YOUR QUESTIONS ANSWERED:
The Internet of Things in Government
## Contents

<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>03</td>
<td>Executive Summary</td>
</tr>
<tr>
<td>07</td>
<td>The New IP: How Software-Driven Platforms Change the IoT Scene</td>
</tr>
<tr>
<td>11</td>
<td>Monitor Locally &amp; Manage Centrally with the Internet of Things</td>
</tr>
<tr>
<td>12</td>
<td>Making a Smart City</td>
</tr>
<tr>
<td>15</td>
<td>Communicating With the Public Through Sensors &amp; Technology</td>
</tr>
<tr>
<td>19</td>
<td>Connected Solutions Promise Increased Efficiency</td>
</tr>
<tr>
<td>23</td>
<td>The Public-Sector Future of Interfacing With the Internet of Things</td>
</tr>
<tr>
<td>24</td>
<td>The Transformation of Public-Sector IoT</td>
</tr>
<tr>
<td>27</td>
<td>Why Sensor Data Collection Is Revolutionizing the Internet of Things</td>
</tr>
<tr>
<td>31</td>
<td>About &amp; Acknowledgments</td>
</tr>
<tr>
<td>04</td>
<td>QUESTION ONE</td>
</tr>
<tr>
<td>08</td>
<td>QUESTION TWO</td>
</tr>
<tr>
<td>16</td>
<td>QUESTION THREE</td>
</tr>
<tr>
<td>20</td>
<td>QUESTION FOUR</td>
</tr>
<tr>
<td>28</td>
<td>QUESTION FIVE</td>
</tr>
<tr>
<td>30</td>
<td>QUESTION SIX</td>
</tr>
</tbody>
</table>
“A couple of years ago, a lot of projects were just ideas, and the focus was on whether they were even possible. Today, nobody really asks whether IoT and smart cities are feasible. We know that it’s possible. Now, it’s more about how can we deploy this.”

Sokwoo Rhee,
Assistant Director of Cyber-Physical Systems, NIST
It’s easy to find ways in which the Internet of Things has affected private and consumer-facing enterprises — you probably have heard of the Nest thermostat or fitness devices that can monitor your movements, location and workouts throughout the day.

But the effect of the Internet of Things on the public sector is less concrete. What’s clear, though, is that today, after a lot of buzz, government is finally setting up programs and doing something with IoT, not just talking about it.

Some of you may still be asking: What is IoT? Simply put, IoT is a series of devices connected to one another via the Internet — and these devices can communicate with you through the information you enter or sensors you wear and operate. Most of it is automated, meaning these interactions can happen without your having to do anything.

So what does this mean for the public sector? And what programs are agencies and organizations developing to make use of this new technology? To ensure IoT’s success at your department, there must be a widespread understanding of what it means, how it works and how the technology could affect everyone from senior officials to entry-level employees.

That’s where this resource comes in. This GovLoop guide is meant to help you better understand these key issues by taking your six most-asked questions about the Internet of Things and answering them throughout the guide. You’ll also hear directly from the experts who play a role in developing the Internet of Things technology in programs and pilots at their organizations.

Want to know more? Let’s get started with Question 1: What is the proper definition of the Internet of Things?
What is the definition of the Internet of Things?

**ANSWER:**

The definition can vary, but a 2014 Pew Research Center report defined the Internet of Things as a catchall phrase for the array of devices, appliances, vehicles, wearable material and sensor-laden parts of the environment that connect to the Internet and to one another and feed data back and forth automatically.

It might sound simple when you put it that way, but it’s a big deal: Internet-connected machines are expected to number 200 billion by 2020, according to research firm IDC Corp. At that rate, these automated machine-to-machine transactions will outnumber human-to-computer transactions.

Need a concrete example? San Francisco provides one. The city has connected several thousand of its parking meters via sensors so that drivers, using an app, can find open spaces faster. To help get to a reasonable level of parking availability, the program and its parking sensors periodically adjust meter and garage pricing to match demand.

**Considering IoT Policy**

In 2015, the National Association of State Chief Information Officers (NASCIO) asked state chief information officers (CIOs) about IoT. While 53% of respondents said they were still investigating IoT with informal discussions, only 1 in 5 had moved to the formal discussion phase and zero states had adopted policies or developed an IoT roadmap.

Source: NASCIO report, The Internet of Things in a Connected State Government

**To what extent is the Internet of Things on your agenda?**

- NO DISCUSSION OF IOT AT THIS TIME - 23%
- STILL INVESTIGATING IOT IN STATE GOVERNMENT WITH INFORMAL DISCUSSIONS - 53%
- FORMAL DISCUSSIONS ON IOT APPLICATIONS, DATA COLLECTION, SECURITY - 18%
- IOT REFERENCED IN STATE IT STRATEGIC PLAN - 6%
- DEVELOPED IT ROADMAP TO GUIDE ADOPTION AND DEVELOPMENT - 0%
- ADOPTED IOT POLICIES, DATA, FRAMEWORK AND SECURITY CONTROLS - 0%
Sensor market spending, by customer agency, FY11-FY15

Defense agencies account for 88 percent of sensor spending from FY11 to FY15. DHS and NASA are the next largest buyers.

Source: Gours report: The Internet of Things: Sensors & Data Collectors

---

**DID YOU KNOW?**

IoT may seem like a new buzzword, but it’s been around for a while. In fact, in many ways, smart objects have been employed for decades. Some examples? Electronic wristwatches, car alarms and coordinated traffic lights. What today’s version of the IoT brings is a greater prevalence of smart objects and a higher connectivity between them.

**$9B**

Federal spending on IoT jumped 20 percent to almost $9 billion in FY15.

**56%**

Sensor spending has nearly tripled from FY11 to FY15, growing 56% in the last year alone.

**50B**

In 2008, there were already more Internet-connected objects than people. By 2020, that number is expected to grow to more than 50 billion objects, according to Cisco.

**$11T**

According to estimates by the McKinsey Global Institute, the IoT will have a total economic impact of up to $11 trillion by 2025.

---

**Further Reading**

- How the Internet of Things Could Transform Public Services
- The Internet of Things in government
- Driving the Internet of Things in the public sector
- The US government is pouring money into the Internet of Things
- Internet of things promises even more competition for vendors
- Report: Federal ‘Internet of Things’ Spending Up by 20%
- Uncle Sam’s IoT deadline
THINK BIG. START NOW.

Federal agencies cannot afford to have a network that holds them back.

Built on open standards, Ethernet fabrics, and a software-centric foundation, the New IP is an innovative approach to networking that empowers agencies to achieve the unlimited possibilities of the cloud, mobility, and Big Data.

Brocade: Your Partner for the New IP

www.brocade.com
#NewIP
Federal government is benefiting in a number of ways from the sensor-driven Internet of Things (IoT) – it’s enabled government to take advantage of traffic lights, sensor-monitored building facilities for power and energy conservation, and even drones on the battlefield.

However, with so much new information being processed, government is desperately in need of infrastructure that is capable of supporting all the data in various networks. That’s why everyone is talking about the New IP – network technology that is able to support IoT at the platform level.

