your FAQ to IoT in government

govloop

We need to come up with the best practices that work from a technology perspective, from a business perspective and also from the government perspective."

SOKWOO RHEE, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Executive Summary

Lubbock, Texas, is going to spend $35 million to purchase and install more than 100,000 advanced electric meters. Last year, the Lower Colorado River Authority received a $650,000 contract from the Department of Homeland Security to increase its use of smart sensors, building atop more than 275 already connected river sensors in its Hydromet program. The U.S. military has already deployed 11,000 unmanned aerial surveillance vehicles, and the Air Force is expanding its Smart Base program to further support it.

The internet of things (IoT) is on the rise within all levels of government. Connected devices and sensors are being used to learn about our nation – its infrastructure, citizens and environment.

But while IoT adoption is on the upswing, it continues to be clouded and misunderstood for many government agencies. Common questions and misconceptions increase public servants' reticence to move forward with this game-changing field of technology.

Is IoT safe? Do we need it? Who should deploy it? What do I need to use IoT, and who can help me? This guide will help address all these questions and more. We've compiled the most common questions asked by government employees regarding the internet of things. Then, we asked other public servants those questions, seeking real advice from IoT practitioners in government.

This guide provides insights, best practices and real-world advice for how to get started with IoT at your agency.

Contents

Our Experts

Gregory Wilshusen

Director of Information Security Issues, Government Accountability Office

Christine Kendrick

Air Quality Lead/Smart Cities Coordinator, Bureau of Planning and Sustainability, City of Portland

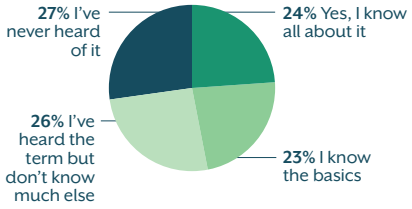
Sokwoo Rhee

Associate Director of Cyber-Physical Systems Innovation, National Institute of Standards and Technology and leader of the Global City Teams Challenge (GCTC)

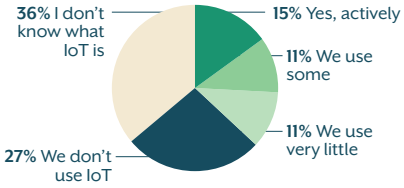
What exactly is IoT?

Via our weekly polls, we asked our GovLoop community members about their current understanding and use of IoT. The results showed that while some agencies are leveraging sensors and other devices, many are still less familiar with IoT technologies.

Do you know what the internet of things is?



Does your organization currently use IoT?



So, what is IoT?

Technically, IoT is "the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment," according to Gartner.

But our government experts also had their own definitions that give more insight into the true meaning of IoT:

"When I hear that term, I picture a distributor network of remotely connected devices that ideally are sending actionable quality data and information that supports decision-making processes." – Christine Kendrick, Air Quality Lead/ Smart Cities Coordinator, Bureau of Planning and Sustainability, City of Portland

"The internet of things refers to the technologies and devices that collect information or data, and then communicate it to the internet or other networks and, in some cases, act on that information." – Gregory Wilshusen, Director of Information Security Issues, Government Accountability Office

"From a technology perspective, the internet of things is connecting devices through a communication mechanism, collecting the data, analyzing the data and acting on the information extracted out of the data. It's a combination of logical systems and physical systems. From a benefits perspective to those cities, it's about improving quality of life, using advanced technologies, like connectivity, sensors and data, as well as some decision-making tools." – Sokwoo Rhee, Associate Director of Cyber-Physical Systems Innovation, National Institute of Standards and Technology

What these public servants' definitions highlight is that IoT is about more than devices or data. It's about leveraging those tools to create actionable insights that ultimately benefit a government's constituents.

How is IoT different from Smart Cities?

IoT is especially growing within cities and communities, where real-time data alerts can directly influence citizen decisions on things like parking, outdoor activity, traffic routing and other common tasks. In turn, this use of IoT has led many municipalities to embrace a "smart cities" ethos or even a formal strategy.

