We're at a key inflection point where we can accelerate and advance the depth and power of that connectivity in ways that we couldn't five or 10 years ago," says CDG Senior Fellow Christopher Cabaldon, the former mayor of West Sacramento, California.

Starting with Data

To understand state and local government initiatives focused on developing connected communities, CDG conducted a national survey of state and local government leaders in September 2021, collecting 150 responses. Most respondents represent municipal (37%), state (25%) and county (22%) governments, spanning a range of roles, including administration, public works, IT, elected governance, finance, health and human services, economic development, public safety, education and more. Sixty-one percent of respondents are in senior leadership roles.

Connected Communities: A Status Report

Connected communities represent the evolution of more discrete smart city and connectivity projects that began more than a decade ago. In Kansas City, Missouri, for example, large-scale efforts launched in 2016 with construction on a streetcar line. The project provided opportunities to add smart sensors to improve traffic circulation and public Wi-Fi access points across more than 50 blocks of the city's downtown.

Communities became more connected during the pandemic out of necessity, with governments shifting service delivery online as their employees and constituents began learning, working and socializing in digital settings. Now, the focus has shifted toward more coordinated approaches to build on these efforts in sustainable ways to meet evolving constituent and employee expectations about digital services and hybrid work.

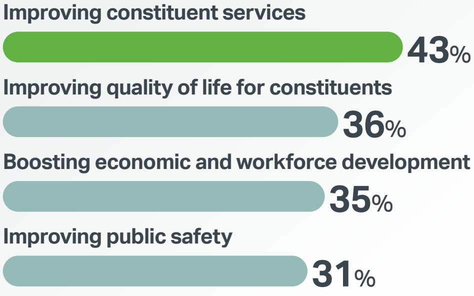
"We're getting out of a reactive mode and trying to get into a proactive one," says Collin Averill, solutions marketing manager for Cisco Meraki.

That more proactive approach focuses on combining smart city technology with intelligent networking capabilities to weave together employees, services, community assets, constituents and information. In this model, the underlying network plays an essential role as the platform connecting these disparate functions and constituencies — and puts government at the center of connected community efforts.

"There are important and critical resources for communities that governments can drive to improve quality of life," says Averill. "The government has the ability to roll out infrastructure in ways that are tough to do otherwise."

Governments are approaching connected community projects with residents in mind. More than half (60%) of CDG survey respondents said their top drivers involve improving constituent services or quality

What are the top drivers for connected communities in your jurisdiction? *(Select up to 3 choices)*



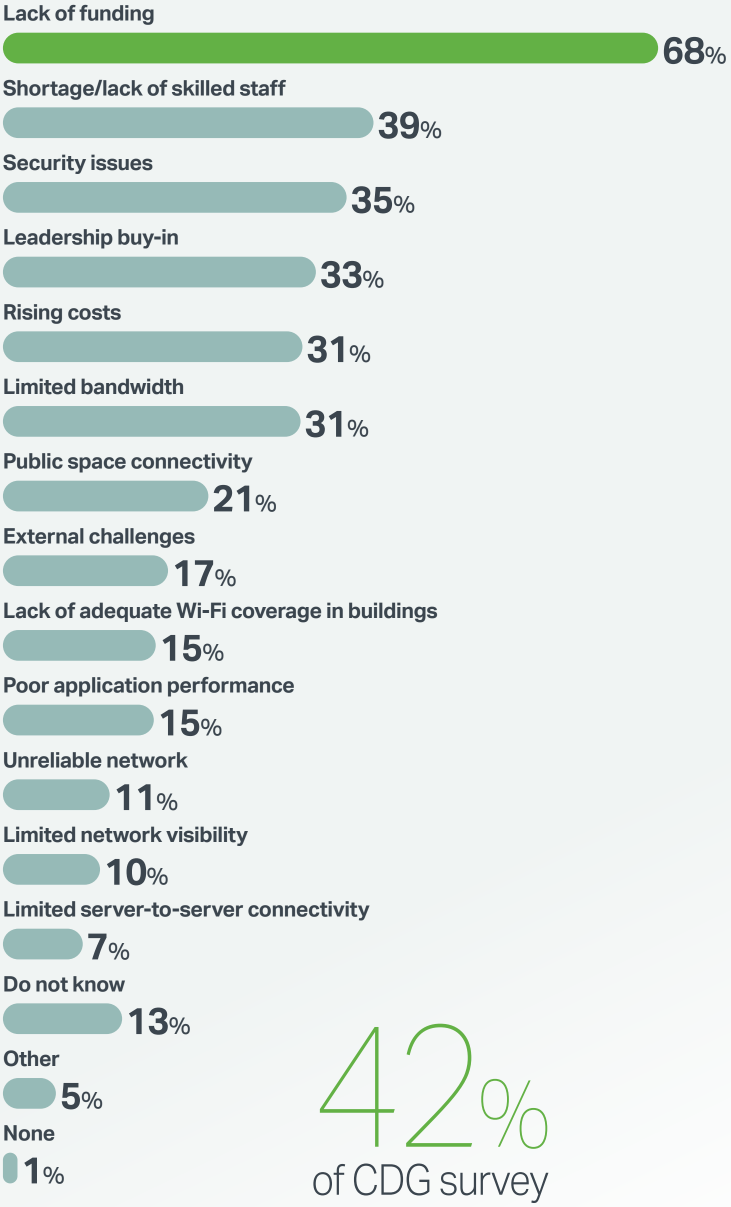
of life, followed by boosting economic and workforce development and improving public safety.