In an interview with GovLoop, Stephen Wallo, Chief Federal Solutions Architect for Brocade, a technology company specializing in data and storage networking products, shared how the New IP can enable government agencies to better take advantage of IoT capabilities.

First, Wallo emphasized the need to address government’s current network architecture systems. “When you look at IoT, somebody has to manage all that additional information so the fundamental premise of the architecture also has to change,” he said.

The problem is with government’s tendency to cling to legacy infrastructure for security purposes, agencies are likely to add more hardware solutions to process the information. This, however, does not solve the problem. Wallo explained that in addition to the burden of keeping up with IoT networks, this adds operational cost expenses. Rather than having networks of IoT monitor themselves, agencies can be locked in with vendors they need to monitor such networks.

That’s why agencies need software-centric solutions. “Software-centric networks relate to universalizing environments,” Wallo said.

“Instead of having hardware boxes everywhere, virtualized network functions allow you to more easily place the service where you need it and when it is required. In addition, software-centric networks give you the agility and ability to easily accommodate new, incoming data.”

By simplifying and automating network processes, the New IP encourages innovation and accelerates speed of service delivery, allowing agencies to take advantage of mobility and gives them flexibility with cloud and big data technologies.

The software foundation of the New IP gives programmatic control over complex tasks as well as tight integration with organizational support systems and end user applications. It’s an agile platform that helps government embrace tomorrow’s innovations while maintaining strict adherence to security policies and considerations.

The second important component of the New IP is open standards. “This is about how you want people to gather the information and how you decide who’s supposed to see what,” Wallo said. Vendors need some common way to communicate amongst a variety of sensors. “The whole point of open standards is you enable different vendors to interoperate together,” he added.

The final component of the New IP is virtualization. Virtualization allows you to innovate on the spot and easily make any changes to your networks without needing to enlist the help of a vendor or your already busy workforce. “The more you can virtualize elements, the cheaper it is to be able to update or change software at a moment’s notice,” Wallo said.

Virtualization in IoT gives agencies more flexibility and agility with your networks by allowing an organization to be ecosystem-driven and more holistic. Moving beyond a dependence on single-vendor limitations helps government tap into the vast pool of resources needed to keep pace with private sector innovation.

Wallo said that, ultimately, the New IP opens the door to “best-of-breed” solutions such as security software that routes network-wide traffic based on a holistic infrastructure view and real-time alerts, rather than inefficiently routing traffic through proprietary legacy hardware. This allows government to build the network and services desired while moving faster and more efficiently.

Brocade provides a Five Step Network Innovation Model that allows organizations to take advantage of the New IP:

1. Audit existing technology to ensure it’s aligned with organizational goals and network priorities.
2. Implement automation that accelerates application delivery and reduces network downtime through an optimized cloud.
3. Increase agility by creating a service-oriented IT environment that enables real-time response to market change.
4. Take advantage of intelligent services and analytics to gain the insights that help speed change, reduce risk, and deliver innovation.
5. Understand that success depends on network modernization and innovation.

In order to modernize, government needs simplicity and cost-efficiency. That’s why innovations like the New IP are especially important in helping government acclimate to new IoT networks and technologies. When government focuses on software-centric platforms, open standards, and virtualization, the possibilities of IoT can be limitless.
How could IoT impact my life & job on a day-to-day basis?

ANSWER:

IoT affects your daily life in more ways than you may think. Whether you’re on your smartphone, exercising, commuting to work or doing your job, there is a whole array of machines and devices communicating with one another to make your day a little easier.

Imagine that IoT can help save you tons of time by making you faster at your job. Take the Financial Industry Regulatory Authority (FINRA), for example. FINRA helps the Securities and Exchange Commission analyze and store approximately 30 billion daily market events it receives from exchanges and U.S. firms. Tackling complex queries could take up to an hour-and-a-half. But with IoT, a system at FINRA can now tackle the query in five to 10 seconds. This translates to about $10 million to $20 million in annual cost savings for the agency.

According to Gartner Inc., the Internet of Things will include nearly 21 billion devices by 2020. That means whether it’s in government, the private sector or civilian life, you can be sure that IoT is impacting your daily life in some way, shape or form.

“Giving everyday objects the ability to connect to a data network would have a range of benefits: making it easier for homeowners to configure their lights and switches, reducing the cost and complexity of building construction, and assisting with home health care. Many alternative standards currently compete to do just that — a situation reminiscent of the early days of the Internet, when computers and networks came in multiple incompatible types.”

— Neil Gershenfeld, Raffi Krikorian and Danny Cohen writing on “The Internet of Things”

Here are 5 ways the Internet of Things directly impacts your daily life:

**TRANSPORTATION**
Thanks to LTE-enabled cars, you could now have more access to real-time traffic information and real-time vehicle diagnostics from your own car.

**HEALTH & EXERCISE**
Wearable technology like smartwatches and wristbands enable you to keep track of your personalized fitness data.

**HOME**
Security systems are tapping more into IoT to help you monitor your home from afar.

**WORK**
IoT is helping government provide better customer service experiences by tracking individual behavior and delivering individualized services.

**ENVIRONMENT**
Through aggregated regional and metropolitan data, IoT technologies now have capabilities to monitor the air quality outside of your home or office.
Glossary

Automation
The use of various control systems for operating equipment i.e. machines, telephone networks, and other applications with minimal human intervention (Wiki).

Sensors
Devices that detect and respond to some type of input from the physical environment, i.e., light, heat, motion or pressure. The output is usually a signal that is converted to human-reader display at the sensor location or transmitted electronically over a network for further processing. For example, in Las Vegas, the city uses sensors on water pipes that can sense and communicate if and when there is a crack or a leak. (Tech Target)

Long-Term Evolution (LTE)
Standard wireless communication of high-speed data for mobile phones and data terminals. Enables technologies to achieve 4G speeds, so that IoT can work to quickly communicate information between machines. (Digital Trends)

The Internet of Things offers a potential economic impact of $4 trillion to $11 trillion a year by 2026.

<table>
<thead>
<tr>
<th>NINE SETTINGS WHERE VALUE MAY ACCRUE</th>
<th>SIZE IN 2025, in $ trillion</th>
</tr>
</thead>
<tbody>
<tr>
<td>FACTORIES - e.g. operations management, predictive maintenance</td>
<td>low estimate</td>
</tr>
<tr>
<td>CITIES - e.g. public safety &amp; health, traffic control, resource management</td>
<td>0.14</td>
</tr>
<tr>
<td>HUMAN - e.g. monitoring &amp; managing illness, improving wellness</td>
<td>0.02</td>
</tr>
<tr>
<td>RETAIL - e.g. self-checkout, layout optimization, smart customer-relationship management</td>
<td>0.04</td>
</tr>
<tr>
<td>OUTSIDE - e.g. logistics routing, autonomous vehicles, navigation</td>
<td>0.06</td>
</tr>
<tr>
<td>WORK SITES - e.g. operations management, equipment maintenance, health &amp; safety</td>
<td>0.02</td>
</tr>
<tr>
<td>VEHICLES - e.g. condition-based maintenance, reduced insurance</td>
<td>0.02</td>
</tr>
<tr>
<td>HOMES - e.g. energy management, safety &amp; security, chore automation</td>
<td>0.02</td>
</tr>
<tr>
<td>OFFICES - e.g. organizational redesign &amp; worker monitoring, augmented reality for training</td>
<td>0.01</td>
</tr>
<tr>
<td>TOTAL: $4 TRILLION - $11 TRILLION</td>
<td></td>
</tr>
</tbody>
</table>

*Adjusted to 2015 dollars; for sized applications only; includes consumer surplus. Numbers do not sum to total, because of rounding.