According to the federal government, smart cities are "communities that are building an infrastructure to continuously improve the collection, aggregation, and use of data to improve the life of their residents – by harnessing the growing data revolution, low-cost sensors, and research collaborations, and doing so securely to protect safety and privacy."

In other words, a smart city is not just a city that simply deploys IoT. It is a community that leverages IoT, as well as other tools, to create a holistic environment for analyzing and acting on data. That data may be solely produced by sensors, or it may be combined with external research. IoT is a necessary component for smart cities, but it is not the only one.

How do I know if IoT is right for me?

The use of connected devices is steadily on the rise. In fact, by 2020, it is expected that more than 28 billion IoT devices will be in operation. Government is no exception to this trend. In fact, Rhee argued that IoT is going to be a value-add to almost every community and municipality in one form or the other.

But just because IoT can add value to government generally doesn't mean that it should be applied to your department or your specific project. Like any other technology, it's critical to ensure that a sensor or smart device meets a specific need before it is procured and deployed. It also needs to be the most cost-effective option that provides the appropriate level of data and support.

Our experts agreed that you first have to determine a problem you, your department or your agency is trying to solve. Then, assess what you need to solve that problem. Do you need more data to solve the problem? Do you need real-time updates from field locations? Do you need more automated collection to increase efficiency?

If you answered yes to those questions, an IoT solution might be what you need. You might, however, be able to get the same information or resources from a different solution. For instance, you may need additional data to complete a program analysis. Another agency might already have that data available, without your having to purchase and deploy a device for collection.

"It really gets down to a bottom line of: Is IoT going to be the best and most cost-effective alternative for the agency to achieve the desired outcome that it seeks to obtain?" Wilshusen said.

Even if new data must be collected by your organization, it might not require establishing a full IoT infrastructure. Wilshusen also reminded us that IoT is not about collecting information from one source, but instead gathering disparate information from a range of devices and correlating it in a central location. If your organization requires only a single dataset to meet its needs, IoT may not be worth the investment.

"Will IoT actually help solve that issue that your city or community is facing?" Kendrick said to consider. "It takes a lot of work to really understand if multiple measurements are going to solve that. Maybe you don't need a distributed network. Maybe you only need one site of improved data collection instead."

In some cases, you might consider a single sensor to meet your needs or, more simply, have an employee manually gather in-the-field data on a one-off basis. This is especially true if you need data for context, rather than extremely accurate or niche data. "From an IoT project or network, we require high-quality, reliable data that's either measuring the local environment, monitoring infrastructure or how community members are interacting with the built environment," Kendrick said.

So, when is IoT the right solution? If your organization requires a consistent flow of complex, niche and accurate data to meet a specific need, IoT can be a worthy investment.

"It really gets down to a bottom line of: Is IoT going to be the best and most cost-effective alternative for the agency to achieve the desired outcome that it seeks to obtain?"

GREGORY WILSHUSEN, GAO

Where do I start with IoT?

Where you start with IoT will largely depend on your organization's existing technical capabilities and program matter expertise. Successful IoT projects require some level of both. Luckily, most organizations likely already have this.

Government is not new to the IoT game, Rhee said. Most agencies, especially on the local level, have deployed things like smart water meters or energy sensors as a way to automate basic public services. They simply haven't called them IoT.

"There are examples where they have to install completely new hardware [to explore IoT]," he said. "But typically, a community already has some sort of water meters employed, or they already have a transportation system that collects GPS signal, for example."

In those instances, the first step into IoT isn't deployment of new sensors. Agencies should instead take the time to learn what works in those programs, and what might be altered to improve a more sophisticated iteration of it.

Rhee also noted that there are some "no-brainers" for communities looking to engage with IoT. "For example, flood measurements and predictions, smart lighting, or smart water meters and utility meters. It's almost a no-brainer now that you can save money or increase efficiency using those sensors," he said.

If your agency is looking for a tried-and-true first step into the realm of IoT, these solutions can be a great starting point. Because many government organizations have already invested in these devices and programs, you'll be able to find a number of public servant practitioners to share their insights and advice from their own experiences.

