The Internet of Things in State and Local Government

Key survey findings point to uncertainty, challenges in building connected communities.

Arguably, no technology has been more transformative in the last decade than the Internet of Things (IoT), which relies on the internet and sensors embedded in physical objects to connect and send data between devices.[1]

IoT has become ubiquitous in the consumer space. If you own a wearable fitness tracker, a smart thermostat, have used wayfinding beacon technology in an airport or museum, or have parked your car in a garage that automatically provides information on available parking spots, you've experienced IoT.

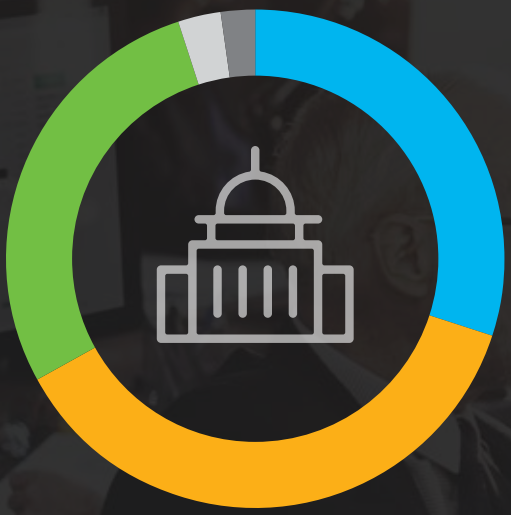
IoT has applications in the public sector as well. Government agencies are exploring IoT to create connected communities, which integrate intelligent technologies into physical environments to improve quality of life, public safety and service delivery.[2]

To explore public sector perspectives on IoT technology, the Center for Digital Government (CDG) surveyed 125 state and local government officials across four major verticals — health and human services, justice and public safety, transportation and infrastructure, and public administration and finance. Respondents' answers to the 21 questions provide insight into IoT trends and challenges, as well as procurement priorities.

RESPONDENT DEMOGRAPHICS

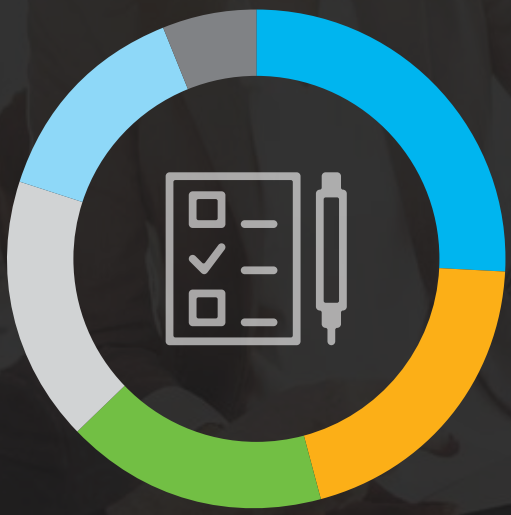
This report is based on a survey of 125 state and local government officials. Thirty-seven percent of respondents work within city or municipal government; 30 percent hold positions in state government; and 28 percent hold positions in county government. The remaining respondents either work in special districts (3 percent) or other levels of government (2 percent).

The majority of respondents (26 percent) work in public administration or finance, health and human services (20 percent), justice & public safety (17 percent), an IT agency that supports all verticals (17 percent), and transportation and infrastructure (14 percent). The remaining six percent work in other agency roles.



Level of Government

- State: **30%**
- City/municipality: **37%**
- County: **28%**
- Special district: **3%**
- Other: **2%**



Agency Function

- Public administration and finance: **26%**
- Health and human services: **20%**
- Justice and public safety: **17%**
- IT agency that supports all verticals: **17%**
- Transportation and infrastructure: **14%**
- Other: **6%**

KEY FINDINGS

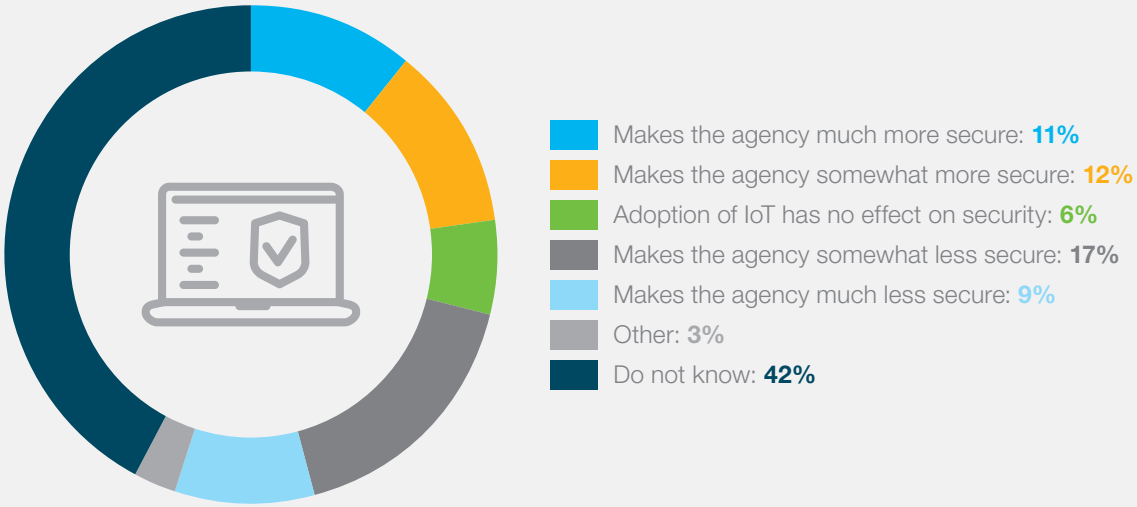
Government needs more education around IoT and connected communities.