Did You Know?
Of the 1,025 hours the average American student spends in the classroom per year, more than 300 are likely lost to interruptions like taking attendance, getting students’ attention or distributing materials. IoT can help eliminate such routine tasks, allowing teachers to shift time from classroom procedures to personal instruction. Imagine if attendance could be taken by having students wear smartbands that help them automatically check into classrooms. Or teachers could send a vibration signal similar to silent notifications on mobile devices to a student’s wearable or tablet, redirecting his behavior in a way that reduces direct confrontation and time wasted for the rest of the class.

Fun Fact:
In addition to smart cars that drive on their own, it is estimated that by 2020, there will be 10.2 million units of Internet-connected smart clothing.

Further Reading

How the Internet of Things is Changing Work
Transforming the Workplace
Connected Government and the Internet of Things
Industrial Internet of Things: Unleashing the Potential of Connected Products and Services

Learn why Information Builders gets the highest percentage of recommendations and the widest adoption rates of any analytics platform at informationbuilders.com/products/intelligence.

Data Integrity

Data Integration

informationbuilders.com

Connect With Us

WebFOCUS  iWay Software  Omni
In well-run organizations, responsibilities are often assigned from the top down. The president of the company delegates as much responsibility as possible to senior level executives. These executives follow suit, passing the same tasks down to managers, who eventually distribute them to individual workers. Within this well-oiled system, leaders “equip people, train them, give them authority, and empower them to execute the mission at their respective levels and communicate back up the chain,” explained Jake Freivald, Vice President at Information Builders, an integrated reporting and data access software company.

Ideally, the Internet of Things (IoT) should function the same way. IoT lets organizations push responsibility for local situations to the lowest level that can handle it, while providing an avenue to move collected knowledge back up to the highest level for strategic direction. With the right data analytics software, government agencies can rely on smart devices to run data collection at more granular levels, freeing human capital to focus on creative analysis and decision-making.

The reality is smart devices offer major benefits to government agencies.

We’re already seeing the benefits in healthcare. As costs have risen, healthcare providers are distributing care across different types of facilities. For example, patients can visit hospitals for major emergencies and reserve less severe issues for their primary care doctor or for a walk-in clinic. Having these options can help to manage costs and ensure that care is thorough, individualized and personal. But healthcare also needs to be managed centrally so providers can identify gaps in care, Freivald noted.

The best response is to rely on devices that can track previous care with great detail, relay the patient history back to healthcare providers and help doctors to measure treatment outcomes.

In addition to healthcare, smart devices can also revolutionize military operations. “A smart device can make it much more reasonable for logisticians to estimate where different kinds of equipment need to be and plan maintenance schedules,” Freivald explained. In time, the data provided by devices will even allow for predictive maintenance and placement schedules, based on past trends. IoT technology can get warfighters the equipment they need, ensure it stays properly maintained and even guarantee the lowest time delays and costs.

According to Freivald, a natural next step for government agencies embracing IoT involves monitoring their energy usage to become more energy efficient. Ideally, energy management will depend on feedback from devices at all levels. Individual devices can track their energy usage and pass that data to smart buildings. Buildings can aggregate those usage patterns and transmit them to energy providers who can engineer their utilities to match users’ needs. From there, government agencies can implement policies that support green solutions.

“With detailed information spread across every level of the organization, you can get a very comprehensive picture of what you can do to manage energy consumption more effectively,” Freivald said.

Energy management offers an enormous number of connection points and potential for information sharing because energy is a central feature in many activities. “We are using it, we are supplying it, and we are consuming it,” says Freivald, “and each one of those individual points is a place where we can understand our usage of energy better and adapt to changing conditions.” This innovation, and others like it, will have an enormous impact on making government agencies smarter and citizens better served.

Although the benefits of localized device reporting are significant, managing the system that centralizes the data can be a challenge. To make the most of IoT technology, large amounts of data must be collected from diverse sources in real time. This process alone can be messy, and the need to see the big picture — ideally in real time — further complicates matters.

However, the data analytics software that Information Builders provides can ease the burden of this analysis. Freivald highlighted the usefulness of integration technology that helps collect data and organize it in a helpful way. Information Builders, for example, seeks to enrich the data with information from other systems and then scrutinize the outcome with tools such as predictive analytics and visualizations.

At the end of the day, a network of empowered devices is only as valuable as the tools you possess to analyze the data, Freivald said. Agencies need access to real-time, high-volume, diverse data sources and the ability to extract meaningful insights from that data in a timely manner.
As IoT develops, local governments are employing new technologies to build smart, connected cities. One such example is Kansas City, Mo. GovLoop sat down with the city’s Chief Innovation Officer, Bob Bennett, to talk about how IoT is shaping Kansas City, what challenges they’re facing and what the future of smart cities looks like.
Bob Bennett views IoT as a means to better engagement with citizens.

“Deployment of technology makes the city maybe a cool city, but if you focus on people and data, that’s when you turn into a smart city … It’s all about making the city work more efficiently for citizens,” he said.

IoT provides cities an opportunity to keep up with changing citizen demands for connectivity. As technology becomes more and more prevalent in everyday life, citizens expect more connectivity throughout the city. Bennett acknowledged this, saying that keeping up with citizens is one of the biggest goals for cities now.

Kansas City has done a lot to keep up with its citizens. It has installed a two-and-a-half-mile streetcar line through the city’s downtown, with free public Wi-Fi covering 51 blocks surrounding the route, provided by a partnership with Sprint. Bennett offered an example of how this connectivity helped him: “I was able to walk out of my office one afternoon, start to download a presentation and by the time I walked about 16 blocks, it had downloaded. Never lost continuity the entire trip.”

Ten percent of that Wi-Fi bandwidth is dedicated to IoT devices, such as sensitivity light systems and people counters in the streetlights. The people counters can identify how many people are in a given area, allowing the adaptive light systems to dim the lights when there are no people nearby. Knowing how many people are in an area can also help the city prioritize services like police coverage or trash pickup. This data also provides insight into things like which areas have huge volumes of people but no restaurants.

The city has also installed 25 information kiosks connected to the public Wi-Fi. The kiosks provide information about where the streetcars are, allowing people to make more informed decisions about their travel plans. In addition, the kiosks offer restaurant reviews and recommendations, allowing people to make decisions about where to go communally. These kiosks had been accessed 14,000 times in the last month, said Bennett.

As one of seven finalists in the Smart City Challenge—which was recently won by Columbus, Ohio—Kansas City proposed a plan based on three pillars: transforming a proposed bus and rapid transit line in the eastern part of the city, building new autonomous vehicle corridors that would connect the eastern and western sides and establishing a series of community empowerment projects. The plan included implementing the same technology—the streetlights and sensors, free public Wi-Fi—that revitalized the downtown area in blighted neighborhoods in the east and creating an innovation center to catalog lessons learned so they could be shared with other cities.