Plus, the project itself will be a low-risk way of learning IoT and gaining buy-in for future projects. "In many cases, that's how you start because you don't want to invest millions of dollars when you do not really know the outcome. When you are successful in those kinds of first few examples, that's when the city will get into a more serious thought process," said Rhee.

> **"It's a matter of figuring out what is underserved today out of the system or the infrastructure you already have."**
>
> **SOKWOO RHEE, NIST**

Nevertheless, many agencies will ultimately decide to pursue more niche or customized solutions. Especially for federal agencies, adopting the most popular IoT program might not be an option if they're trying to meet a specialized mission. In those cases, the first step won't be exploring sensors or devices to deploy.

If your agency is truly charting unexplored territory with IoT, you'll want to start with data. At its heart, IoT is about collecting needed data to help agencies form complete insights and make decisions. Thus, your first step will be to understand what additional data your agency needs.

"If you have a lot of existing data or something that you're already collecting, I would really take a look and see what's missing from that data," Kendrick said. Once you know what data you would like to collect, you can start investigating sensors that can collect and translate that information for your agency.

"It's a matter of figuring out what is underserved today out of the system or the infrastructure you already have," Rhee said.

Who from my agency should be involved in this project?

Of course, every IoT team will look different depending on the budget, staff resources and specific parameters of the IoT project. But our experts said there are a few must-have staff members who should comprise your IoT team.

CIO

Having either the CIO or the CTO buy into an IoT project is critical, said Rhee. "You need somebody who understands technology and someone who can talk with authority to the broad range of departments about those aspects," he said. "And you need somebody who may not have a complete budget, but somebody who can influence the decision process."

IT Professionals

Beyond having an IT leader spearhead IoT, you also need skilled professionals to manage the technology components of IoT. "Certainly, IT and networking folks will need to be involved to determine how the IoT application will be architected across the agency's networks to assure that each of the elements and technologies that are needed for an IoT application are being addressed," Wilshusen said.

Security Officers

"You must have at least one person who can take care of cybersecurity and privacy issues," Rhee said. These team members should work closely with the IT professionals to understand and mitigate risks before sensors are deployed, as well as during program operations.

Data Analysts

IoT can collect and correlate data from a variety of sources, but it cannot fully overtake the role of data analysis for an agency. "Even if you have a really automated data management and dashboard system for a project, we're learning that it still takes a lot of staff time for testing data management, doing additional data analysis and validating or transforming that data into information that's usable and customized to what your other project managers need," Kendrick said.

Subject Matter Experts

"The first thing you really need to have are subject matter experts for the type of measurement you're conducting," Kendrick said. "For example, I'm an air quality scientist. Having that expertise on an air quality sensor project is really needed to be able to evaluate what sensors can impact the project and how to process data from the device." Every IoT project should include someone who can knowledgeably assess the validity and relevance of produced data.

Technicians

Kendrick pointed out that many devices require in-the-field mechanical and/or electrical attention to maintain functionality over time. Be sure to include maintenance technicians and other field workers in your team planning. Wilshusen mentioned that in some instances, these experts may be provided by the device vendor or manufacturer.


Elastic
Map
Reduce
Amazon
Machine Learning
AMAZON
WEB SERVICES
BUILD
ON
aws
www.BuildOn.aws
REAL TIME
DATA
Amazon EC2
Model Repository
Developers

More than IoT: How to Build a Smart City

An interview with Hardik Bhatt, Leader of Smart Cities & Mobility Business at Amazon Web Services

IoT has become synonymous to a smart city. But as any city that has deployed IoT can attest, becoming a smart city requires more than that.

"When you think of smart cities, you think about sensors, but technology is only a third of what makes a smart city," said Hardik Bhatt, Leader of Smart Cities and Mobility Business at Amazon Web Services (AWS). In addition to connected devices and data, Bhatt explained in a recent interview that communities must also focus on people and processes to build a successful smart city. AWS provides the cloud infrastructure and services and collaborates with a robust partner community to give customers access to solutions from both big technology providers and small startups.

Consider a common component of smart cities – ACES. The number of autonomous, connected, electric and shared (ACES) vehicles is rapidly growing in urban areas, with many cities heavily investing in solutions to increase ride sharing, streamline traffic patterns, and improve transportation.

