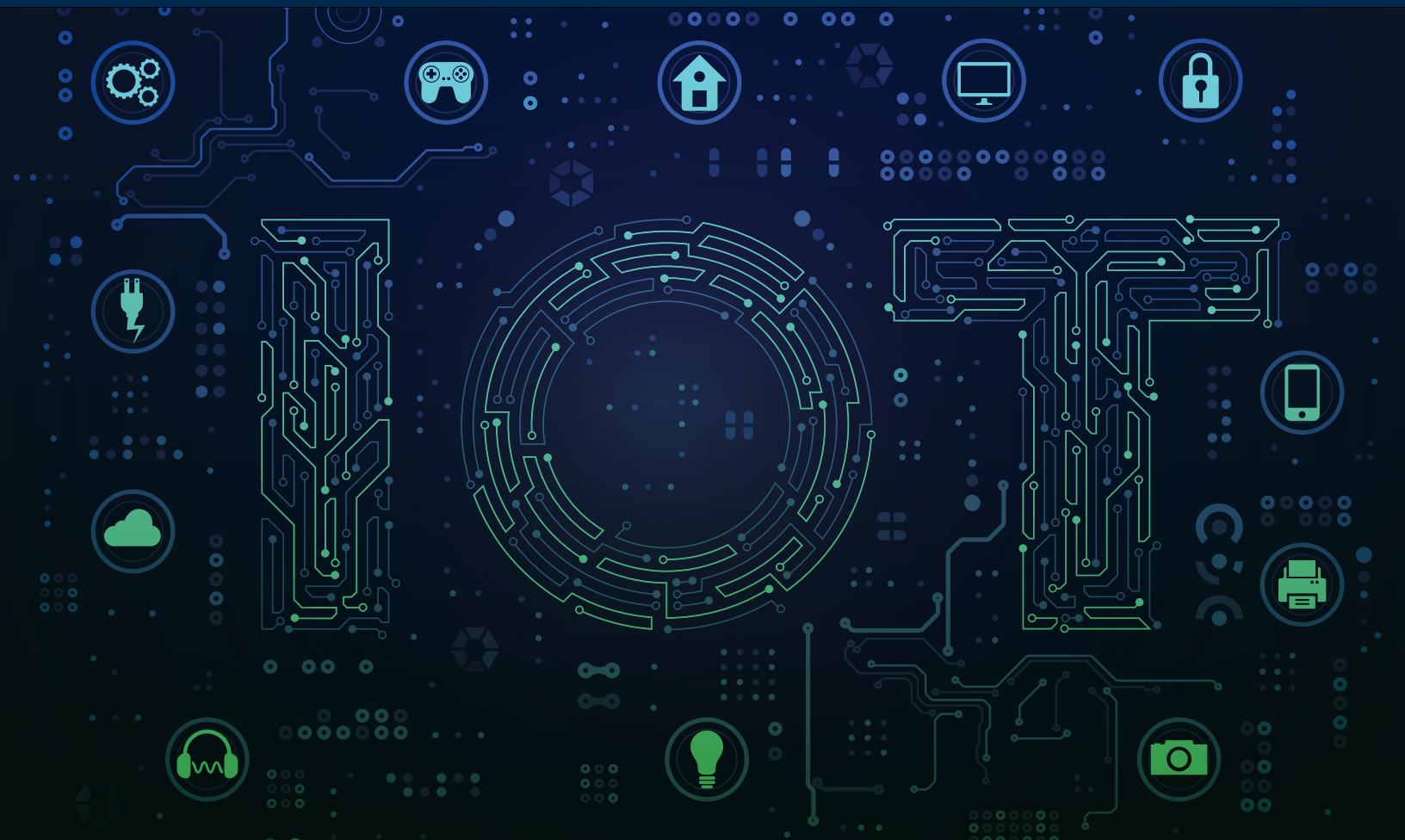
THE INTERNET OF THINGS: AN ADOPTION GUIDE FOR COMMUNITIES

IoT will change how state and local governments handle operations, serve citizens and think about the future.



State and local government leaders clearly see the Internet of Things (IoT) as an opportunity. Almost half of government officials responding to a Center for Digital Government (CDG) survey say they are planning for or deploying IoT technologies. These findings are in step with worldwide activity around IoT-driven digital transformation. The number of IoT devices deployed globally is expected to hit 10 billion this year and then nearly double to 22 billion by 2025.[1]

But what does IoT adoption really look like for communities standing on the brink of this evolution? The CDG survey of 126 local government professionals — one in a series of "Intelligently Connected" surveys conducted in collaboration with Spectrum Enterprise — seeks to understand the current state of IoT adoption in state and local governments and its role in digital transformation.[2] This guide addresses trends and challenges identified by the survey and suggests a path forward for organizations entering the IoT universe. Using this guide, organizations will be better equipped to develop and implement realistic solutions that solve the pressing needs of today while creating lasting value for the future.

The State of IoT Adoption Today

The IoT is a network of sensors and other devices that communicate and interact with the environment to perform tasks or collect and transmit data. State and local governments are aggregating and using data from the IoT to improve operations and asset management, fuel smart city initiatives, enhance quality of life and save money. Overall, about 27 percent of CDG survey respondents are deploying IoT technologies, 22 percent are actively discussing IoT technologies and 41 percent are considering implementing IoT technologies.

Potential government use cases for IoT are wide-ranging. The city of South Bend, Ind., put sensors in its storm sewer infrastructure to track in real-time the flow of rainwater entering the system. Using data from the sensors, the city's Department of Public Works makes immediate decisions to maximize the sewer system's conveyance capacity and eliminate overflows. The solution reduced the potential cost of the city's long-term control plan by an estimated $300 to $400 million.[3] The city of San Diego uses its street lighting infrastructure as the backbone for an IoT sensor array and smart city platform. Intelligent sensors deployed during the LED lighting upgrade help the city optimize traffic flow and parking, monitor air quality, enhance public safety and more.[4] Municipalities also are merging government IoT and consumer IoT devices. In Austin, Texas, the city utility can manage energy utilization by remotely adjusting residents' Nest thermostats by as much as four degrees.[5]

Almost half of state and local government leaders surveyed by the Center for Digital Government (CDG) say they are actively planning or deploying IoT technologies.

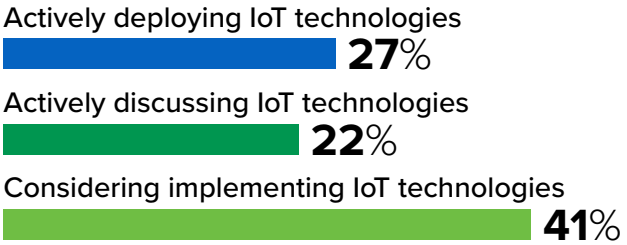
As IoT activity picks up, IT leaders need a cohesive strategy to take full advantage of IoT opportunities, maximize investments and ensure sustainability of these efforts. Former city of Minneapolis CIO Otto Doll, now a CDG senior fellow, describes sustainable IoT as "ubiquitous deployment of a solution that reaches a societal need at a reasonable long-term cost and ROI."

Components of an effective and sustainable IoT initiative include formal policies, a future-ready IoT ecosystem, data tools and security.

Formal Policies – Moving from Ad Hoc to Holistic

Despite overall interest in IoT and substantial deployment activity, the CDG survey shows that policies related to these initiatives are relatively immature. Respondents are having discussions to develop IoT policies — but only about 15 percent have formal IoT policies in place today. Where formal IoT policy development is underway, both CIOs and agency heads are highly involved, indicating that leadership recognizes IoT as a business issue, not just an IT responsibility.

A GROWING NUMBER OF STATES AND LOCALITIES ARE DEPLOYING AND CONSIDERING IOT TECHNOLOGIES



Source: CDG Intelligently Connected Survey

Formal policies take on growing importance as organizations move from piecemeal IoT deployments that target specific problems to broader IoT initiatives. These policies address how multiple IoT technologies fit together to increase value. Effective policies incorporate input from all key stakeholders, including agency heads, CIOs, public officials, citizen groups and business leaders.

When developing IoT policy, organizations should keep in mind the following considerations.

- **Alignment with overall vision and strategy.** Good IoT policy aligns with IT and business strategy related to spending, deployment and community priorities. CDG survey respondents were almost evenly split when asked if their current IT strategy addressed smart city initiatives by using IoT technologies. Thirty-two percent said yes, 36 percent said no and 32 percent didn't know.

- **Infrastructure governance.** Organizations must consider how they will govern the infrastructure to which IoT sensors and devices are attached. In many communities, infrastructure is owned by a private utility and not the city or county, so governments must find ways to work with these private entities.

- **Use of public data and other assets.** Communities will need to address how citizen data is used and protected. These policies must extend to vendor partners involved in IoT and smart city initiatives. In addition, communities need to create policies related to commercial use of public assets such as light poles and other infrastructure.

Besides addressing what happens to citizen and other data, organizations must create policies related to the commercial/ private use of both data and public assets such as infrastructure and poles.

- **Flexibility to facilitate emerging technologies.** Policies should facilitate the use of pilot projects that promote development of new IoT-related businesses and smart-city initiatives while maintaining adequate oversight.

"You want an open marketplace for ideas and solutions, but at the same time you need some degree of responsible control and regulation so everything goes smoothly and safely," says Doll.

- **Equity.** Communities must determine how they will provide a path for deploying IoT solutions that serve all residents.

Building a Future-Ready IoT Ecosystem

To collect, store, transmit, process, analyze and protect the vast volumes of data coming from IoT sensors, organizations need an IoT ecosystem that scales and adapts to future needs. This ecosystem is built on smart network infrastructure, a flexible platform, a variety of IoT tools and robust security.

Smart Network Infrastructure

Smart network infrastructure is the backbone for sustainable IoT initiatives. It provides connectivity to the myriad locations where data exists and enables organizations to optimize their use of the data coming from IoT sensors. This is an area where many communities may have deficiencies. Fifty-nine percent of respondents in a separate CDG survey said their network either can't handle expected IoT demands over the next 12 to 18 months or they don't know if it can.[6]

Although multiple network technologies can be used for IoT connectivity, cellular, WiFi and fiber optics technologies are core components of smart network infrastructure and sustainable IoT. When choosing network technologies, organizations should consider the types of data they'll collect from IoT devices, where it will come from and how they'll use the information. It's also a good idea to look for opportunities to use existing infrastructure or share infrastructure with other agencies that are adopting IoT initiatives. Regardless of the network technologies chosen, organizations need the capacity to handle massive volumes of data moving through edge devices, the cloud and applications.

▶ **Cellular.** Eighty-seven percent of CDG survey respondents primarily use cellular technologies to support their smart city initiatives. Cellular enables IoT applications to operate over long distances, but the cost and power consumption can be prohibitive for high-volume data transfer. As 5G becomes more ubiquitous, it will fuel new opportunities for IoT because 5G can simultaneously connect many more smart devices than 4G and other mobile technologies.

▶ **Wireless.** In the CDG survey, 84 percent of respondents use WiFi or other forms of wireless network technology for smart city initiatives. WiFi networks are often used to provide connectivity between sensor devices and local area networks. WiFi can handle large quantities of data and provides high data transfer rates; however, its power consumption may be too high for many IoT applications. Radio-Frequency Identification (RFID), Bluetooth, Zigbee and Z-wave connected devices are included under the wireless umbrella, although they typically have a shorter range than WiFi.

High-performance capabilities are especially important for real-time analytics, machine learning, artificial intelligence and other data-intensive processes associated with IoT solutions.

▶ **Fiber.** Sixty-five percent of CDG survey respondents use fiber for their smart city initiatives. With extremely high speed and low latency, fiber optic networks provide the performance, scalability and availability that IoT solutions need for real-time, data-intensive operations in dynamic, highly distributed environments. One IoT device alone does not require the bandwidth capabilities of fiber; rather, it is the totality of devices generating and transmitting continual streams of data that need these capabilities. A fiber optic network enables IoT data to travel from connected devices to the organization's data center or cloud solution at extremely high speeds and with minimal power consumption.

JURISDICTIONS USE MULTIPLE NETWORK TECHNOLOGIES TO SUPPORT SMART CITY INITIATIVES

Source: CDG Intelligently Connected Survey

Flexible Platform

Organizations will need a user-friendly platform to provision, automate and manage heterogeneous connected devices within the IoT ecosystem. This platform enables organizations to monitor IoT endpoints; translate proprietary protocols; analyze data; and integrate with other IT systems that store, process and interact with the data coming from IoT devices.

In many cases, cloud-based platform solutions provide a level of scalability, performance and reliability that is difficult to achieve in house. High-performance capabilities are especially important for real-time analytics, machine learning, artificial intelligence and other data-intensive processes associated with IoT solutions.

Whether organizations use an on-premises data center or a private, public or hybrid cloud solution, the key to maximizing the value of IoT is interoperability between different IoT systems. Cloud platforms and other open standards-based systems enable interoperability across a range of applications and provide the flexibility necessary to support long-term IoT initiatives.

"At any given time, you will have multiple generations of non IoT-connected devices like streetlights that would otherwise interact with IoT empowered streetlights; or you will have multiple vendors, depending on which department executes a contract," says Bob Bennett, former chief innovation officer for Kansas City, Mo., who is now a CDG senior fellow. "In Kansas City, regardless of which sensor collected the data, the APIs from those devices would transition the data to a centralized data set or at least interoperable datasets so that we could leverage the multiple departments' expertise to come up with a better picture of what's happening in the city."

Security

IoT creates new risks in multiple ways. Many sensors and IoT devices have inherent security vulnerabilities that are difficult to correct and manage over low power, remote connections. These vulnerabilities can be exploited to create botnets that execute distributed denial of service (DDoS) attacks and other forms of havoc. In addition, IoT devices are connected via an extensive network infrastructure, and many endpoints may not be under direct control of government agencies.

Compounding the problem, some IoT devices don't have the computing capacity to support traditional security controls such as public key infrastructure (PKI) encryption, leaving devices and the data they store or transmit vulnerable to hacking and other abuse. Finally, organizations may not monitor IoT systems and they often fail to reset the default passwords that come with IoT products, making them easy targets for cybercriminals.

While attacks on IoT devices themselves pose risks if the devices are disabled or mined for data, attacks on IoT endpoints also can lead to wider network security breaches. Worms and botnets (used in DDoS attacks) account for many IoT attacks. Targeted threats such as ransomware and emerging persistent threats such as VPNFilter, which can survive a reboot and are difficult to remove, are also threatening the IoT landscape.

State and local government leaders take these threats seriously. In a recent CDG network security survey,[7] also conducted as part of the Intelligently Connected survey series, more than half of all respondents were actively securing IoT technologies;

IoT funding and public-private partnerships

CDG survey respondents noted that funding for smart technology initiatives primarily comes from operating budgets. Other significant sources include capital budgets, state grants, external grants and federal funding. In addition, government leaders are exploring business models that can help sustain IoT initiatives. CDG's Bennett says effective funding strategies are crucial for long-term success.

"Over the lifetime of a 10-year contract with a vendor, the IoT system will require at least two significant technological upgrades," he says. "From a sustainability perspective, you need a revenue generation model to make sure that maintenance and life cycle replacement will take place."

For many organizations, this model may involve a public-private partnership (P3). The data generated by IoT devices is attractive to many private organizations, and with proper governance a P3 relationship can be an important source of revenue, expertise and innovation.

"Public-private partnerships allow cities to use the types of technologies that residents and visitors expect but are too technically challenging or expensive for a city to field at scale," says Bennett.

more than one third had a formal policy on securing IoT technologies; and more than half were planning to enhance security overall due to IoT implementation.

Policies and standards for specific IoT security components are just now being developed across established standards bodies and institutions. For guidance, organizations can refer to the National Institute for Science and Technology (NIST) draft recommendations for IoT security features as well as California's statewide IoT cybersecurity policy. At a minimum, policies should address data privacy and protection; device configuration; the device life cycle; and inventory tracking, device patching, device monitoring and event logging.

The IoT Toolbox

CDG survey respondents identified multiple tools needed to support IoT initiatives, including sensors to gather real-time data, data storage solutions, and analytics and security applications. These technologies are foundational to a sustainable IoT ecosystem.

While an infrastructure and platform that allows integration of data across the IoT ecosystem is essential for leveraging IoT data, organizations also need tools for visualizing data.

- **Sensors.** Sensors collect data and are usually coupled with technology that transmits data. Sensors range from cameras, microphones, and motion and gunshot detectors to devices that measure water levels and send a signal when certain thresholds are met.

- **Data storage.** Cisco estimates the amount of data stored in data centers will grow to 1.3 zettabytes (one zettabyte equals one trillion gigabytes) in 2021 and IoT will be largely responsible for that growth.[8] Cloud-based storage that can rapidly scale to accommodate these volumes will help organizations manage data growth without the financial and operational complexities associated with in-house deployments.

- **Analytics.** IoT has the potential to greatly expand an organization's ability to make data-driven decisions; however, most of the IoT data collected today is not fully leveraged. As they implement IoT strategies, agencies will

Ask these questions before you start

Organizations should be able to answer the following questions before they embark on an IoT project.

- ☑ **What societal problems does the project solve?**
- ☑ **Can the project be financially successful based on the current or expected economy?**
- ☑ **What is the balance between one-time and ongoing costs, and where will funding come from to sustain the recurring costs of connected devices?**
- ☑ **What other opportunities might be lost by investing in this project?**
- ☑ **How will we deal with the data produced by this project?**
- ☑ **How resilient is the system, and how will we secure it and the assets connected to it, including data?**
- ☑ **What other technologies need to be in place? What are the residual costs of these technologies?**
- ☑ **Is the solution equitable?**

need tools to visualize and analyze data. Data visualization tools let organizations take the raw data coming from IoT devices and turn it into actionable intelligence. They facilitate data analysis by helping users see real-time and historical patterns.

▶ **Artificial intelligence.** Artificial intelligence (AI) is another tool that will play a prominent role in IoT systems. Overall, CDG survey respondents were most interested in procuring IoT technology related to AI solutions.

"As organizations move from simple reporting analytics to predictive analytics, artificial intelligence will have to be part of those algorithms and assessments, simply because you have to extrapolate data to places where you don't necessarily have the same type of data coverage," says Bennett. "Wherever time is a factor in implementing a data-empowered decision — especially with edge processing at places such as streetlights or traffic lights — AI will have to be embedded into that technology."

Organizations can start to prepare for AI by understanding what decisions they will let computers make independently. They should also identify ways to let AI inform and improve decisions made by human users. Having a data scientist on staff can be beneficial to better understand what inferences can be made from data and to educate colleagues on the opportunities and vulnerabilities that exist when data is aggregated.

Getting Started: Best Practices for IoT Adoption

The following best practices will help communities create effective, sustainable IoT initiatives.

▶ **Develop formal policies.** As with many initiatives, this practice is vital for good governance, cost savings and the long-term success of any IoT project.

▶ **Focus on services that matter most.** To make the greatest impact, tie use cases to systems that are foundational to your community — such as transportation, electricity or water.

"In an ideal world, you're able to impact every resident and visitor in your community on any given day," says Bennett. "If you start with those three systems and then figure out what problems you want to solve, you can layer on from there with new sensors or new IoT devices."

▶ **Identify meaningful, measurable benefits.** It's important to understand the full benefit and cost of any project so that

To make the greatest impact, tie use cases to systems that are foundational to your community — such as transportation, electricity or water.

agencies can assure officials and the public they're making the best use of funds. Doll says governments also need to distinguish between cost savings and cost avoidance.

▶ **Pay attention to emerging technologies and their impact.** IoT solutions can entail significant investments of time and money. Consider whether a project will solve what is most important to the community and whether it will still be relevant in a few years' time. For example, if the future points to autonomous vehicles, does it make sense to invest heavily in parking-related IoT solutions?

▶ **Conduct pilot projects.** Pilots provide real-world experience with emerging technologies and help organizations better understand the potential issues and policy areas these technologies impact.

▶ **Seek mutually beneficial alliances.** Governments may be able to partner with other jurisdictions or the private sector to build out infrastructure and create shared solutions.

▶ **Prepare your workforce for change.** With IoT, some tasks will be automated, freeing up staff to do higher-value work. At the same time, agencies will need workers with cutting-edge skills in artificial intelligence and IoT. Identify needed skillsets for new technologies and conduct workforce planning accordingly.

Making Sustainable IoT a Reality

State and local governments are reaching an important threshold as IoT adoption skyrockets among consumers and industry and makes significant inroads in the public sector. Citizen demand and large-scale IoT-dependent innovations such as autonomous vehicles will soon change the civic landscape.

To ensure that IoT moves beyond a niche endeavor into something more valuable and sustainable, organizations need sound policies, a future-proof IoT ecosystem, strong security, advanced data tools and ongoing funding. These are the building blocks for long-term IoT success. They equip communities to develop and implement realistic solutions that solve the pressing needs of today while creating lasting value for tomorrow.

Endnotes:

1. IoT Analytics, State of the IoT 2018: Number of IoT Devices Now at 7 B — Market Accelerating, August 2018, https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/
2. Center for Digital Government. Intelligently Connected Survey Series, November 2018
3. U.S. Environmental Protection Agency, Smart Data Infrastructure for Wet Weather Control and Decision Support, August 2018, https://www.epa.gov/sites/production/files/2018-08/documents/smart_data_infrastructure_for_wet_weather_control_and_decision_support_-_final_-_august_2018.pdf
4. The City of San Diego, Smart Streetlights Program — San Diego Deploys the World's Largest Smart City Platform, Accessed December 2019, https://www.sandiego.gov/sustainability/energy-and-water-efficiency/programs-projects/smart-city
5. S. Hasan, KUT/NPR, Austin Requires Smart Thermostats in All New Homes, September 2016, https://www.kut.org/post/austin-requires-smart-thermostats-all-new-homes
6. Center for Digital Government, Smart Network Infrastructure: The New Standard for State and Local Government, December 2018.
7. Center for Digital Government Survey, Connected and Secure, Intelligently Connected Series, November 2018
8. C. Tozzi, Informatech. Cisco: IoT Data, Hyperscale Infrastructure Highlight New Cloud Trends, February 2018, https://www.channelfutures.com/strategy/cisco-iot-data-hyperscale-infrastructure-highlight-new-cloud-trends

IMAGES PROVIDED BY SHUTTERSTOCK.COM

Produced by:

CENTER FOR DIGITAL GOVERNMENT

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. The Center conducts e.Republic's annual Digital Cities and Counties Surveys; the biennial Digital States Survey; and a wide range of custom research projects. **www.centerdigitalgov.com**

Sponsored by:

Spectrum ENTERPRISE

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

SE-GV-RR005