With the growth of connected devices and cities, security concerns grow as well. Bennett explained how the city approached data privacy and security. Essential to security is the city’s partnership with Sprint.

“We have the benefit of having Sprint’s web security involved. And we’re the beneficiaries of their advances. Their R&D is significantly faster than a typical city procurement process,” he said.

The city will never see individual data from the public Wi-Fi, Bennett said. Rather, the city receives general, anonymized data about the general population in order to develop and adapt its strategies. This data is available on its open data site.

Bennett offered some advice for other governments beginning their smart city journeys. His first piece of advice is to “embrace the fact that cities can’t do this all by themselves.” Cities have to build and engage partnerships that transcend a single project. Cities are, however, obligated to respect citizens’ privacy.

Kansas City worked to achieve this by partnering with a local law school to establish a citizens’ bill of rights for data. Bennett emphasized, “You have to make sure you engage your citizenry to let them know what you’re doing and why you’re doing it.” His final piece of advice is to have a sense of humor and to “look at today’s failure as the impetus for tomorrow’s success because you’ve learned something along the way.”

In the future, Bennett imagines greater smart integration of the remaining departments, such as water and energy. There are advances happening, like a building that generates its own energy, that wouldn’t have been possible without smart technologies.

“I think that type of thing will grow as we get to the point where we’re being more efficient with the resources that we’ve been given,” Bennett said.
Transforming the Citizen Experience

1,800 public sector agencies use GovDelivery to connect with citizens

Our customers use GovDelivery to increase digital engagement, grow their digital audience by cross-promoting content, build communities around data, and create modern training experiences.

Learn more: govdelivery.com
Communicating with the Public Through Sensors and Technology

An interview with Richard Fong, Technical Implementation Consultant, GovDelivery

In the early 2000s, the social landscape looked vastly different. No Facebook. No Twitter. No Instagram. It would be quite a while until the first iPhone was introduced and acronyms like LOL, OMG and TTYL would enter the picture.

But today millions of messages are sent each day to connect with citizens around the world, and the public sector is more engaged than ever on social and communications platforms.

Behind it all, said Richard Fong, Technical Implementation Consultant at GovDelivery, a leading company in the public sector digital communications space, there is an acronym that is making an ability to engage with one another possible: API, or Application Programming Interface.

GovLoop sat down with Fong to discuss how APIs are currently interacting with the Internet of Things (IoT), enabling public sector organizations to automate communications with their citizens about everything from air quality issues to traffic conditions.

While a seemingly complex term, APIs are simply the middleman between a programmer and an application. In other words, APIs are a common boundary between a set of information and a user.

“Have you ever streamed a show on Netflix? Do you have an app that tells you when you could expect the next bus, or what traffic looks like?” asked Fong. “All of these examples use APIs to connect to an information source, approve the transfer of information, and then allow access for a user.”

Fong also discussed how public sector organizations could potentially use sensors as well to extend information to citizens through the reach of email and other digital communications using an example from Maricopa County, Arizona.

“In the Maricopa County area in the past few years, they’ve installed a series of sensors,” Fong explained. Their goal in doing this was to be able to measure the air quality and alert citizens if the quality was too poor to spend a significant amount of time outside. They then implemented a Rapid Response Notification System.

“Whenever a certain air quality level was discovered, they wanted to be able to alert citizens to stay inside, to not drive, and to not work outside if you had health issues,” Fong said. “This was all done in response to a federal mandate that said to get a particular amount of funding, you have to have some kind of notification system. So they came to GovDelivery.”

GovDelivery worked with the county and their sensor system to set up an automated email process related to poor air quality measurements. The air sensors send an email to county staff if the air quality reaches a certain limit. Once that information reaches a county staff member and it has been verified, the staff person will use their mobile phone to send a message to GovDelivery with the alert. GovDelivery in turn will send the message to that specific monitoring site distribution list.

“In essence,” Fong added, “it’s using automation to connect people and communicate to them in an efficient, automated way about really important topics. These sensors can gather information, relay an action, and part of that action is a communication to the public that helps them stay healthy.” The Maricopa County Rapid Response Notification System has 31,000 subscribers across 16 monitoring site distribution list.

Fong added that the ability for other organizations to use this sort of automated sensor communication is unlimited — natural resources departments could use it for alerts about water pollutants; departments of transportation could use it for traffic alerts; and much more.

The power of exposing resources via sensors or APIs is apparent for many organizations. There are APIs for mapping, weather, search, photos, data, stocks, and music. According to an article by ReadWrite, 75 percent of Twitter’s traffic is done via API and 60 percent of all tweets come from a third-party app.

“By extending the GovDelivery platform with APIs, we can expose various resources so a government agency’s system or application can communicate with GovDelivery via APIs,” Fong explained. “This matters because government can save time and reduce staff resources by automating tasks, everything from growing their audience, driving engagement, call-to-action messages, more informed citizens, eliminate errors, managing topics, and sending out alerts via email or SMS.”

“GovDelivery is processing more than 180,000 API requests per day and we are seeing this number growing as more government clients use our APIs,” Fong said. “As the world continues to evolve, so does the way we serve government and thus, how government communicates with citizens. Just imagine where we’ll be in another 15 years.”
What do I need to know about security & safety of the Internet of Things?

ANSWER:

IoT can enable government to improve efficiency, reduce waste and connect citizens to services in faster and more affordable ways. But with that value comes vulnerability. In a world that’s never been more connected, there is significant risk for security and data breaches since IoT can create targets and vulnerabilities. In fact, a recent Hewlett Packard report revealed that 70 percent of the most commonly used IoT devices, like phones and tablets, contain serious vulnerabilities.

That’s why it’s important to consider security, privacy and safety when it comes to the Internet of Things. Federal, state and local government employees increasingly need to use more devices, all of which connect with secure agency networks. This use of devices means that the device itself has to be secured along with the network.

To pair cybersecurity and IoT, there also has to be a change of overall mentality in federal agencies. Much of that different thinking involves working on shorter cybersecurity sprints that can evaluate critical holes in networks and devices, then patching them quickly enough to allow employees to keep working effectively.

An important tactic for addressing IoT and cybersecurity concerns is public-private partnerships, as emerging automated technology and devices are primarily derived from the private sector. Take the state of California, for example. The Economic Development Subcommittee of the California Cybersecurity Taskforce recently launched the CyberCalifornia initiative to help further the position of California as a leader in cybersecurity as it relates to commerce and IoT. CyberCalifornia will address IoT by helping to organize public-private partnerships in cybersecurity, facilitating research and innovation in cybersecurity, educating California businesses about cybersecurity needs and resources and connecting California’s robust workforce development system with the needs of California employers.

Many other security practices can also be leveraged, such as hardening IoT systems and using secure protocols for communication or installing the latest updates. Government also needs to consider that the future of security will be managed automatically by systems instead of users and start designing accordingly.