A city needs the infrastructure to support ACES – like charging stations for electric cars or traffic signals that can communicate with connected vehicles. That requires careful planning, as well as solutions to integrate different technologies into a comprehensive system. And that planning involves many stakeholders including other municipalities and/or states, as connected roadways extend beyond one city's borders.

Additionally, the data created by these connected roadways and vehicles must be collected somewhere, and likely shared across government departments in order to keep traffic running smoothly. Departments will need to analyze that data to make real-time and future decisions about traffic and infrastructure.

In this scenario, sensors placed on these vehicles are a critical component of a smart city, but they are only one piece. For cities to become "smart," they must create a holistic architecture that enables them to connect the technologies, processes, and people of IoT.

That's why many municipalities leverage cloud computing. Cloud provides a scalable infrastructure that can easily connect to disparate devices, including smart technologies. Cloud allows ingestion of various data sources from city-owned or managed on-premises, SaaS systems, or from third-party systems. Once information is ingested, it can be correlated and analyzed in the cloud. Plus, that data can be securely shared with others as needed.

"Cities need to start thinking about outcomes, about what they are going do with their data from smart devices," Bhatt said. "Cloud provides a secure way to manage that data and use analytics."

Kansas City, Missouri provides an example of cloud in action. Along the two-mile corridor of the Kansas City Streetcar, a $15 million public-private partnership has supported deployment of 325 Wi-Fi access points, 178 smart streetlights and 25 video kiosks, as well as pavement sensors, video cameras, and other devices. But what makes this investment more than a group of sensors is that all of their data is collected, correlated, and analyzed through a holistic cloud infrastructure.

Kansas City uses an integrated suite of AWS services and applications to make sure sensor data is used to its fullest extent. The city uses Amazon Kinesis to process more than one million real-time events per day from devices. That data is then queried and analyzed automatically by AWS Lambda, and when necessary, stored along with long-term city and regional data on Amazon Redshift. This is done by the third-party urban analytics and intelligence platform built by Xaqt, an AWS partner, and integrated with the AWS cloud to provide deeper insights into actionable data.

Using all of these IoT solutions together in the cloud, Kansas City can make accurate predictions about traffic infrastructure and patterns that save money while improving safety and convenience for its citizens.

And Kansas City is just one example. Virginia Beach is using a combination of sensors and cloud-sourced data for their early flood warning system. The state of Georgia, city of Las Vegas, and state of Utah are using Alexa skills to provide better customer engagement, and Louisville, Kentucky is using open-source traffic analysis tools built on AWS to make informed traffic flow decisions.

As more government organizations adopt and deploy connected devices, sensors, analytics, and machine learning in a strategic manner, they'll also inevitably have to consider how their internal systems and services support that goal. Only with the cloud can agencies connect, analyze, and share their sensor-generated data and excel with IoT.

What technologies do I need for IoT?

When you think of the technical needs of IoT, you most likely think of the sensors that collect data at the perimeter. Those sensors are necessary, but they aren't the only technology requirements for IoT. To build an infrastructure of connected devices and data, agencies will also require robust networking, storage and data analytics.

1 Networking

First, agencies must have networks for IoT. After all, we're talking about the internet of things. Devices must be connected to your central IT systems in order to transmit data. They often also receive data, such as automated alerts or action triggers, from your central systems.

In many cases, networking is the most diverse component of an IoT project because agency IT also varies widely. Whether you rely on the internet or create a closed network that only serves your organization will be largely dependent on your agency's security needs and organizational footprint. Additionally, the setup of your current IT infrastructure – whether it relies on outdated or legacy systems or more modern architectures ¬– will also heavily determine how you connect devices.

In most cases, agencies will forgo fully re-architecting their infrastructures to create new connections. But there are ways to upgrade networking to pursue IoT. For instance, software-defined networking is a cloud-based approach to networking that centralizes network management, even as it layers atop a large sprawl of different hardware configurations. It provides more flexibility and quicker scalability than a traditional, hardware-defined configuration, making it easier to integrate new sensors into your network.