However, many barriers remain. Funding was the top challenge cited by more than two-thirds (68%) of CDG survey respondents, followed by staffing and security issues, leadership buy-in, rising costs and limited bandwidth. Even addressing the security concerns involved with connected communities is perceived through the lens of funding constraints, which was the top security challenge cited.

Smaller but significant percentages of respondents also recognize the limitations of their existing infrastructure, citing additional networking issues, including public space connectivity, lack of adequate Wi-Fi coverage in buildings, and unreliable networks and limited visibility as barriers to connected community initiatives.

But perhaps the biggest obstacle is the lack of a broader vision, with 42% of survey respondents saying their governments lack a plan, roadmap or strategy for connected communities. The remainder of this handbook outlines strategies in four critical areas that together will drive governments' connected community efforts: managing the Internet of Things (IoT), addressing the digital divide, enabling hybrid work environments in and beyond government, and ensuring connected communities remain safe and secure.

What challenges, if any, do you anticipate while trying to achieve plans for connected communities? *(Select all that apply)*



42%

of CDG survey respondents said their government lacks a plan, roadmap or strategy for connected communities.

Managing the Internet of Things (IoT)

As with other connected community initiatives, governments had begun implementing the connected and automated devices that compose the IoT well before the pandemic to collect data, inform and improve decision-making, and automatically control remote systems. However, financial realities often limited efforts to smaller pilots.

"We could not do things at a scale that was capable of delivering impact and outcomes that could be viable," Cabaldon says.

The pandemic provided new impetus to monitor and control systems remotely. At the same time, the influx of federal stimulus funding has given governments the opportunity to scale up infrastructure-related IoT systems, including ones connected with municipal utilities like water.

More than one-third of CDG survey respondents (35%) have begun using IoT devices, with most (20%) integrating them into other systems and applications. Smart cameras and sensors for security and cameras for law enforcement represent the top current use cases, followed by location sensors, environmental sensors, and smart streetlights and traffic sensors.

The number of use cases involving security and public safety illustrate a key challenge around large-scale IoT deployments. The bandwidth needed to stream video and leverage artificial intelligence and machine learning (AI/ML) to trigger security alerts and monitor traffic is taxing existing networks. It's not surprising that one-third (33%) of CDG survey respondents said their jurisdictions are already

> Before, governments were making decisions based on limited data. Now, it's almost the opposite problem — over the course of a year, you could be looking at tens of thousands of data points."
>
> *Anthony Hizon, Product Manager, Cisco Meraki*

experiencing network constraints that hinder their ability to use IoT devices.

"The architecture behind CCTV hasn't changed since analog cameras," says Clint Russell, Cisco Meraki product sales specialist. "Now technology is being forced upon the network, which can be a massive burden."

Among the strategies for deploying IoT at scale for connected community efforts:

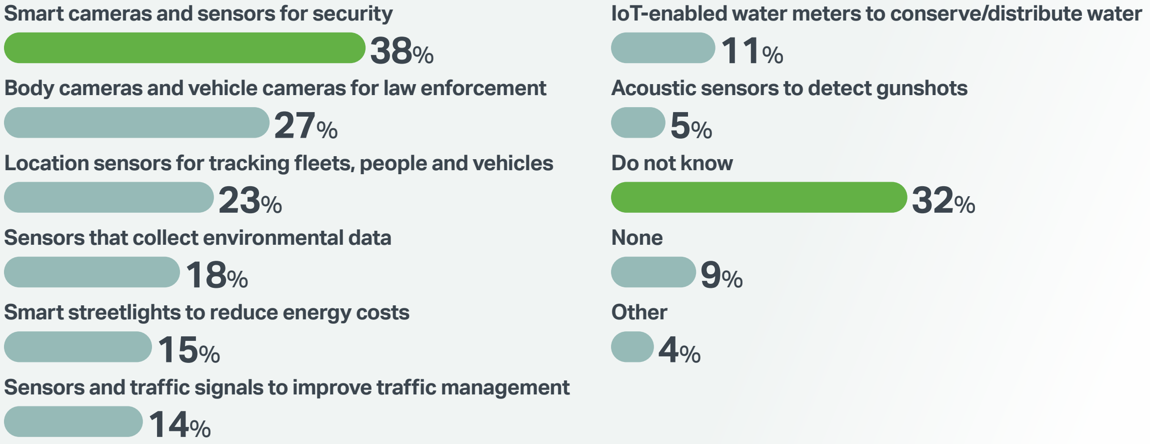
✓ **Identify specific needs.** Let use cases drive the selection of IoT devices, not the other way around. Governments "need to focus on the problems they're trying to solve, which should reveal what data they need to solve the problem, which in turn gives them the device," says Bennett, who formerly served as Kansas City's chief innovation officer. "Then you have a network that grows organically and residents see as a worthwhile investment."