Glossary

**Bring Your Own Device (BYOD)**
Federal agencies are embracing BYOD policies so that government employees don’t have to carry multiple phones or tablets provided by their workplace. Devices include Apple and Android phones and applications, and employees are even starting to request Apple watches. While the BYOD movement is meant to embrace efficiency, there is also a significant security risk that government is trying to address with BYOD policies.

**Privacy**
Government has to be mindful of privacy and the way data is collected from citizens by sensors or mobile devices. It’s important that citizens should know what they are sharing and why and should never be surprised that government has certain information about them.

**Ecosystem**
A “smart” environment in which everyday objects/devices are embedded with network connectivity in order to improve functionality and interaction. Agencies need to be proactive in securing all devices and networks in an ecosystem. (KPMG International)

**FUN FACT:**
For a device to be labeled as IoT, according to the Internet of Things Global Standards (IoT-GSI), it must have seven design features: sensors, Internet connectivity, processors, energy efficiency, cost effectiveness, quality and reliability and security.
DID YOU KNOW?
Citizens are already concerned about IoT and security. At least 69 percent of U.S. consumers think they should own the personal data on all Internet-connected devices they own.

“If you look at where we’re going with Internet of Things, this is going to become more important than ever before. We used to think of things as a secure network of devices, and the network was kind of that security boundary. We need to flip that upside down and say, ‘really it’s a network of secure devices.’ Those devices become really important.”

Susie Adams, Federal Chief Technology Officer of Microsoft, in a recent MenTalk article

“As we willingly connect more data emitting things to third-party and public services, there is a greater likelihood that data can be used against us by bad actors, law enforcement, government agencies, and even insurers, contracted to act on our behalf. Critical factors for the success of the Internet of Things at scale are an informed public, sensible policy, and trusted service providers.”

Brenda Michelson, a self-employed business-technology consultant, in a recent Pew Study

Internet of Things Cybersecurity Market

Business Insider Intelligence estimates that by 2020, the U.S. Internet of Things Cybersecurity Market will be valued at $40 Billion (2015).

Further Reading

- Cybersecurity and the Internet of Things
- Internet of Things Global Standards Initiative
- State of the States on Cybersecurity
- The President’s National Security Telecommunications Advisory Committee (NSTAC) Report to the President on the Internet of Things
- Hewlett Packard Internet of Things Research Study 2015
Wish You Were Here.

When NASA needed a company to handle mission critical data from Mars - it turned to Amazon Web Services. Come see what AWS can do for your agency’s data.

AWS.AMAZON.COM/GOVERNMENT-EDUCATION/#IOT
Without the right support, making the most of the Internet of Things (IoT) can be a challenge. Even if devices are capable of sharing data, establishing a secure and effective network to collect and evaluate data is rarely easy. The impediments to success increase as the demands for larger and more scalable solutions grow.

At Amazon Web Services (AWS), a leading cloud platform provider, the answers to these problems have come in the form of connected solutions, said Sri Elaprolu, Global Lead for Public Sector IoT. By using a managed cloud platform, agencies can easily connect billions of devices, securely analyze the resulting data and do this cost effectively.

“The AWS IoT, a fully managed, scalable, and secure service from AWS for connected solutions, acts as the front door through which data comes in from devices, and customers have access to the broader AWS platform to be able to do data analytics, machine learning, and other types of information extraction processes,” Elaprolu said.

This approach shows a strong ability to help agencies create cost savings and increase efficiency. For example, some agencies are working to better manage utilities such as energy and water, allowing for smarter agriculture practices and more efficient water conservation. Others have focused on public safety by leveraging data from wearable devices such as body cameras.

Though current government organizations are successfully employing IoT technology in a wide variety of ways, via many different types of software, there is one common need: security. In an extensively connected system, each device is a potential entry point for a threat. That’s why AWS has made security a top priority.

“We want to make sure that any device that’s connecting to the service is something that you, as the application owner, have trust in and can rely on,” Elaprolu said. To ensure this level of protection, each connected device requires authentication or a credential. Data is encrypted, both in transit and at rest, and AWS even offers fine-grained control over the set of actions each device is authorized to perform.

Despite stringent security procedures, IoT remains flexible, offering government organizations options. AWS works with a number of third party solution providers, allowing them to build solutions on top of the AWS platform that can be leveraged by customers.

This style of collaboration has proven useful. The State Department awarded a multi-year contract to C3 IoT, an AWS Partner Network (APN) company. The company’s AWS cloud-hosted enterprise application development Platform-as-a-Service (PaaS) will allow the department to monitor and track energy consumption across 22,000 buildings around the globe, Elaprolu said. The resulting data will be analyzed to ensure energy use and consumption is optimized and used to predict maintenance needs. This project, according to Elaprolu, is just the beginning of government agencies using IoT to improve sustainability.

Collaborations between AWS and other IoT technology companies have worked on a smaller scale as well. The government-run Technology Strategy Board in the U.K. is funding a project called the Smart Airport Experience at the London City Airport.

“Our goal is to enable customers with a flexible and secure technology platform, so they can provide their users with the best possible services. In the case of airports, it’s providing a smart airport experience to travelers, improving overall operational efficiency, and allowing customers to do simple things like fast check-ins,” Elaprolu explained.

AWS is also smoothing commutes on the ground. With the help of Spectrum, a third-party solution offered by an APN member, existing traffic light software can be upgraded to give traffic feedback. Traffic lights and cameras record information about street use and signal maintenance. This real-time feedback makes it easy for transportation departments to identify broken lights without relying on citizen complaints. By applying analytics to the captured data, cities are optimizing traffic signal timing to manage the flow of cars in real time.

Similarly, the Boston Mayor’s Office of New Urban Mechanics is using a mobile app that tracks bumps on the road using your device’s accelerometer and GPS. The data is collected in real time, allowing the city to better decide which streets need to be repaved. For Elaprolu, these are just additional examples of how connected devices can collect data and agencies can “use the cloud to aggregate it, analyze it, and react to it, as soon as possible.”

The public sector is often slower to adopt new technology trends, even when private industry embraces them enthusiastically. But IoT is different. Governments at all levels are sharing their excitement about the prospects for their own connected solutions, Elaprolu said: “IoT is a fast-emerging space, and we’re seeing a lot of excitement around its capabilities both in the U.S. and abroad.”
How is the Internet of Things being regulated, if at all?

ANSWER:

Instead of a unified policy, IoT regulations and standards have generally fallen to individual agencies. This is not for a lack of attention. In January 2015, Reps. Suzan DelBene and Darrell Issa created the Congressional Caucus on the Internet of Things. That month, the Federal Trade Commission (FTC) published a report on privacy, security and IoT. In February that year, there was a Senate hearing examining IoT. In March, the Senate passed “The Internet of Things” resolution.

The product of all this attention? A general agreement that IoT devices should be secure without a consensus on whether a unified regulatory strategy is necessary. At a U.S. Chamber of Commerce event in February 2016, FTC Commissioner Terrell McSweeny focused on the importance of having strong, voluntary self-regulation and security frameworks that aren’t “overly prescriptive.” Instead of a global strategy, individual agencies, such as the Food and Drug Administration, are developing their own IoT and data-privacy standards to guide companies and devices.