2 Storage

With networking in place, your organization can begin digesting data from sensors. But when it comes to IoT, we're not just talking about a couple spreadsheets of data. Remember, IoT is a network of multiple devices, constantly collecting robust and disparate data. That means your agency is going to receive a deluge of data that it will need to store.

There are some technologies, such as gateways and rule engines, that can mitigate traffic from the perimeter to agency data centers. But even if that middleware is applied to sort through data and only send the most relevant information to the agency, you're still confronted with a large volume of data.

That means agencies must have significant storage capacity in order to leverage IoT. In traditional architectures, this storage is based on-premise in a data center that is owned and operated by the agency itself. That model, however, is quickly being sunsetted as organizations pursue things like IoT.

"If you're collecting large volumes of information, often that will be stored out in cloud computing environments, usually operated by private-sector companies," Wilshusen said. Cloud is easily deployed, scalable and elastic. As a result, it's a good option for agencies pursuing IoT because it can quickly expand to meet the load of new data volumes. Plus, it costs agencies less than installing new hardware racks of on-premise storage. Cloud is also a necessary component to support the aforementioned software-defined networking.

"The more you can figure out those tools before you deploy an IoT project, the more successful you're going to be."

CHRISTINE KENDRICK, CITY OF PORTLAND

3 Data Analytics

Finally, when you've collected your data in a central storage system, it will need to be analyzed. The real value of IoT is the ability to act on data and make better decisions for your organization and its constituents. But to achieve that requires more than a couple of data scientists poring over spreadsheets of data. "The sensors are only one part of the system. You really need to have tools ready for data management, data analysis, data exploration and visualization," said Kendrick.

Agencies require a data analytics capability – most often a cloud-based software or platform ¬– to ingest, correlate and analyze data. Again, the type of analytics technology required will vary by organization. But in this case, the choice of solution is made based on project needs, rather than an agency's IT capabilities.

"You need to identify what type of analysis you want to have performed over that data, and what your objective is to be able to do with the results of that analysis," Wilshusen said. "That understanding will then lead you to identify the type of data analytics software you need and potential vendors to provide that capability."

In addition to determining what analysis you will perform, you must consider how the platform will correlate your IoT data with other information your agency has already collected or might pull from a different source. Integration and data standardization capabilities are another important consideration when choosing an analytics platform.

Finally, you'll most likely seek a platform that makes it easy to leverage your data because you can't rely on data scientists alone. Your analytics suite should offer easy-to-understand reports that are accessible by many users to ensure you make the most of your IoT information.

Sensors are only one piece of a more complex IoT system. Not only will agencies require these capabilities, Kendrick believes they have to consider these well before they invest in IoT. "The more you can figure out those tools before you deploy an IoT project, the more successful you're going to be," she said.

How do I work with the private sector?

With very few exceptions, government is not in the business of creating devices or sensors. As a result, "for most agencies, it will be very difficult to have an IoT application that is completely in-house, where the agency is responsible for all elements of the app or program," said Wilshusen.

Rhee mentioned that, in some instances, a university or other non-government organization may prototype a device without private support but, even in those cases, the device is usually acquired by the private sector before becoming available to government organizations at scale.

For government, working in IoT requires working with the private sector.

For some agencies, that private-sector partnership will begin and end with device acquisition. In those instances, Kendrick emphasized the need to clearly outline the criteria you have for a device – including what it measures, how it operates and what level of detail it can provide – as well as expectations for service.

But in most cases, collaboration will not be a one-and-done step to achieve IoT results. Kendrick also explained that, in many cases, a technology or sensor will require further development after deployment. For instance, as you integrate the tool with other parts of your network, you may find the need to update or alter certain specifications.