✓ **Address bandwidth needs.** Networks need the capacity to support large numbers of connected devices and the data they generate. Along with increasing bandwidth, emerging technologies such as Wi-Fi 6 are optimized for large numbers of IoT devices and the recent rollout of Wi-Fi 6e adds an additional wireless spectrum.

✓ **Simplify device management.** As connected devices grow exponentially into the thousands in many localities, it will be critical to have centralized platforms that automate onboarding, managing and collecting information from multiple devices, particularly given most governments' constrained IT resources.

✓ **Focus on how you can use data.** The constant stream of data from connected devices can be a double-edged sword. "Before, governments were making decisions based on limited data. Now, it's almost the opposite problem — over the course of a year, you could be looking at tens of thousands of

What are your organization's uses for IoT devices within your jurisdiction?



data points," says Anthony Hizon, Cisco Meraki product manager. "It can be overwhelming." Governments can benefit from systems that aggregate, analyze and generate visualizations that help leaders make actionable decisions. These kinds of capabilities will be critical for governments to leverage IoT for more sophisticated use cases, such as monitoring the usage of public facilities and optimizing transit routes and schedules.

✓ **Consider security implications.** The addition of thousands of devices represents a massive influx of endpoints for IT managers to oversee. The early history of IoT deployment was rife with examples of devices left with default passwords and similar security gaps. Today, more sophisticated capabilities allow agencies to onboard new smart hardware in a way that establishes them as trusted devices. It's also important to ensure that data — even seemingly harmless information — between devices and central servers is encrypted. "Even though it may not seem that sensitive, that infrastructure will be leveraged for more sensitive data," says Hizon.

✓ **Consider redundancies and remote locations.** Given the mission-critical nature of the systems that connected sensors monitor, it's important to consider cellular failovers and other technologies to ensure systems aren't disrupted. Emerging 5G networking and other technologies can also help governments deploy devices in far-flung locations such as parks or remote utility stations.

✓ **Leverage IoT to monitor the heart of the connected community — the network itself.** Sensors that monitor critical networking infrastructure, such as routers and access points, and identify environmental threats or physical tampering, can become a critical part of network operations. "These are the plumbing of your digital organization. A single hour of downtime could be catastrophic," Hizon says. The sheer number of connected devices and the data generated by IoT deployments present a challenge for government organizations with limited IT resources. Having a platform with the capabilities to manage devices, analyze data and strengthen end-to-end security will be critical to ensure they can effectively enact IoT strategies.

In Opelika, a Sensor-Driven Smart City Emerges

Located in a fast-growing region of Alabama, the city of Opelika embarked on its connected community mission with three priorities. Along with deploying public Wi-Fi in municipal buildings and parks, the city plans to roll out more than 1,000 connected environmental sensors and smart streetlights.

The city is partnering with Auburn University to deploy sensors to monitor parking, industrial park emissions and water quality, with the university helping leaders identify the right data to inform decision-making. Opelika is also installing smart streetlights that are expected to reduce energy costs by 50% by dimming lights during periods of low activity.

Like many municipalities, large parts of the 55 square miles within Opelika's boundaries are forested and rural, and the city is the first in North America to deploy a LoRaWAN-compliant solution, which provides long-distance wireless connectivity to IoT endpoints with low power consumption.[1]

Bridging the Digital Divide

As millions of people began working and learning from home during the pandemic, the availability of high-speed internet access became a necessity, not a luxury. Yet the level of at-home access to broadband internet barely budged during the pandemic. Nearly 60% of students in low-income households and 43% of adults still lack at-home broadband internet access,[2] providing an imperative for governments focused on connected community initiatives.

"Providing a base level of connectivity where people can apply for work, engage with the city and do homework — that's the bare minimum," Bennett says.

Ongoing disparities in broadband access represent "a market failure," says Mitchell Gorsen, Cisco public funding advisor. In urban areas, the primary barrier is affordability, while in more rural ones — both rural regions and less populated areas of large counties or municipalities — access to high-speed broadband may not be available at any cost.

State and local governments have long played a critical role in access to public infrastructure and utilities, and one-third (34%) of CDG survey respondents said their jurisdictions are currently working to address the digital divide, bolstered by unprecedented federal funding to address broadband gaps. "The last mile is now maybe the last half-mile," Cabaldon says. The pandemic, he adds, "pushed our own internal questioning."

Among the strategies for addressing the digital divide:

✓ **Focus on the big picture.** While broadband availability is the most visible constraint to universal access, affordability and adoption are also critical barriers. "Governments need to focus on all three," says Chris Gugger, solutions marketing manager at Cisco Meraki.

✓ **Consider whether to go it alone or find partners.** Some jurisdictions — as many as 1,000, by one estimate — have become internet providers, as Fort Collins, Colorado, has done with its Connexion municipal broadband utility, or by entering public-private partnerships, leasing existing fiber rings or offering RFPs to multiple providers to develop new connectivity.

Over the past three decades, these efforts have yielded "a wide spectrum of successes and bankruptcies," says Gorsen. "The business model is viable, and there are examples of success, although governments must be cognizant of the potential for failure, particularly around technology refresh and being able to keep up with commercial providers."

✓ **Coordinate at all levels of government — and beyond it.** States and large municipalities must develop broadband plans to access federal funds, and all governments will benefit in the grant process from regional or statewide coordination and consortia. “Grant reviewers look favorably upon these kinds of collective, well-thought-out networks that have lots of anchor tenants,” says Gorsen. “It’s the single-use networks that are harder to justify.”

> “Providing a base level of connectivity where people can apply for work, engage with the city and do homework — that’s the bare minimum.”
>
> *Bob Bennett, Senior Fellow, Center for Digital Government*

✓ **Leverage ‘middle mile’ infrastructure.** Governments that have been successful in providing access on their own have focused on using existing rights-of-way or utility infrastructure to connect key institutions, such as colleges and universities, public schools and hospitals. “Look at physical systems not just as something that

In Miami-Dade, Connected Communities Start with Libraries

The Miami-Dade Public Library System found itself an essential part of the South Florida region’s internet connectivity during the pandemic, standing up 200 public Wi-Fi access points to allow people to connect to the internet from both inside and outside its 49 locations.

“The pandemic drove us in a direction that we were already thinking of going, but really sped us up,” says Ray Baker, director of the library system. “People shouldn’t be marginalized by access to technology or bandwidth. That’s been central to everything we’ve been doing around the digital divide.”

As part of a refresh of the library’s network, which added more than 1,000 smart cameras and 200 public Wi-Fi access points, the system now offers one of the fastest Wi-Fi connections in South Florida, says IT Manager Julio Campa. Along with improving security, the smart camera technology provided new insights into traffic flow, facilities usage, and where floor plans helped or hindered patrons. “It’s our mission to interpret what happens when people visit the library,” Campa says.

Smart cameras also facilitate the sharing of information to other departments that help maintain facilities, and a unified dashboard allows two staff members to manage the system.

The library system has since acquired more than 600 internet-enabled devices that residents can check out and use at home and is preparing to deploy more than 2,000 Chromebooks. “It’s changed our role to making sure people can get connected to the internet, whether the library’s open or closed,” Baker says.[3]

has to be maintained, but as an asset that you can use to provide additional internet coverage or a point for IoT devices that can help you better manage other city services," Bennett says.

"There are a lot of things you can do when you change your mindset about these assets."

✓ **Consider new options for rural or last-mile access.** The challenge of providing universal access is that the "last 1% to 2% becomes infinitely more challenging," Russell says. However, 5G and technologies such as microwave radio and fluid mesh networking are providing new options that allow some remote areas to be reassessed on a case-by-case basis.

"Five years ago, to have reliable connectivity, it had to be fiber." Averill says. "With the increased affordability of cellular, pairing the two can be a really great solution."

✓ **Address staff capacity issues.** Municipal networks with open Wi-Fi access points typically also support other government functions, including employee access and IoT sensors, challenging small IT staffs to manage multiple functions and constituencies. "Those are big hurdles they have to overcome," Averill says. "Having a platform that lets you set policies across the network at every location and customize as needed helps with the limited IT resources of staffing, budget and time."

✓ **Recognize funding sources and limitations.** Broadband expansion is the top-cited use planned for federal stimulus funding among CDG survey respondents. It's vital for governments to understand and navigate the requirements and potential exceptions involved with federal grants and other programs, according to Gorsen.

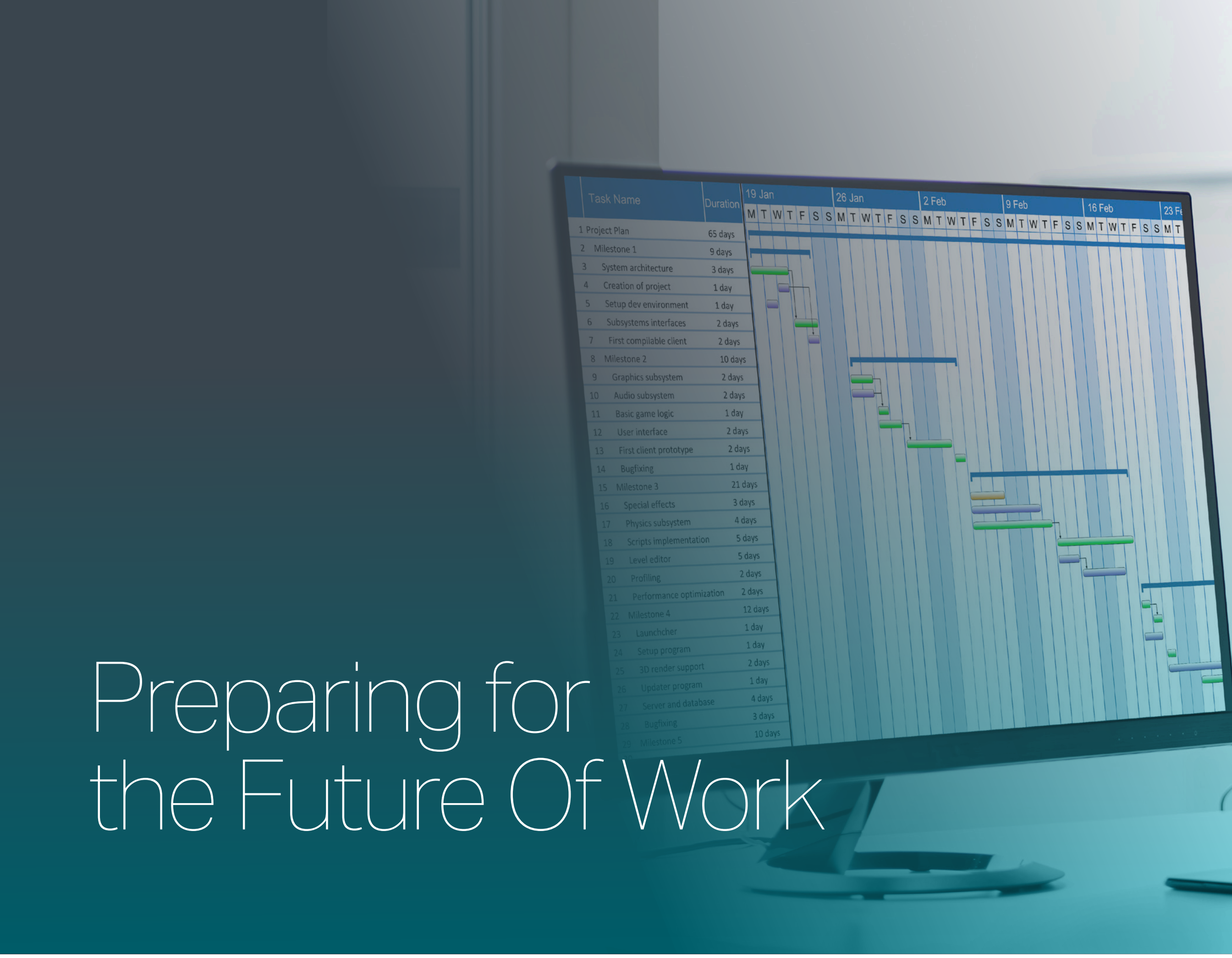
✓ **Focus on supporting adoption among underserved communities.** The federal infrastructure bill includes funding for outreach to encourage people who lack internet access to sign up for broadband. That's critical if governments intend to fully address the digital divide, says CDG Chief Innovation Officer Dustin Haisler.

In Kansas City, community groups took the lead to ensure digital inclusion in connected city efforts. "It's okay for the city to stand back and take a supporting role," Bennett says.

In El Paso, a Digital Initiative Extends to Schools

Located near the Mexico-United States border, the Canutillo Independent School District in El Paso, Texas, serves more than 6,000 students, many of whom lack internet access at home. When the pandemic closed school buildings, the district launched Canutillo Connect, a secure, private wireless network to provide students with free internet access for remote learning.

The network leveraged the district's existing fiber network and public utility poles to create a Wi-Fi backhaul network. Fluid mesh radios and access points were then deployed to create Wi-Fi access networks in nine of the district's most impacted neighborhoods. Now, the district and the broader community — which first launched the Digital El Paso community wireless project in 2007 to address digital divide and economic development issues — are working together to address broadband access issues across the entire county. The community plans to use Canutillo Connect as a proven model it can replicate as it seeks grant funding from multiple sources.[4]


Task Name
Duration
19 Jan
26 Jan
2 Feb
9 Feb
16 Feb
1 Project Plan 65 days
2 Milestone 1 9 days
3 System architecture 3 days
4 Creation of project 1 day
5 Setup dev environment 1 day
6 Subsystems interfaces 2 days
7 First compilable client 2 days
8 Milestone 2 10 days
9 Graphics subsystem 2 days
10 Audio subsystem 2 days
11 Basic game logic 1 day
12 User interface 2 days
13 First client prototype 2 days
14 Bugfixing 1 day
15 Milestone 3 21 days
16 Special effects 3 days
17 Physics subsystem 4 days
18 Scripts implementation 5 days
19 Level editor 5 days
20 Profiling 2 days
21 Performance optimization 2 days
22 Milestone 4 12 days
23 Launchcher 1 day
24 Setup program 1 day
25 3D render support 2 days
26 Updater program 1 day
27 Server and database 4 days
28 Bugfixing 3 days
29 Milestone 5 10 days

Preparing for the Future Of Work

For many governments, the transition to remote work in March 2020 happened literally overnight, as IT departments cobbled together solutions that successfully allowed service continuity in the face of stay-at-home orders. Now, the task for governments is to build on those early efforts in more sustainable ways.

"We survived," Russell says. "Now we have to adapt."

One thing that's clear is that hybrid work is here to stay — both in and beyond government. Half of CDG survey respondents said their organizations remain in hybrid work environments, and nearly as many (46%) say they anticipate hybrid work continuing over the next 12 to 18 months.

Government leaders will have to address ongoing challenges to ensure these hybrid efforts remain effective. Network connectivity and issues with effective communication and collaboration are the top challenges with hybrid work cited by CDG survey respondents, followed by lack of adequate equipment, security requirements, and outdated hardware and software.

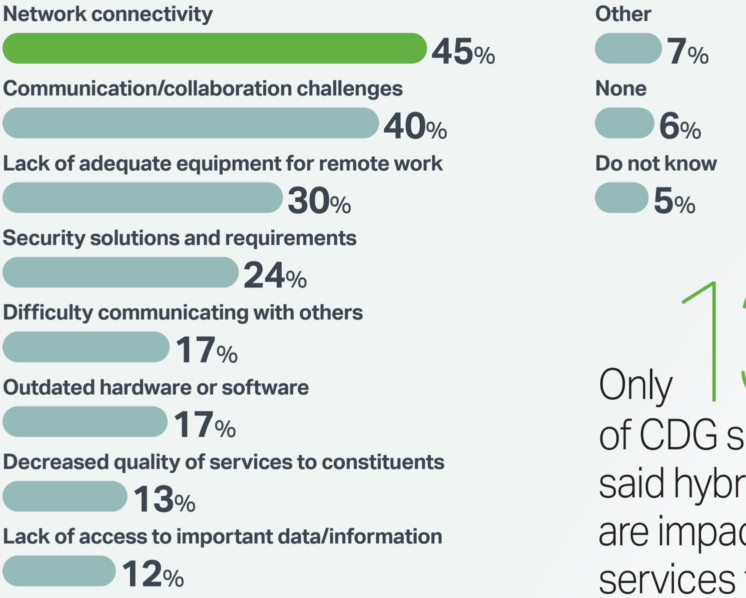
Notably, only 13% of respondents said hybrid environments are impacting the quality of services to residents. And the ability to hire employees beyond a jurisdiction's boundaries for many roles holds potential for governments to improve their own recruiting for hard-to-staff positions.

"It's very evident that employees prefer to have flexibility around when and where they do work," Haisler says. "The underlying infrastructure that supports this is key to making that stick."

Among the strategies for building a sustainable infrastructure for hybrid work:

✓ **Focus on simplicity.** Agencies must find better approaches to enable remote access for employees, including user-friendly ways to onboard and manage devices, access virtual private networks (VPN)

What are the top challenges in instituting or planning to institute a hybrid workplace? *(Select all that apply)*



Only 13%
of CDG survey respondents said hybrid work environments are impacting the quality of services to residents.

and authenticate securely. "If something's not easy, people aren't going to do it," Averill says. "That's really going to drive how organizations of any kind are going to advance their hybrid work solutions."

Catalog and identify gaps. IT organizations should catalog the tools they used for remote work and collaboration across departments during the pandemic, determine what's worth keeping, what they can discard, and identify opportunities to consolidate solutions when possible. They should also identify gaps and strategically partner with solution providers, according to Russell. In doing so, however, it's important to recognize that different government agencies and functions will likely require different tools to work effectively.

"It's going to be a conglomeration of multiple technologies," Russell says. "As much as we'd love to have an end-to-end solution, at the end of the day people use lots of different tools, and the needs are going to be different across different departments."

Build atop a unified platform. While there likely won't be a one-size-fits-all approach to hybrid work applications, governments still need to avoid a fragmented IT environment — a "Frankenstein's monster" of piecemeal point solutions, Averill says. The key is to build on a common platform that can weave together multiple cloud-based applications into a common system.

Don't neglect in-office needs. The future of hybrid work increasingly involves employees spending at least some time in office settings. Connected IoT solutions can help manage hybrid workplaces. Beyond immediate public health needs such as monitoring capacity limits, networking hardware can manage a wide range of office conditions — foot traffic and wayfinding, access, temperature, noise levels, occupancy and air quality among them — to help in-office employees, welcome guests, secure critical areas, plan meetings and collaborate effectively.

> "If something's not easy, people aren't going to do it. That's really going to drive how organizations of any kind are going to advance their hybrid work solutions."
>
> *Collin Averill, Solutions Marketing Manager, Cisco Meraki*

Think beyond government employees. More than one-third (35%) of CDG survey respondents see economic and workforce development as one of the top drivers for connected community projects. Ensuring the entire community has the bandwidth to enable hybrid work is a critical component of these efforts. "Part of our role is to make it possible for our citizens to have these options as well," Cabaldon says.

Bennett notes that Amazon selected Northern Virginia for its HQ2 project in large part because of the technology skillset of the region's workforce and its investments in broadband and education. "The pandemic illustrated for a lot of people that what the cities talked about in their Amazon bids were critical enhancements they made for people to go to school or work," he says.

For both governments and private companies, the end goal is the same — what Russell calls an "omnichannel environment" in which workers have the capabilities to do their jobs in the office and at home. That, in turn, can help governments meet their primary goal for creating connected communities — providing better services for constituents, who now have gotten a taste of governments providing digital services on par with their commercial counterparts.

"If a citizen needs to pay utility bills or talk to customer service, that experience needs to be the same whether the employee is in the office or at home," says Chris Allen, Cisco Meraki audience marketing manager.

Securing It All

Securing connected community initiatives is an extension of the ongoing evolution of government IT — from legacy mainframes secured in a data center to a growing array of cloud-based applications and storage providers, as the edge extends to encompass IoT sensors and those devices used by hybrid employees. But the scope of the challenge has continued to grow.

"It's an area where we need a lot of help at the municipal level and industry partners to help us think through how to approach this not just from a tech perspective, but how to evaluate that at the leadership level," Cabaldon says. "The frameworks and tools available at the policymaker level just aren't there yet."

Only 8% of CDG survey respondents reported no security challenges with their connected community initiatives. Along with funding issues, respondents said ensuring network security when employees use their own devices, training, finding staff with cybersecurity skillsets, securing remote cloud-based applications and access, and managing endpoints are key challenges.

At the same time as the threat surface has expanded through the deployment of IoT and hybrid work environments, record numbers of ransomware attacks have targeted governments, utilities, education institutions and other public entities. More than 2,300 local governments, schools and healthcare organizations across the country faced ransomware attacks in 2021, according to one report, with efforts shifting to smaller counties and towns. Local governments alone suffered an estimated $623.7 million in losses.[5]

The growing scope of governments' IT environments and the threats against them necessitate a broader shift in thinking about cybersecurity, according to Haisler. "People still think things are securable — that's not a reality," he says. "It's about how to manage the impact and protect personal information."

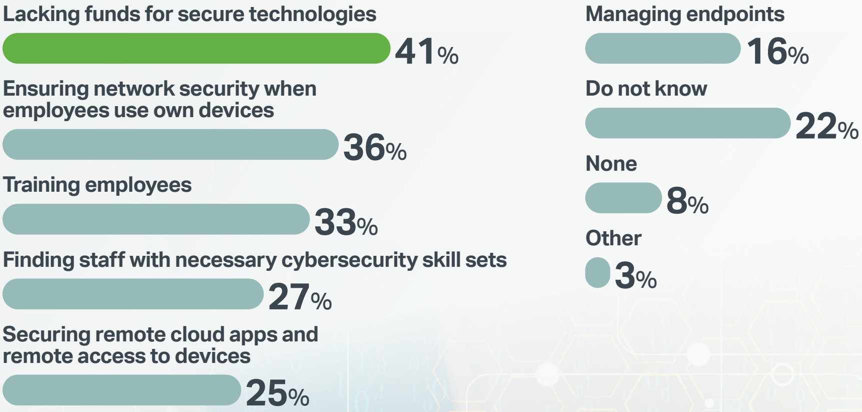
Among the strategies for ensuring that connected community initiatives remain secure:

✓ **Focus on a continuous approach to risk mitigation.** Governments can look to their utilities for a conceptual framework. "You know accidents will happen with the utility infrastructure, but they have programs in place to mitigate the risk," Haisler says. Technology platforms can help translate this framework into practice by enabling IT staff to continuously monitor for threats across the network and its endpoints to speed response and recovery.

✓ **Bring together internal stakeholders.** Even within an IT department, different functional roles — security, connectivity, cloud and operations — all have critical roles to play in securing systems and data. "One of the biggest hurdles to overcome is getting consensus on where to start," Gugger says. "They all need to have a place at the table."

✓ **Identify the most critical needs and the appropriate solutions.** Depending on where a government is in its connected community journey, its leaders may choose to focus first on securing existing infrastructure or expanding

What security challenges, if any, has your organization experienced related to connected community initiatives?



> “People still think things are securable — that’s not a reality. It’s about how to manage the impact and protect personal information.”
>
> *Dustin Haisler, Chief Innovation Officer, Center for Digital Government*

connectivity in secure ways. That decision guides what solutions will have the greatest impact. Secure web gateways and Zero-Trust access systems can provide secure access to existing infrastructure for remote employees, while new software-defined wide area networks (SD-WANs) can help expand connectivity securely, according to Gugger.

Ultimately, cloud-based technologies can unify both security and connectivity. Secure Access Service Edge (SASE) represents a consolidated, cloud-based networking architecture that combines both domains into a single solution. “By combining these, it really allows users to connect in a secure way anywhere from any device,” Averill says. “It democratizes our ability to deploy securely everywhere.”

Cloud-based security will also shift how governments approach cybersecurity investment, according to Haisler. “They won’t be able to treat it as an appliance versus a continuous investment in risk mitigation,” he says.

Ensure solutions meet privacy standards and requirements. Connected government services and workforces must ensure they secure certain types of data, including personal information such as health records, payment data and other sensitive information in ways consistent with federal guidelines such as HIPAA, FEDRAMP and its emerging state counterparts, and other privacy standards. It’s also vital to make certain that constituent privacy is a key design component of connected community initiatives. In Kansas City, for example, privacy considerations involved in the city’s IoT deployment — which included license plate readers — were developed and communicated months before launch. In similar fashion, the Miami-Dade Public Library System has focused on ensuring that its public Wi-Fi deployments safeguard user privacy. “Privacy on a public library network needs to be protected in the same way as protecting a patron’s reading history,” says Ray Baker, the library system’s director.

Focus on training — and simplicity. Most governments have established plans to train employees and periodically test their resistance to phishing attempts, which should continue. However, the simplicity of mobile device management solutions and other procedures can help train users to access hybrid work environments. “The consolidation and convergence of networking and security across every connection allows you to take responsibility off the end user,” Allen says. “You can go to employees and say we’re simplifying security so you don’t have to remember if you have the right password … and they can think more about how they are providing service to citizens.”

Recognize that securing communities remains a community-wide effort. The impact of cyberthreats is community-wide, and some governments are taking steps to educate residents about cyber hygiene and help protect their personal devices. New York City, for example, created its own free smartphone app to alert residents when they’re accessing insecure networks or using unsafe applications, all while assuring them the NYC Secure app collects no private information about its users. “The ability to forget you and your ability to be forgotten is as critical as the ability to protect devices,” Bennett says.

Conclusion: Seizing The Opportunity

Efforts to build and strengthen connected communities are accelerating. For many government leaders, the COVID-19 pandemic served as "the stroke of lightning that opened up these opportunities," Cabaldon says,

If the pandemic was the stroke of lightning sparking connected community initiatives, federal stimulus and infrastructure funding represent what Cabaldon calls a flood of potential to make them a reality. "City halls are drowning in funding opportunities at the moment," he adds.

Broadband expansion remains the top planned use for federal stimulus funding across all types of jurisdictions, according to CDG survey respondents. Network modernization, cybersecurity upgrades and remote work solutions were also highly ranked, and state governments in particular plan to use stimulus funding to accelerate the development of constituent-facing applications.

To determine where to start, IT leaders should consider the policy goals and outcomes that have been identified by elected officials and budget directors — and then think about how technology can be used to help achieve those goals. "Your digital strategy needs to match those priorities, and if it doesn't, then maybe you need to look at what those priorities are," Bennett says.

Given the narrow timelines for applying for funding, it's important to move quickly, according to Cabaldon. "One of the key lessons has been to figure out the baseline strategy and potential points of connection and unleash the technology and programmatic folks to try and make it fit

How is your organization utilizing or planning to utilize federal stimulus funding for technology?

1. **Expanding broadband**
2. **Modernizing networks**
3. **Upgrading cybersecurity**

instead of developing a master plan that covers everything," he says. Those silo-breaking connections are critical: "Connect your IT and tech folks to those other teams from public works looking into infrastructure funding to make sure you're seeing IT opportunities across this band of funding, not just those principally for IT itself," he adds.

It's also important to develop the internal capacity to forge strong private-public partnerships. "Knowing how to broker opportunities is so critical," Cabaldon says. "It's much more incumbent on IT offices to get signals from the private sector on the opportunities out there and how to navigate them."

Together, these efforts can help governments meet an enduring part of their mission. "In some ways, this is the most fundamental role government plays," Cabaldon says. "It's that connectivity that creates meaning and belonging, and the kinds of collisions that are necessary for entrepreneurship, innovation, commerce and community building."

Connectivity is also essential for governments to address the challenges outlined in this handbook — managing the growing number of connected devices that inform and support services, addressing the digital divide issues that impact constituents' lives, ensuring effective work environments in and beyond government, and assuring residents that their personal information and the systems they rely on remain secure. Meeting these needs through the effective deployment of technology can ensure that governments will remain at the center of connected communities for years to come.

Endnotes

1. https://meraki.cisco.com/wp-content/uploads/2020/09/city_of_opelika_cs.pdf
2. https://www.pewresearch.org/fact-tank/2020/09/10/59-of-u-s-parents-with-lower-incomes-say-their-child-may-face-digital-obstacles-in-schoolwork/, https://www.pewresearch.org/fact-tank/2021/06/22/digital-divide-persists-even-as-americans-with-lower-incomes-make-gains-in-tech-adoption/
3. https://meraki.cisco.com/customers/miami-dade-public-library-system/
4. https://blogs.cisco.com/internet-of-things/welcome-to-the-iot-industry-roundtable-on-closing-the-digital-divide-in-education
5. https://www.zdnet.com/article/2300-local-governments-schools-healthcare-providers-impacted-by-ransomware-in-2021/

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:

cisco Meraki

At Cisco Meraki, we create intuitive technologies to optimize IT experiences, secure locations, and seamlessly connect people, places, and things. Our cloud-based platform brings together data-powered products including, wireless, switching, security and SD-WAN, smart cameras, and sensors, open APIs and a broad partner ecosystem, and cloud-first operations. We hope to connect passionate people to their mission by simplifying the digital workplace — making IT easier, faster, and smarter for our government customers.
Learn more at www.meraki.com/government

IMAGES PROVIDED BY SHUTTERSTOCK.COM