Globally, IoT is also attracting attention. The Global Privacy Enforcement Network, a group of data-protection authorities from different countries, examined the privacy practices of IoT devices and companies during its 2016 Global Privacy Sweep. In April 2016, the European Parliament approved new data-protection regulations, setting a uniform level of data protection across the EU and giving citizens greater control over their personal data.

From an industry perspective, several groups, such as the Open Interconnect Consortium and AllSeen Alliance, are emerging with competing IoT standards. However, IoT is a massive industry, ranging from thermostats to drones to street-light sensors and encompassing many layers of technology. This variance creates a challenge to easy regulation and universal standards.

However, some progress is being made. In May 2016, the Senate Commerce Committee passed the Developing Innovation and Growing the Internet of Things (DIGIT) Act, which would create a working group to identify proposals to facilitate IoT development.

Top three recommendations from FTC’s Internet of Things: Privacy and Security in a Connected World:

DATA SECURITY:
IoT companies should ensure that their devices are physically secure.

DATA MINIMIZATION:
Companies should only collect the necessary personal data from citizens.

NOTICE AND CHOICE:
Citizens should have the opportunity to choose what personal data is shared, and they should be notified if there is a data breach.
The several layers & components of IoT technology make it difficult to institute a cohesive set of standards.

Source: Cisco, 2015

“... there’s an underlying mismatch between the way the government handles issues and the way this new technology actually works. Government operates in silos ... The IoT is precisely the opposite. It is a freewheeling system of integrated objects and networks, growing horizontally, destroying barriers so that people and systems that never previously communicated now can.”

Source: Politico, “What Washington really knows about the Internet of Things”

FTC Report Findings

According to the FTC’s report, “[c]onsumers are more likely to buy connected devices if they feel that their information is adequately protected.”

A majority of consumers uninstalled an app because of concerns that it was collecting too much personal information or that they did not install the app in the first place.

87% 87 percent of consumers worry about the type of data collected through smart devices.

88% 88 percent want to be able to control that data.

NTIA Public Notice

The National Telecommunications and Information Administration (NTIA) published a public notice in April 2016, asking for input “from all interested stakeholders” on “what role, if any, the U.S. Government should play” in the IoT landscape.

The notice received over 130 comments from organizations, including:

BOOZ ALLEN HAMILTON
ELECTRONIC FRONTIER FOUNDATION
IBM
MICROSOFT
UNIVERSITY OF MICHIGAN

Further Reading

Internet of Things: Privacy and Security in a Connected World

Senate Resolution 110, a resolution expressing the sense of the Senate about a strategy for the Internet of Things to promote economic growth and consumer empowerment

DIGIT Act

Laws that can apply to IoT

Children’s Online Privacy Protection Act
Federal Trade Commission Act
Fair Credit Reporting Act
Health Information Technology for Economic and Clinical Health Act
OSIsoft enables agencies with real-time, actionable, and predictive operational intelligence from all sensor-based data to be more:

- Cost Efficient
- Reliable
- Secure
- Scaleable
- Interoperable

Learn how agencies are fully harnessing the potential of sensor-based data and the Internet of Things at OSIsoft.com/Federal
The Internet of Things (IoT) has caused an explosion of sensors and connections across all industries – in fact, prominent think tanks and consultancies have predicted that 50 billion devices will be connected to the Internet by 2020. IoT has also received attention in the public sector because of its potential to disrupt and radically change the way agencies do business. Endpoints are getting smarter and smaller, sensor costs are dropping radically, and wireless networks continue to expand capacity. As a connected enterprise, how will government agencies capture this data with their infrastructures and make it decision ready?

To discuss more about how the public sector can properly interface and interact with this new world of data and sensors, GovLoop sat down with Steven Sarnecki, Vice President, Federal & Public Sector, and Stephen Bates, Director, Advanced Analytics at OSIsoft, an industry leader in operational intelligence and advanced data analytics for over 35 years.

“IoT is about an explosion of sensor data,” said Sarnecki. “And as sensors become more common, not all of them will be based on modern standards. Some of them will be older or unique and not modernized. But at OSIsoft we feel very strongly that any IoT or analytics solution has to be a complete solution that can integrate all sensor data and technology.”

In short, if sensors are not standardized, and IoT data is disseminated across a variety of silos, accurately identifying how and where to improve operations and make better decisions can be extraordinarily challenging. Data needs to be funneled into a centralized system for it to be of real value; if it is not and data that holds answers is scattered among different incompatible systems, formats and processes, it becomes very difficult to achieve any sort of insight.

That’s where OSIsoft’s PI System comes in. The platform uses operational intelligence, or historical and real-time insights from data, to connect and aggregate sensor-data from disparate vendors and control systems to enable real-time decision-making and security improvements for critical equipment and facilities.

For years, Bates explained, sensor-based data has provided visibility and information to support decisions influencing the control, design and management of industrial operations. Today, the lower cost and increased connectivity of sensors are making it cost-effective for organizations to extend that reach into remote or mobile monitoring of geo-dispersed assets. Connecting IoT to the PI System enables organizations to integrate IoT data with existing operational data to close information gaps, sharpen insights and create new business models.

“The PI System aggregates large amounts of data, very rapidly, and it enables frontline managers, senior managers and other stakeholders to visualize that data,” said Bates. “And when data is visualized, whether it’s operational data, process data, or geospatial data, agencies can immediately see value – value now, and value over time.”

But it’s not necessarily an easy path. For much of the public sector, Sarnecki explained, a full-scale IoT approach to data capture, integration and storage to drive enterprise performance is neither practical nor cost-effective. The reality of today’s public sector world is that technology is already in place to monitor many mission-critical machines and key operational processes. While newer “smart” machines may include embedded sensors, it is more cost-effective to extend the lifecycle of existing assets using existing technologies. Deriving value from IoT will more likely mean finding ways to capture and store data from new technologies, sources and open networks and integrate this with pre-existing sensor-based data systems.

To overcome these challenges, partnerships between vendors, government and service providers will be required to build systems to capture, integrate and distribute IoT and sensor-based data in a way that aligns with mission critical objectives and creates revenue-bearing deliverables.

The PI System can help government to optimize processes and receive data driven efficiency insights. With greater demands and efficiency challenges, the PI System will help the public sector capture, aggregate, share and visualize data that can be analyzed across an enterprise. It allows real-time data transmitted from sensors to be aggregated and turned into actionable data. That powers insights and situational intelligence.

“Data is inherently useful,” Bates said. “But it becomes really valuable when it adds context, and then becomes information. In turn, when that information enables better decision making, it becomes intelligence.” With this helpful context and the right intelligence tools in place, both systems and humans can make better data-driven decisions that benefit citizens and the overall agency’s mission.
The Transformation of Public-Sector IoT

An interview with Sokwoo Rhee, Assistant Director of Cyber-Physical Systems, NIST

The Internet of Things relies on innovation, creativity and imagination. Organizations that promote those characteristics can develop effective new programs that can change lives. That’s what the National Institute of Standards and Technology (NIST) is doing with its Global City Teams Challenge (GCTC), a program dedicated to bringing together leaders in the public and private sectors to develop new IoT applications for smart cities.
GovLoop talked to Sokwoo Rhee, Assistant Director of Cyber-Physical Systems Program at NIST, about projects developed through GCTC, how IoT has changed and where it is going.