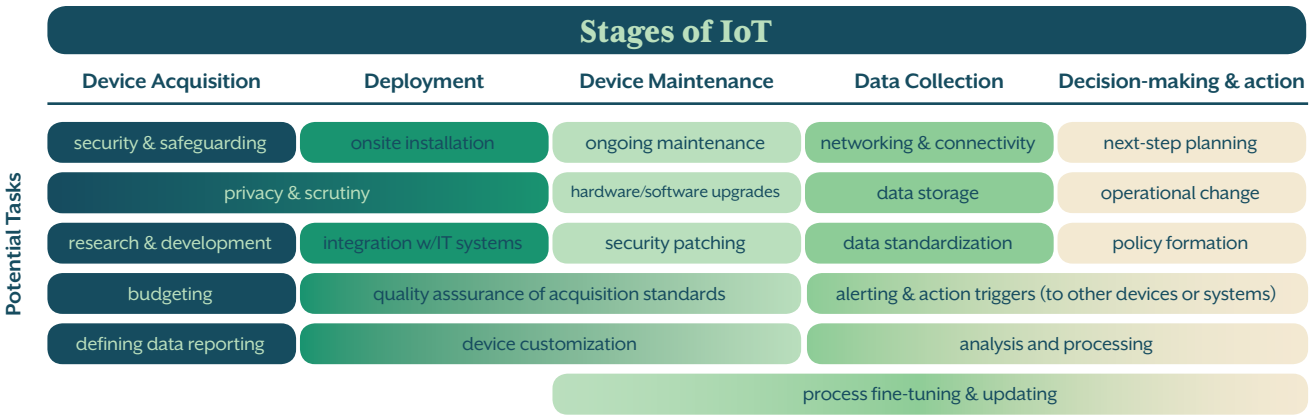
Additionally, once your agency begins using the data generated by sensors, it may find new use cases that require modifications to the original device's functionality.

For that reason, most IoT projects require ongoing public-private partnership. The terrain of IoT has adapted to this model.

"Five or six years ago, IoT or 'smart cities' was really just a two-party interaction," Rhee said. "But more recently, things started changing. Now additional players have come into play, including research institutions like universities. That also includes nonprofits and more philanthropic foundations, and also the federal government. So, now it's not a simple sales and revenue procurement process; it's a multiparty collaboration process."

A collaboration can take many forms and involve any number of stakeholders or organizations. Agency work with private partners will happen along a complex spectrum. "The bottom line is there's no single model that is a silver bullet for everybody," Rhee said.

To determine the right model for your agency, assess your in-house capabilities and how they can support your program throughout the lifecycle of an IoT project. Use the chart below to understand the tasks associated with IoT and what capabilities you might need to find within private-sector companies or academic institutions.



What are the risks of IoT?

The benefits of IoT are nearly endless, including outcomes like increased efficiency, cost-savings, better data-driven decisions and ultimately better governance. Nevertheless, there are risk associated with any new information technology project, especially when that project involves attaching new devices to secure government networks. Specifically, our experts called out three major risks involved with IoT, as well as tips to overcome those potential obstacles.

Privacy

In many instances, IoT collects environmental, infrastructure, agricultural or other non-personal data that poses minimal privacy risks. That can make it easy to forget how other projects can actively monitor constituent behaviors or even collect their personally identifiable information. For instance, the government of Canada once recruited a set of volunteers to wear sociometric badges that measured their location, movement and voice tones to analyze the positive and negative aspects of employee work life. While the information may be valuable, it should only be collected with the right privacy measures in place.

Tips to overcome: Wilshusen said it's imperative to include privacy officers in your IoT project before it is launched. Together with cybersecurity or mechanical professionals, they can determine the privacy implications of collected data and create technical safeguards to ensure that private information isn't exposed. Additionally, make sure to transparently communicate what information is being collected, how it will be used and how it will be secured to all relevant stakeholders – including constituents. Finally, communicate all privacy needs to your vendors and ensure appropriate language is included in contracting.

Security

It's no secret that IoT has a lot of security implications. "The interconnectivity between these types of networks greatly expands the avenues of attack and increases vulnerability," Wilshusen said. Without proper security measures applied to devices, as well as the connections it creates to a network, IoT can become an endpoint cybersecurity risk for government.

Tip to overcome: Rhee suggested that agencies look for cybersecurity guidance from authoritative bodies like NIST. He also said, however, that in conversations with some communities, they were not sure federal standards could be directly applied to what they needed for municipal governance. In those cases, Rhee encouraged cities to seek other local organizations and the private sector to combine resources and collaboratively develop common security standards for IoT applications.