Government officials are aware they need to leverage new technologies, but also acknowledge there are significant barriers to adopting IoT. Ninety-two percent of respondents said they need help to develop a connected community, and 87 percent said there are security challenges to overcome. However, some agencies are being proactive in this area: 50 percent are actively working with other government partners to move forward with plans to become a connected community. This indicates that some agencies realize the advantages of these technologies and are taking incremental steps to incorporate them into how they do business.

Agencies aren't sure if IoT is good or bad for security.

Security is an overarching issue for many government officials, and they disagree as to whether IoT puts them more or less at risk of a cybersecurity breach. Twenty-three percent of respondents said they think IoT will make their agencies more secure; 26 percent believe the opposite; and 42 percent said they're unsure of IoT's impact on cybersecurity.

How does the adoption of IoT technology affect an agency's cybersecurity posture?

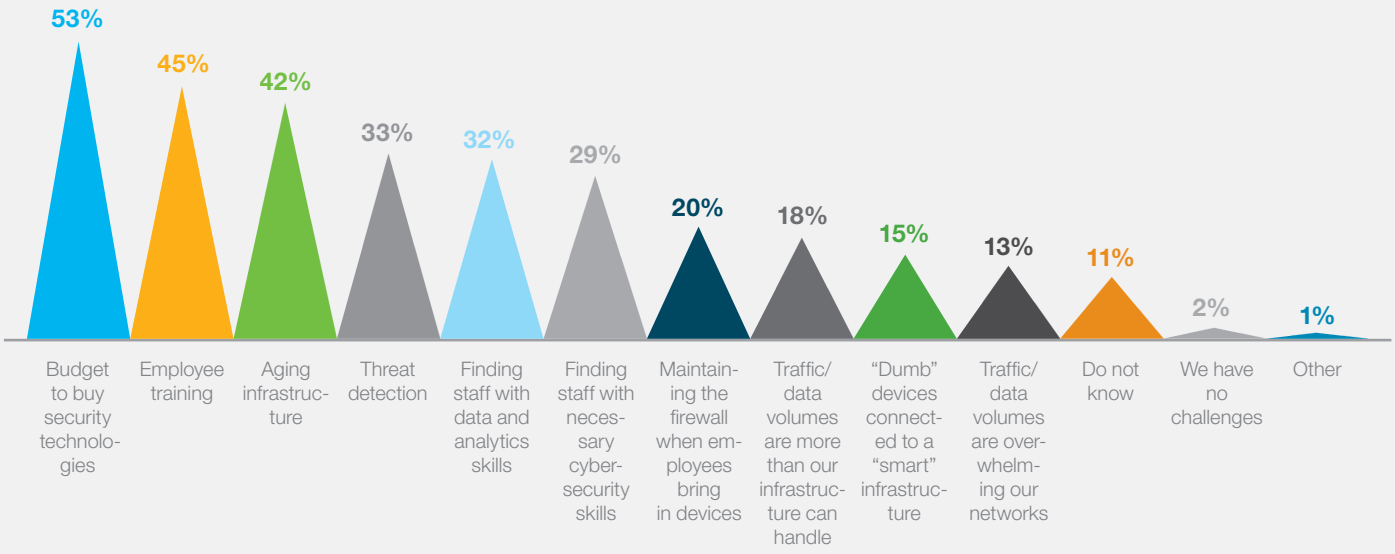


Those who believe IoT could introduce security risks noted that it increases the number and complexity of devices on their networks. They also cited political obstacles, including legislative and policy barriers to enacting shared security agreements. Government officials who think IoT could improve cybersecurity said these technologies will push their agencies to update aging infrastructure and re-engineer their networks to support IoT — a move that also could make it easier for agencies to integrate other newer and more innovative technologies in the future.

Government officials (87 percent) also worry about the security of connected communities. The main concern for a majority (53 percent) is allocating budget to security technologies, while 45 and 42 percent, respectively, said employee training and aging infrastructure that doesn't support IoT are significant concerns. Other government officials cited threat detection (33 percent), finding staff with data and analytics skills (32 percent), and data and traffic volume overwhelming their IT infrastructure and networks (31 percent total) as primary security challenges.

At a department level, officials who work in justice and public safety and public administration and finance said their main security challenge with becoming a connected community is the budget to buy security technologies. Conversely, transportation and infrastructure officials and HHS officials said their primary security challenge is aging infrastructure that doesn't support IoT technologies.

Within your field, what are the primary security challenges related specifically to becoming a connected community?

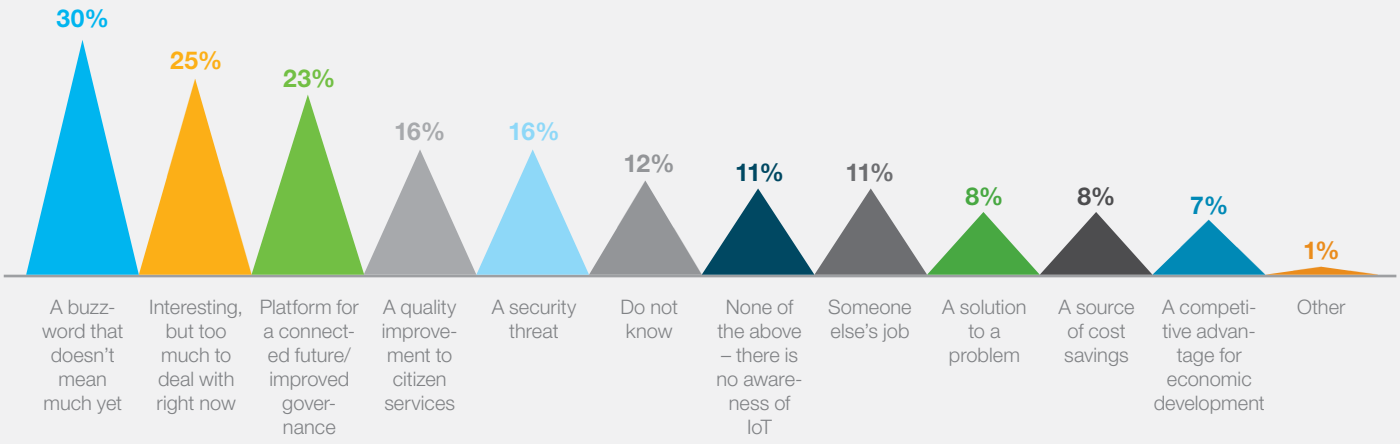


There's a conundrum for agencies. When asked where IoT is needed the most, citizen access to services (37 percent) and public safety (25 percent) rank at the top. Thirteen percent also said IoT could help protect their digital infrastructure and support cybersecurity. Delivering quality service and keeping citizens safe are two of government's most important roles. However, budgetary constraints, the scope (in terms of implementation and staff training) required to update technology, and valid concerns about how to securely and cost-effectively integrate new technologies keep many agencies from making progress.

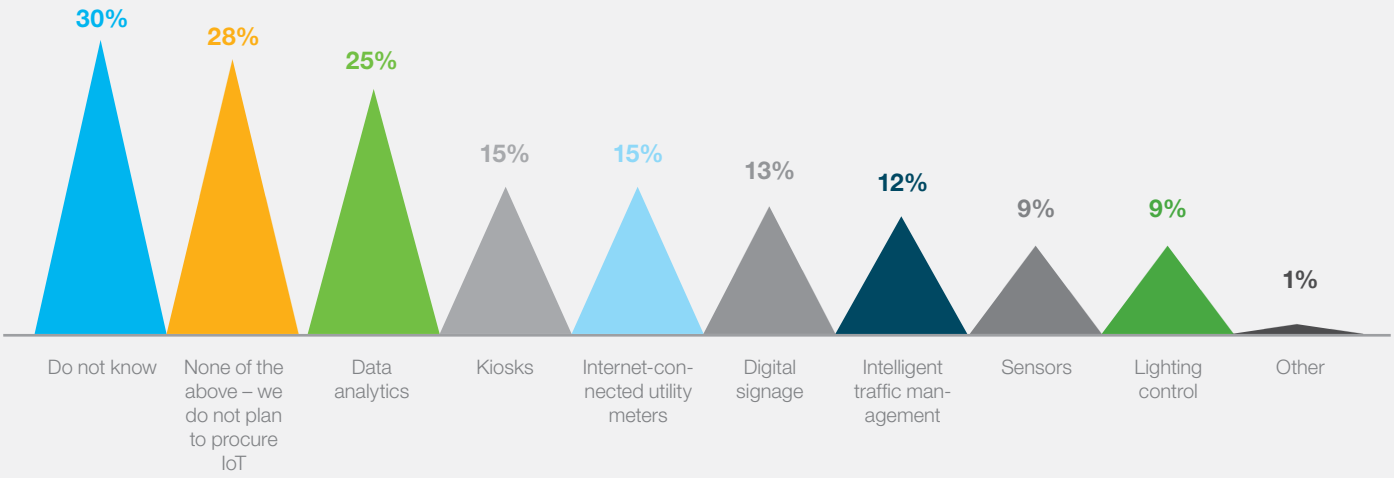
Leaders see the IoT as a future initiative, but many are already implementing IoT technologies.

More than half of respondents (55 percent) said IoT is "a buzzword that doesn't make sense yet" and it's "interesting, but too much to deal with right now." However, despite this skepticism, many agencies are already buying these technologies and plan to procure them in the next year.

In general, how is IoT perceived within your agency?



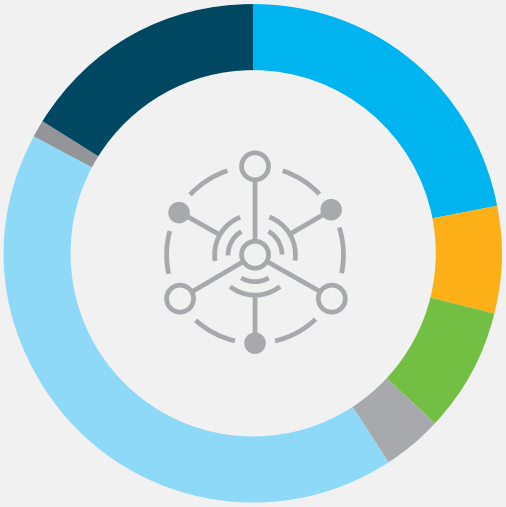
Which of the following IoT technologies do you plan to procure in the next 12 to 18 months?



This may be because they see the potential for how IoT technologies can help them achieve larger business goals — 68 percent of respondents said having a connected infrastructure will help their agency achieve its mandate. However, from these responses, there appears to be a gap between sentiment and actual implementation, which may be due to competing government priorities and the financial and time investment required to transform an agency's IT infrastructure.

Governments lack a strategy or vision to implement IoT holistically, across multiple agencies.

Multi-agency, holistic procurement of IoT technologies seems to be the exception rather than the rule. Twenty-two percent of respondents are procuring these technologies, but only on a one-off, case-by-case basis, while seven percent are procuring IoT technologies, but only within their agency and in a siloed fashion. Only eight percent of respondents said their procurement was part of a multi-agency effort to move forward with becoming a connected community. An even smaller share — four percent — said this was a holistic, enterprise-wide effort involving all agencies.



In your jurisdiction, are you procuring IoT technologies?

- Yes, but only on a one-off, case-by-case basis: **22%**
- Yes, but only within our agency in a siloed fashion: **7%**
- Yes, as part of a multi-agency effort to move toward a connected community: **8%**
- Yes, as part of a holistic, enterprise-wide effort involving all agencies to become a connected community: **4%**
- No, we are not procuring IoT: **42%**
- Other: **1%**
- Do not know: **16%**

When it comes to procuring citizen service technologies, quality, security and cost are the top priorities for agencies, but the key factors that accelerate the procurement process are public demand and the allocation of funding for specific projects. These two drivers will be critical for more agencies to see IoT as an urgent priority rather than a future initiative.

PREPARING FOR AN IOT-DRIVEN, CONNECTED FUTURE

If IoT is to become as prevalent in the public sector as it is in the consumer world, several barriers and needs for government agencies must be addressed. Chief among them is funding, and the more difficult task of overcoming the perceptions of some government officials that these technologies are interesting but will have more real-world applications in the future.

It's encouraging that many agencies view IoT and connected communities as a way to enhance the quality and quantity of citizen services. However, there's still a significant gap between perception and reality, and doing all the tactical and strategic work required for agencies to deliver a better citizen experience. IoT can empower agencies to lay a foundation for connected communities — more of them just need to realize that the time to integrate these technologies isn't far off into the future. The time is now.

Endnotes:

1. https://www.gartner.com/it-glossary/internet-of-things/
2. https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=505364

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

For:

CISCO

Every day you seek innovative ways to connect the unconnected in your communities. But budgets, staffing limitations, and outdated infrastructure are proving a challenge. At Cisco, we understand, and can partner with you to implement IoT strategies to meet these challenges, and more, including unifying data from sensors and devices throughout your communities into a single platform. All while working to keep agency and private citizen data secure.

Cisco is already helping governments like yours develop a strategic and holistic approach to IoT. And together we're empowering greater opportunities, security, and resilience that enhances quality of life in their communities. Now it's your turn.

Learn more at **cisco.com/go/SLG**