Rhee said he divides the IoT landscape into three sectors. The first sector is consumer applications, which includes items like Fitbits or other wearables. The second is industrial applications, such as factory automation and productivity improvement. The third is public-sector applications, including smart city technologies.

GCTC fits into the third sector. The program brings together local governments, industries, nonprofits and academics into “action clusters.” These teams develop IoT projects that have quantifiable goals, such as reducing the average commute time in a city by 35 percent or decreasing the level of air pollution by 20 percent.

Rhee said that each team works with at least one city and three to five technology providers to implement its project idea. The most recent phase of GCTC had around 90 teams from 14 countries, working in 120 cities with around 300 technology providers. Almost 2,000 people attended the GCTC Expo in June 2016, making it one of the largest smart city events in the country.

The projects cover a wide array of issues, including transportation and public Wi-Fi. For example, when implementing autonomous vehicle projects, other issues arise: How do you ensure that the vehicles are taking the best possible route? How can you spread the vehicles across the city so there isn’t a traffic jam? A project based in Columbus, Ohio, worked to address those issues.

Another project, LinkNYC, worked to replace phone booths in New York City with structures that provide free Wi-Fi, device charging and phone calls. The project generates revenue through advertising. Air-quality monitoring, water management, crime prediction and disaster relief are also popular projects, Rhee said.

The variety of projects at the expo shows how much IoT has changed over the past few years.

“A couple of years ago, a lot of projects were just ideas, and the focus was on whether they were even possible. Today, nobody really asks whether IoT and smart cities are feasible. We know that it’s possible. Now, it’s more about how can we deploy this,” Rhee said.

Another major change is the growing involvement from municipal and local governments. In the past, IoT was primarily a project by technology providers, but now cities are taking greater leadership roles. In addition, by partnering with the private sector, cities can now implement new projects without a large financial commitment.

“For example, universities are working very closely with cities, and a lot of universities already have some kind of funding,” said Rhee. “A city’s role in that case is providing the venue where a university can test their research and create the real benefit.” A similar move is happening with private industries. “It’s not just about technology anymore; the companies are actually creating new models. They’re not selling only the products anymore. They’re offering the whole solution and business model, so cities can adopt them without too much effort upfront,” he said.

Government agencies have shown greater interest in IoT and smart cities, but the majority of projects are one-off endeavors, customized to individual cities. In the future, Rhee sees IoT focusing more on scalable and replicable models for deployment: “There are about 19,000 cities in the United States alone, and the majority of those cities do not have either the resources or technical expertise to take on the major smart cities projects.”

Rhee said there will be a focus on replication of successful solutions and economies of scale, and NIST in particular will work on developing systems of measurement. He explained why this was important: “If you want to replicate any program, the first question the cities are going to ask is, ‘What is the impact?’ So you have to understand what the investment is and what the outcome is. There’s a lot we can do to improve the measurement of the impact.”

For anyone hoping to implement IoT programs, Rhee recommends thinking about the application and benefits of such a program first.

“For the last 20 years, the IoT industry has worked in the opposite direction, starting with the technology development without understanding what the application is. That time is over,” he said.

In the end, smart cities are about improving the lives of citizens, and the shifts in public-sector IoT reflect that.
A DATA ANALYTICS PLATFORM FOR INTERNET OF THINGS

ViON's DataAdapt Platform accelerates the data discovery of IoT through:

• Accelerated data ingest
• Agile processing workflows
• Data analytics for greater insights

Learn more: www.vion.com/dataadapt
The rise of the internet led technology companies to build products capable of data collection that were designed for personal use. This development resulted in a “bring your own device” system, or BYOD. Individuals used their laptops, and eventually their tablets and smartphones and other devices to collect data and connect to other devices, creating the Internet of Things (IoT).

Today, IoT has moved the connected world beyond BYOD to incorporate new sensors and other embedded platforms. Traditional data collection generally required direction from individual users, unlike sensors, which can be programmed to record data without requiring expertise or interaction. By liberating data collection from users, the number of connected devices increases, and the accompanying supply of information grows exponentially.

As sensors are exponentially increasing the volume of data points that are collected, organizations today must have a system, platform and process in place to organize this data in order understand and act on it.

The use of sensors will be revolutionary, explained Clint Green, Director of Advanced Analytic Strategy and Development at ViON, a leading data management company. “The ability to connect a diverse set of systems so they can communicate over a standard set of protocols locally and globally, is going to be applied to systems in the physical world that had never before been connected,” he said.

The technology advancements that enabled sensors are not only changing how we collect data, but also how we analyze our data sets and use human capital. For example, traditionally, doctors have written or dictated their notes on patients by hand, and then later others transcribed these notes and manually entered them into a specialized database. Now, with help from health sensors, this information can be automatically recorded and analyzed.

These types of flexibility are some of the greatest benefits from a sensor-driven IoT for Green. “That’s where it takes the human out of the loop, out of harm’s way, out of the lower level tasks of data capture, and allows people to move to more efficient and effective uses of their limited time and resources,” he explained.

This newfound ability gives agencies the opportunity to build a far richer view of the world, but only for those prepared to make the right investments in the collection and organization of this data. Many agencies mistake the small scale of each new individual IoT source as not requiring large scale solutions, only to find themselves unable to scale in the future.

To capitalize on IoT data, agencies need a solution that can manage the complexity and scale of data collection and organization, while providing the visibility needed to understand and act on the data they have collected. Without the right tools, agencies can’t fully benefit from the increased availability of data through sensor collection.

ViON manages these concerns by providing a centralized solution blending systems integration, networking and big data analytics capabilities. This combination helps ensure that agencies have the system, platform and process to analyze and respond to their data. This centralized method both reduces costs and improves service delivery.

“People often say that 80 percent of the data scientist’s time is spent getting organized and understanding the data, and only 20 percent is acting on the findings,” Green said. The best way to cut down on time spent arranging data is to invest in a strong and robust infrastructure to enhance collection and organization processes. When accompanied by big data tools to promote descriptive, diagnostic, predictive and prescriptive analytics, the supporting solution ensures agencies can make the most of their sensor data.

“The ViON advantage for our customers,” explained Green, “is our steady-handed focus on the mission or business outcome that the customer needs.” Included in that focus is an acute awareness that the size of IoT systems will only continue to grow as new devices are outfitted to join the network. For this reason, ViON solutions emphasize delivering scalability and security from day one.

ViON’s managed services approach can be especially helpful for government agencies who must collaborate with a multitude of vendors, geographies and technologies within their IoT infrastructure. The simplicity provided by a single consistent interface makes it much easier for agencies to embrace the power of IoT.

When you have a managed system that is able to collect and organize the massive amount of data from IoT, only then will agencies be able to understand and act on this information. An investment in a system of sensors and data processing software can be used in multiple applications, both for an answer today and to provide context for the questions of tomorrow.
**QUESTION FIVE**

Who are the people & organizations involved with IoT I should know?

**ANSWER:**

IoT is a wide-reaching field, affecting industries, agencies and citizens in a variety of ways. Because of this dispersed nature, navigating relevant people and organizations as you develop your IoT strategy can be challenging. In order to make your job easier, here are a few federal, state and local leaders and organizations who are influencing the IoT landscape as well as some of the major private-sector players.

**Federal Leaders & Organizations to Keep an Eye on:**

**NATIONAL TELECOMMUNICATIONS & INFORMATION ADMINISTRATION (NTIA)**

The NTIA has an Internet Policy Task Force. It highlights events and blogs related to IoT, and the administration will produce a paper based on public comments about what the government’s role in IoT should be.

- **Terrell McSweeney**
  As FTC Commissioner, McSweeney approaches IoT as a balance between protecting consumers and promoting innovation. She has said that the FTC is not likely to produce strict standards and calls for self-regulation instead.

- **Edith Ramirez**
  Ramirez, the Chairwoman of FTC, emphasizes data transparency and security when it comes to IoT. She has called for greater clarity on data collection and more education of privacy practices.

**FEDERAL TRADE COMMISSION (FTC)**

Through its protection of consumers, FTC has a direct role in regulating how IoT companies can deal with citizens. Agencies can use its 2015 report for general security standards for IoT.

- **Terry Virts**
  Virts approaches IoT as a balance between protecting consumers and promoting innovation. He has said that the FTC is not likely to produce strict standards and calls for self-regulation instead.

- **Edith Ramirez**
  Ramirez, the Chairwoman of FTC, emphasizes data transparency and security when it comes to IoT. She has called for greater clarity on data collection and more education of privacy practices.

**NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)**

NIST may call IoT by a different name — cyber-physical systems (CPS) — but it’s shaping the landscape in several ways. First, it has a working group to prepare a CPS framework with definitions and guidance; the group released a draft in September 2015. NIST laboratories are researching and developing new programs and standards for CPS technology.

- **David Wollman**
  Wollman, Deputy Director of NIST’s Smart Grid and Cyber-Physical Systems program, has been working to develop the agency CPS framework. Incorporating the multitude of domains that IoT affects, however, has been challenging.

- **Sokwoo Rhee**
  As the Associate Director of Cyber-Physical Systems at NIST, Rhee leads the Global City Teams Challenge, which works with dozens of cities across the globe. He views IoT as a concept or an enabler instead of an industry and finds IoT’s value in the services built on connectivity.

- **Sokwoo Rhee**
  As the Associate Director of the Cyber-Physical Systems Program at the National Institute of Standards and Technology (source)

“**A lot of people think that IoT is all about sensors and chips and radios, and a lot of manufacturers think that it means they are going to sell more chips. But that’s probably a very small piece of the whole IoT value. The real value comes from establishment of services on top of the connectivity; that’s where the value is going to be.”**

**State & Local IoT Leaders**

**HARDIK BHATT**

Bhatt is the CIO of Illinois and the Secretary Designate of the Department of Innovation Technology. He is leading a drive to make Illinois the first “smart state” and aims to develop IoT adoption statewide by bringing new tech companies to the state, using IoT to improve state operations, and incorporating the technology at local levels as well.

**ROB PHOCAS**

The Energy and Sustainable Manager for Charlotte, N.C., Phocas works with Envision Charlotte on the board of directors. Envision Charlotte is a “public-private plus” partnership that brings smart technology to the city to promote economic and environmental sustainability. The program has used connected technology to cut power consumption by 8.4 percent since 2011.

**NATIONAL ASSOCIATION OF STATE CHIEF INFORMATION OFFICERS (NASCIO)**

NASCIO provides a network for state CIOs to exchange information and promote best practices. As IoT has developed on the state level, NASCIO followed its progress, eventually publishing a policy brief that covers the current landscape, potential trends and guidance.
The Department of Transportation is one of the leading agencies in IoT adoption and support. Its Smart City Challenge promotes innovative connected technologies in the local transportation infrastructure. Out of 78 applicants, seven cities emerged as finalists, leading the way in implementation of IoT and connected vehicles. The finalists presented final pitches to Secretary Anthony Foxx in June.

Source: https://www.transportation.gov/smartcity

1400 local officials, companies, academics and non-profits joined their webinars

300 companies have expressed interest in partnering

7 Smart City Challenge finalists announced in March at SXSW

800 people participated in their Smart City Forum

78 applications received for the Smart City Challenge

1 Smart City Challenge winner: Columbus, OH
How should I get started at my agency with the Internet of Things?

1. FIGURE OUT YOUR PROBLEM FIRST – THEN APPLY IOT.
Dr. Michael Chui, a partner at the McKinsey Global Institute: “First, go through your agency and think: If you could continuously measure something that was core to your agency’s mission, what would that be? How would that allow you to provide your services? How would it solve problems for your citizens? Then, after you’ve figured that out, seek out IoT solutions — not the other way around.” In short, start with a practical application or need, then figure out whether IoT technologies have a role to play.

2. DON’T FORGET ROI.
It’s important to spend some time early on thinking about risk and ROI. Before forming large-scale partnerships on IoT investments, consider demonstration projects that can help prove your business case and better inform questions about risk allocation. Remember that IoT is an evolving field, and the path to a public-private partnership is not always clear.

3. BE AGILE — AND USE PROTOTYPES.
Dan Hoffman, Montgomery County Chief Innovation Officer: “Don’t get sold on a product. Don’t just go buy a product because you got a good sales pitch off it. I would say, look to pilot, look to prototype something. Get some devices quickly, test them out, figure out how it would work and then move forward in that iterative fashion. But, you know, sometimes these projects die because upfront we decide, ‘Oh this is great, and I know that I want to budget money for this and because procurement in government is often a time-consuming challenge, I’m just going to plunk down X number of dollars to build out my safe community network or whatever they want to call it.’ You know, it’s those kinds of big, slow procurement actions that fail because by the time you get the technology, it’s out of date. By the time you install it, you realize it’s not quite right or that it’s not quite what you need. By taking that agile, iterative approach, we can shift gears, we can learn what works without having invested millions of dollars into something. Sail fast and figure out what works.”

4. FAIL EARLY AND OFTEN.
Using sensors and ecosystems for simulation training requires employees to learn from mistakes and failures. To not be afraid of failure means trying new experiences. There are things that go right, there are things that go wrong. But you’ll learn in an amazing amount of time just by designing, implementing and then learning from that experience.

5. THINK ABOUT THE USER FIRST.
Keep the user as the central focus when creating new IoT sensors. The simpler you can make the interface, the better.
About GovLoop
GovLoop’s mission is to “connect government to improve government.” We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 250,000 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 connect and improve government.

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

www.govloop.com | @GovLoop

Thank You
Thank you to Amazon Web Services, Brocade, GovDelivery, Information Builders, OSIsoft and ViON for their support of this valuable resource for public-sector professionals.

Authors
Catherine Andrews, Director of Content
Francesca El-Attrash, Staff Writer
Sonia Chakrabarty, Editorial Fellow

Designer
Kaitlyn Baker, Graphic Designer