Budget & Sustainability

The maintenance of devices, infrastructure to support a large influx of data and the specialized labor to oversee both can all quickly add up to make IoT a costly investment over time. Many organizations can underestimate the resources required, which risks underfunding the project and diminishing success. Especially if budgets only estimate cost for the first segment of a project, IoT projects are likely to end prematurely.

Tips to overcome: Kendrick recommended carefully tracking any hours or costs associated with a single IoT project to set realistic budgets for future or larger endeavors. Rhee added that successful projects from other organizations can be used to estimate costs for similar internal programs. Additionally, Rhee said to plan for projects as if they were permanent strategy additions, rather than one-off deployments of sensors and devices. "You have to really cross the chasm of all the excitement, and to consider it a mainstream business trend that is here to stay," he said.

Where do I find help?

Throughout this guide, we've mentioned the value of finding likeminded organizations that have already pursued IoT. Agencies with more experience can offer lessons learned, provide guidance in new projects and help your organization avoid common missteps in the first stages of IoT. But where do you find these IoT-savvy organizations? Here's a list of IoT resources to help you take your next steps:

Case Studies to Review:

The **General Services Administration** has been a pioneer in installing smart building technology across federal government infrastructure.

San Leandro, California, plans to integrate a 10-gigabit fiber loop into public infrastructure and services to support IoT.

The **Lower Colorado River Authority** built a network of 275 connected river sensors — called Hydromet — to monitor and report stream flows and other data.

The U.S. Air Force has a "Smart Base" trial underway at **Maxwell Air Force Base** in Alabama to see how IoT can help monitor perimeter security, gates, vehicle fleet management and other operations.

Virginia Beach, Virginia, is using data from sensors that measure water levels and wind speeds to develop a hydrodynamic modeling system to monitor and prevent flooding.

Pittsburgh is replacing 40,000 city-owned and operated streetlights with smart devices as a pilot for IoT, while also tackling neighborhood equity issues.

Organizations to Find Support:

The **Global City Teams Challenge** – A program run by NIST to encourage collaboration and problem-solving among cities deploying IoT

IEEE Smart Cities – A global network of cities pursuing IoT and other smart technologies for humanitarian purposes

Green Electronics Council – An organization that helps governments acquire, deploy and maintain environmentally friendly technology solutions

The Internet of Things Consortium – A global organization focused on increasing partnerships, knowledge-sharing and funding opportunities related to IoT adoption

Research for Further Reading:

Recommendations for the Development and Implementation of Distributed Sensor Networks – A comprehensive report by NIST, the city of Portland, Oregon, and others regarding their insights into creating IoT ecosystems

How to Implement the Internet of Things – A free, 10-minute online course describing how to architect networks to support IoT

Smart City Challenge: Lessons for Building Cities of the Future – A best-practices report on IoT in cities, from the U.S. Department of Transportation

Internet of Things: Enhanced Assessments and Guidance Are Needed to Address Security Risks in DoD – A report from GAO on the risks and recommendations for IoT deployed across the Defense Department

Conclusion

The internet of things has the potential to revolutionize the way government meets its mission on the local, state and federal levels. With so many organizations only in the early pilot stages of IoT, however, the task of deploying robust networks of sensors and devices to create actionable data can seem daunting for a single agency. That's why this guide has focused on the most common questions asked by public servants. Our answers not only highlight the shared misconceptions and concerns that agencies have for IoT; they also highlight the many ways that organizations can collaborate to pursue better outcomes.

"We need to come up with the best practices that work from a technology perspective, from a business perspective and also from the government perspective," Rhee concluded. Only by working across organizations and levels of government will that be achieved.

About GovLoop

GovLoop's mission is to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 270,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to the public sector.

For more information about this report, please reach out to info@govloop.com.

govloop.com | @govloop

Thank You

Thank you to Amazon Web Services for their support of this valuable resource for public sector professionals.

Author

Hannah Moss, Senior Manager of Production

Designer

Kaitlyn Baker, Creative Lead

1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop