The Internet of Things:

Challenges & Opportunities in Government

It's clear that the Internet of Things is becoming a reality in the public sector. Our questions: What role do we see government playing in this new arena and what obstacles are currently holding it back?

Contents

04 Executive Summary

05 Meet the Experts

06 Map of IoT Successes

11 Scaling the Internet of Things with Cloud Technology

15 Helping Government Agencies Embrace IoT Technology

19 Evolving the Digital Workplace with the Internet of Things

23 Communicating with the Public Through Sensors and Technologies

26 Conclusion

27 About & Acknowledgments

CHALLENGE # 1 08 SECURITY

CHALLENGE # 2 12 PROCUREMENT

CHALLENGE # 3 16 REGULATION

CHALLENGE # 4 20 WORKFORCE

CHALLENGE # 5 24 BROADBAND & INFRASTRUCTURE

Executive Summary

Through the integration of computers, sensors and networking in physical devices, the Internet of Things (IoT) fuses the physical and digital worlds to develop new capabilities and services, which in turn create new jobs, businesses and opportunities.

IoT is, after many years of development and pilot programs, starting to truly take off in the public sector. The technology is creating opportunities in everything from public transportation to workplace automation to public safety efforts. But even as IoT programs expand across government, the public sector faces some very real challenges in deploying this new technology.

IoT led the world to incorporate new sensors and other embedded platforms for connection. Traditional data collection generally requires 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 exponentially increase the volume of data points collected, governments today must have a system, platform and process in place to organize this data in order understand and act on it.

This shift presents several challenges for government. As with many new technologies in the public sector, security is a massive challenge – each device that is connected increases privacy and security concerns. Acquisition is also a hurdle – today's procurement policies often make it difficult for agencies to quickly and easily adopt the technology. Additionally, the regulatory framework around IoT is not well-defined, leading to murky standards and disparate data. Finally, the lack of skilled workers who understand IoT technology and the need for more robust infrastructures to support the technology are also obstacles that need to be dealt with.

Until government is able to address and overcome these challenges, the adoption of IoT may remain limited within the public sector.

That's why we've created this new GovLoop guide, The Internet of Things: Opportunities and Challenges in Government. We'll explain those challenges, help government understand why they are occurring and talk to government experts about the best ways to break through obstacles to realize the full potential and promise of the Internet of Things. Additionally, we'll detail the main challenges facing the government in the use of IoT and offer up solutions for overcoming them.

MEET THE INTERNET OF THINGS EXPERTS

For this guide, GovLoop interviewed several IoT leaders from federal, state and local government, as well as the private sector. You'll find their insights, advice and knowledge woven throughout this guide. Here's who we talked to and a little bit about each of them:

NABA BARKAKATI

Chief Technologist at U.S. Government Accountability Office

Barkakati serves as GAO's spokesperson on issues involving technical matters in the areas of information systems, systems development, information security and assurance, and land/air/space-based advanced technologies and exercises the responsibility for presenting testimony on technical matters at congressional hearings and for representing the GAO. The GAO recently released a report about IoT, "Internet of Things: Status and implications of an increasingly connected world."

SOKWOO RHEE

Associate Director of Cyber-Physical Systems Program at NIST

Rhee currently leads the Global City Teams Challenge (GCTC), which aims to create a replicable and scalable model for collaborative incubation and deployment of IoT and Cyber-Physical Systems (CPS) solutions to improve the quality of life in smart cities around the world. He previously served as a Presidential Innovation Fellow on CPS, a program by the White House Office of Science and Technology Policy. During his fellowship, he co-led the Smart America Challenge, which brought together IoT technologies and CPS across the nation to demonstrate concrete examples of their socioeconomic benefits.

JASCHA FRANKLIN-HODGE

Chief Information Officer, city of Boston

Mayor Martin J. Walsh appointed Franklin-Hodge Boston's Chief Information Officer in June 2014. As Chief Information Officer, Franklin-Hodge leads the city's efforts to enhance online service delivery, empower employees with effective digital tools and improve access to technology and the internet for all Boston neighborhoods. Boston is currently preparing for a major $10 million broadband and core infrastructure expansion with the aim of supporting more IoT initiatives in the city.

JOSEPH WILLIAMS

Director of Economic Development for the Information and Communication Technology Sector, Washington state

Williams is a veteran of Microsoft as well as Sun Microsystems and was also recently dean of the School of Business, Government, and Economics at Seattle Pacific University. In his current role, he provides the governor and Legislature with insights into events and policies that affect the state's tech industry.

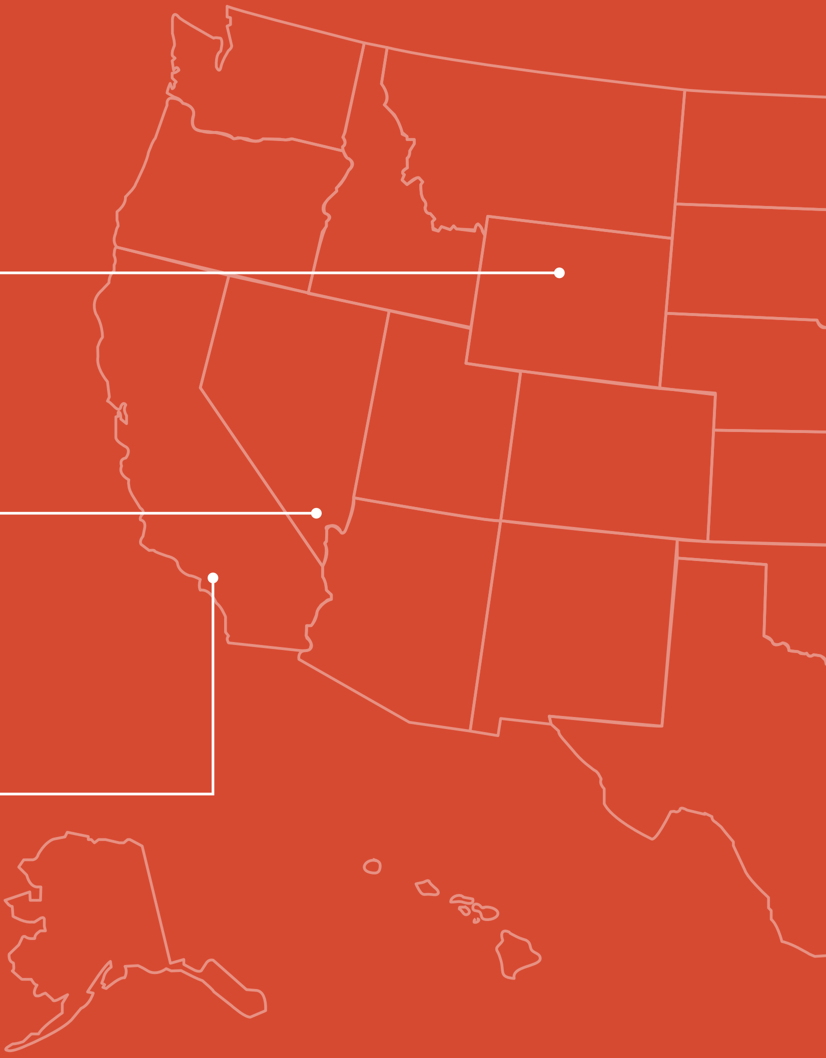
JOSHUA NEW

Policy Analyst at the Center for Data Innovation

New's research at the center focuses on methods of promoting innovative and emerging technologies as a means of improving the economy and quality of life. New has written or co-written several Center for Data Innovation reports on IoT, including the 2016 report "How Is the Federal Government Using the Internet of Things?"

Map of IoT Successes

The use and adoption of IoT has skyrocketed across the public sector in the past few years. Take a look at this map to learn about a few of the programs developing across the country.



WYOMING

Wyoming is testing a new communications system in its busy I-80 freight corridor that will give truck drivers automated alerts about weather, traffic and collisions.

LAS VEGAS, NV

The city's water system implemented an IoT monitoring platform that combines proven acoustic leak-detection technology with wireless connectivity and visual end-user dashboards to create a cost-effective monitoring solution.

LOS ANGELES, CA

The city and the California Institute of Technology (Caltech) developed a project called "Quake Alert," which uses sensors to detect the nearly constant tremors in the area.

INDIANA

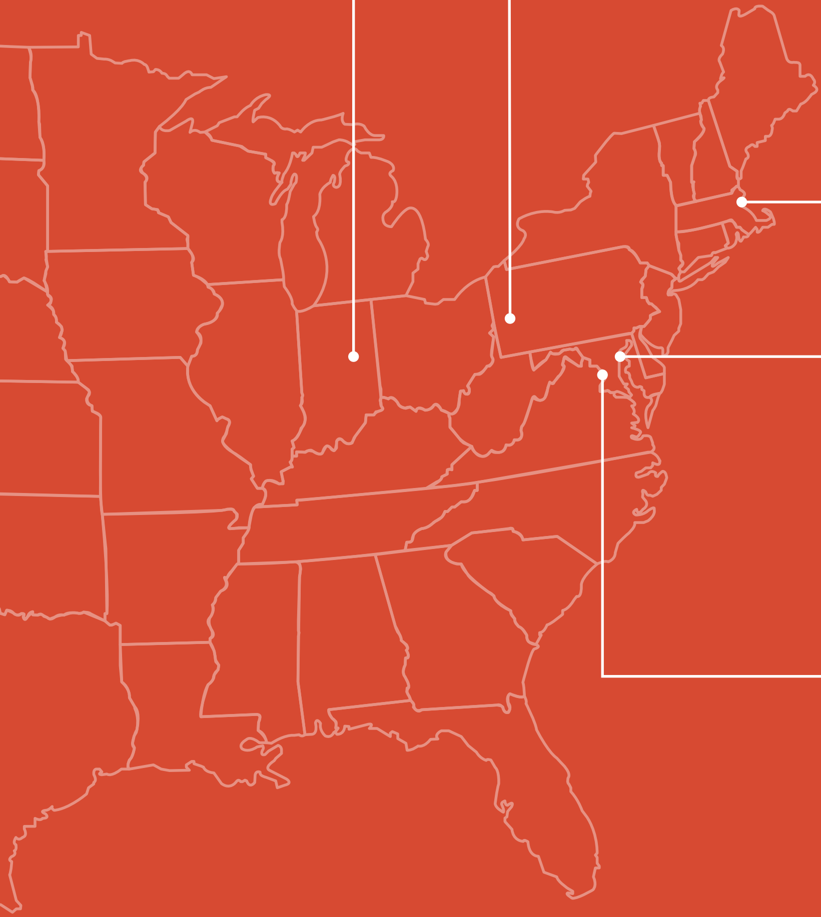
Just outside of Indianapolis, the first Internet of Things lab in the state of Indiana has recently been announced. With 24,000 square feet, the space will offer room for meetings, ideation and a makerspace.

PITTSBURGH, PA

The city is using smart lighting powered by IoT to reduce energy and costs and to keep the streets across all neighborhoods – wealthy or poor – equally lit to improve safety.

BOSTON, MA

The city has used sensors to pilot a smart parking program, where it installs smart meters that calibrate prices according to the time of day and driver demand.



BALTIMORE, MD

The city introduced new water meters that can measure how much water a customer uses hour by hour and beam back information to the water department wirelessly to ensure more accurate billing.

WASHINGTON, DC

Lots of federal agencies are using IoT, but one that stands out is the General Services Administration. For the past few years, it has been experimenting with a network of sensors in its building meant to cut energy use and wasted resources in its facilities management.

CHALLENGE # 1

Security

There have been multiple predictions over the years that there will be tens of billions of connected devices – if not more – by 2020. But each device that is connected increases privacy and security concerns surrounding IoT. These concerns include hackers stealing data and even threatening lives and more. How can governments prevent attacks on connected systems and maintain the privacy of their citizens' data?

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 because IoT can create a massive number of targets and vulnerabilities with every connected sensor or technology that is deployed.

As a recent GAO report on IoT states, "IoT brings the risks inherent in potentially unsecured information technology systems into homes, factories, and communities. IoT devices, networks, or the cloud servers where they store data can be compromised in a cyberattack. For example, in 2016, hundreds of thousands of weakly-secured IoT devices were accessed and hacked, disrupting traffic on the Internet. Additionally, smart devices that monitor public spaces may collect information about individuals without their knowledge or consent. For example, fitness trackers link the data they collect to online user accounts, which generally include personally identifiable information, such as names, email addresses, and dates of birth. Such information could be used in ways that the consumer did not anticipate … That data could be sold to companies to target consumers with advertising or to determine insurance rates."

In an era where the perceived risk and stakes of cyberattacks on the government is higher than ever, this has considerably slowed IoT adoption in the public sector.

"Cybersecurity risk is kind of a third rail in government technology," said Joshua New, Policy Analyst at the Center for Data Innovation, who has published several reports on IoT use in government. "And when you have the government being so hesitant to be an early adopter of the technology, that's really detrimental to the growth of the whole ecosystem."

This hesitancy to absorb risk because of cybersecurity fears may be the most significant challenge to IoT adoption, New said. "In fact, in recent action plans, no agency, other than the U.S. Postal Service, even ever mentioned the phrase Internet of Things."

> **"When it comes to anything connected, you have to start right away with the cybersecurity issues, because that's what is the most prominent fear in using the technology."**
>
> Naba Barkakati,
> *Chief Technologist at the GAO*

OVERCOMING SECURITY CHALLENGES

Despite the serious challenges privacy and security pose to IoT, the public sector is coming up with ways to move forward.

Sokwoo Rhee, Associate Director of Cyber-Physical Systems Program at the National Institute of Standards and Technology (NIST), said NIST recommends agencies consider risks that may be introduced when information systems are connected to other systems with different security requirements and controls.

NIST also explains that organizations typically do not have control over the external networks (e.g., the internet) with which their devices directly connect, and so it suggests applying boundary protection devices, such as firewalls and routers, to mediate between the devices and the external networks.

One way to move forward, suggested by the GAO report, is to notify users of any IoT use or technology whenever their personal information is collected and retained, and to give users the opportunity to choose whether to allow such collection.

Additionally, Naba Barkakati, Chief Technologist at the GAO, said he believes that some kind of uniform framework for the security and privacy aspects of IoT data might emerge. "The data can be from different places, but we must find a way to apply some rules where it's applicable to ensure privacy and security of all the data."

Rhee agreed that this is the potential path forward in addressing security issues for IoT. "NIST has a cybersecurity framework that a lot of private-sector entities have adopted," he said. "However, it's not a regulation, it's really a guideline. And I think in IoT creating some recommended framework for cybersecurity and use like that is probably the right approach as of right now for the government."

INDUSTRY SPOTLIGHT

Scaling the Internet of Things with Cloud Technology

An interview with Sri Elaprolu, Senior Manager & Global Lead for AWS Public Sector IoT Practice

By now, most public sector employees are aware of the capabilities that the Internet of Things can provide government. IoT technology can help with everything from transportation, to real-time and predictive analytics, to energy efficiency, and much more.

But the rapid growth of IoT in and of itself can pose a problem even as it is helping solve critical issues. In fact, IoT is growing at a very rapid pace, with some estimates saying over 50 billion things will be connected by 2020.

So how can IoT scale properly in government? GovLoop sat down with Sri Elaprolu, Senior Manager and Global Lead for AWS Public Sector IoT Practice, to find out why cloud technology will be the backbone infrastructure for IoT solutions of the future.

"The reality is that more devices are coming online, which means more data is going to be collected and needs to be stored, processed, and analyzed in some way," Elaprolu explained. "This translates to an increased volume and pace at which data is going to be collected. And trying to do this on premise is going to be near impossible, from a capacity perspective as well as cost."

This is where cloud technology comes in from four important aspects of supporting and expanding the Internet of Things: storage, agility, cost and security.

As Elaprolu noted, scaling IoT will first require the storage that only cloud can provide. Cloud providers have made storage and compute virtually limitless with on-demand, scalable infrastructure that meets the demands of big data manipulation.

The second way cloud helps scale IoT, said Elaprolu, is agility. "IoT is a fast-moving field," he noted. "Innovation is happening in almost real time which means experimentation is absolutely key for an agency so that they're not locked into something. Cloud is an ideal platform for easy experimentation without committing resources for the long run."

But experimentation and agility cannot happen if the costs of doing so are prohibitive. Fortunately, cloud technology can be paid for only as much as it is used, allowing government to experiment with IoT solutions. Once again, this allows government agencies to scale and grow IoT.

Finally, government agencies should incorporate security into all layers of their IoT solutions: device identity and authorization, security of data in-transit and at-rest, and security within edge processing. Without proper security, scaling IoT solutions is very challenging.

That's where AWS and its solutions geared towards scaling IoT come in. Using services such as AWS IoT and AWS Greengrass, customers can design and deploy highly reliable, secure and real-time connected solutions.

"AWS IoT is a managed cloud platform that customers can use to connect devices, whether they're starting with 10 devices, or 10 million devices," Elaprolu said. "With AWS IoT, they're able to connect all those devices to the cloud based platform securely, and can transmit data into the cloud as well as receive instructions from the cloud in order to change the behavior in the physical world."

AWS Greengrass is software that lets you run local compute, messaging, data caching, and synch capabilities for connected devices in a secure way, while seamlessly extending AWS to devices so they can act locally on the data they generate, while still using the cloud for management, analytics, and durable storage.

"AWS partners are also innovating on top of our cloud platform and bringing IoT solutions to public sector customers. A few examples include MioVision and GridSmart for smart traffic management; Philips CityTouch for smart street lighting and C3 IoT for predictive analytics," Elaprolu said.

"AWS can help governments leverage their multiple sources of data inputs to maximize insights and outcomes. They can become smarter, more efficient and leverage resources more effectively," said Elaprolu.

For example, Peterborough City Council, which is tasked with governing the City of Peterborough is becoming smarter and more efficient. Using AWS, they can integrate data from weather stations, Smart Energy Meters, IOT devices installed in people's homes, and automated libraries with council's core applications and data sets. The AWS deployment acts as a hub for all legacy applications, integration to Smart City IoT Devices, Analytics, and SaaS applications. And this is just one of many examples.

Within the public sector, IoT is being used for areas important to all citizens. And in order for it to truly scale and provide the insights and services that it promises, cloud technology must be the backbone on which it runs.

CHALLENGE # 2

Procurement

Slow procurement processes and low funding levels have been cited as major challenges in efforts to secure, develop and acquire IoT platforms in government. Agencies often do not have sufficient funding to modernize their IT infrastructure and begin implementing IoT pilot projects. But even when funding does exist, procurement policies often make it difficult for agencies to quickly and easily adopt the technology.

Procurement in government has never necessarily been easy, no matter what technology or products the government was looking to acquire. Because the U.S. government is the largest buyer of services and goods in the country, it does make sense that there must be a number of regulations and limits in place to protect taxpayers and the process.

But this slow approach and numerous regulations to purchasing new technology and services is a serious boon to the adoption and growth of IoT technologies in government at the federal and local levels alike.

In fact, 39 percent of respondents to a recent survey of government employees singled out insufficient funds and concerns over procurement times as one of the biggest blocks to adoption of IoT.

"Procurement schedules being far too slow was one of the biggest complaints we heard when interviewing people for our reports," said New. "These are emerging technologies and we know they have real benefits; we can't be waiting five years to start testing them out."

It's no lie. In fact, recently in San Francisco, it took the city two years to put together an RFP for a program to help guide visually impaired individuals through San Francisco International Airport.

Another challenge faced in the procurement process is simply the amount of services and technology involved in any IoT project or capability. According to the GAO, IoT devices consist of three common components (hardware, network connectivity and software), which are all supported by different technologies.

Additionally, several common architecture models are used to describe how IoT devices connect to a network to collect, share and communicate information. Procuring all of the necessary software and hardware to successfully run an IoT implementation is difficult and risky – and the government is notoriously risk-adverse.

Finally, because the procurement and regulation process of RFPs in government can be quite lengthy, by the time the purchase process has resulted in buying a particular product or technology, the next generation of that product might have already been developed and come to market, rendering the already purchased solution moot or unusable. This is particularly true of IoT, as its technology is evolving more quickly than almost anything else.

> **"Standard federal procurement practices are designed to purchase tested and mature technologies, not new and promising ones."**
>
> *Center for Data Innovation Report*

OVERCOMING PROCUREMENT CHALLENGES

Some federal agencies are trying to address the looming IoT procurement challenge through new acquisition programs. For example, DHS created the Homeland Security Innovation Programs (HSIP), which uses a more flexible purchasing method than the lengthy traditional procurement process, New explained.

Additionally, the approach the government is currently taking may be wrongheaded; with IoT, government should not necessarily be buying the hardware, Barkakati said. “They could be working with the vendors of the world to provide the hardware. This creates less risk.”

New also explained that government should consider creating a council to discuss IoT issues across government, particularly in procurement. If government can identify how to reform procurement policies so that agencies can purchase IoT solutions more easily and with less delay, adoption will be faster and more successful and the benefits will be more quickly realized.

One other possible solution, Franklin-Hodge suggested, is issuing RFPs for the outcome wanted or the problem needing solving, rather than the technology and hardware. In this way, the government would avoid absorbing the risk of expensive IT solutions not working.

Microsoft

Azure Government

By the people, for the people

The most trusted cloud for government, ready for your mission workloads

Learn more about Azure IoT >

Request a free Azure Government trial >

INDUSTRY SPOTLIGHT

Helping Government Agencies Embrace IoT Technology

An interview with Sam George, General Manager, Azure Internet of Things at Microsoft

The Internet of Things (IoT) is rapidly transforming the way local, state and federal agencies are meeting their missions. IoT brings the ability to collect data in real time from physical assets critical to a mission, gain insights from them and act on those insights in real time.

From more efficient and timely delivery of services, to significant reductions in operating expenses, to new insights that were not possible before, IoT has empowered agencies to digitally transform the way they do business and serve their citizens. But, how do agencies get started?

In a recent interview with GovLoop, Sam George, General Manager of Azure IoT at Microsoft, explained that government organizations can reap benefits from IoT including enhanced security, productivity and efficiency if they put the resources in place to truly leverage connected devices and the data they produce.

“IoT projects consist of three high level areas: devices, insights and actions,” said George. “For devices, Azure services like IoT Hub enable agencies to connect, communicated with and manage IoT devices which monitor physical assets in a secure, scalable way. Azure data and analytics offerings power insights, and rich business process integration services like Azure Logic Apps help agencies react to insights in real time.”

George shared that it is important for agencies to explore how IoT can benefit their mission and then start with a tactical proof of concept to gain understanding and build momentum. Azure has a rich set of offerings and a partner ecosystem that can help.

“It’s amazing to see how quickly a proof of concept can help agencies understand the value IoT can bring to bear in a mission,” said George. “Once agencies understand the impact IoT can have, we see them realizing how it can be applied to other missions.”

While security and privacy are always a concern, Microsoft has comprehensive cyberphysical security guidelines to keep customers safe. “We even have a security auditing program, called the Security Program for Azure IoT, where trusted auditors can inspect IoT solutions, find issues and recommend remediations,”said George.

Admittedly, IoT can be complicated. It can have massive scope with several moving parts and require an understanding over devices, data, and backend services. Sometimes this can be what prevents organizations from taking the first step.

Fortunately, there are technology partners that can help government agencies navigate this space. “Simplifying complex technologies for broad usage has been the focus of Microsoft and its partners throughout our company history,” George said.

Microsoft’s industry-leading portfolio of IoT offerings – extended and deployed for government by the largest partner ecosystem in the world – is what helps reduce complexity and cost, ease deployment, and speed time to market. All in a manner that is scalable, secure, and open, according to George. State and local governments are now able to use Azure IoT Hub in Azure Government, Microsoft’s cloud platform designed exclusively for U.S. government. IoT Hub in Azure Government will especially benefit agencies with mission scenarios that require a secure, compliant bridge between the IoT device or endpoint and a cloud storage solution.

Many organizations are already leveraging Microsoft Azure IoT services in a wide range of scenarios. In the case of public safety, dangerous road conditions in the U.S. result in 7,400 deaths and 700,000 injuries each year, while businesses and municipalities spend $2.3 billion on snow and ice control operations.

To help make important road-treatment decisions around snowstorms in Fairbanks, Alaska, the state’s Department of Transportation developed a sophisticated weather-tracking solution, WeatherCloud, with IoT solutions provider Fathym. WeatherCloud is built leveraging Microsoft’s Azure IoT platform and provides data analytics and insights for a more complete understanding of real-time road weather.

The potential for IoT innovation in government is powerful ¬– from reducing response times for emergency services to using usage tracking and smart grids to drive energy efficiency. Today’s military organizations can embrace IoT to improve their military effectiveness by attaching sensors to combat vehicles and other equipment that help monitor assets and obtain a real-time picture of what’s happening on the ground. Likewise, fighter aircraft are increasingly being equipped with advanced sensors that give pilots a 360-degree view of battle information.

With new IoT features on Azure Government, government organizations have expanded options for delivering on their missions with innovative and secure solutions.

CHALLENGE # 3

Regulation

IoT shows potential in terms of efficiencies and decision-making, but is also extremely risky. So who will regulate its use and how it goes forward? Several agencies currently have authority over some aspects IoT, but the regulatory framework is not well-defined. What's next in terms of IoT regulation and what will standardization look like?

One challenge that government often faces is standardizing approaches in technology. Since it is such a massive entity, the technology that one agency or city adopts is very likely to be different from the way another goes. This often poses no problem, but in IoT the lack of regulation, standardization and interoperability could be a real problem to continued growth, particularly at the state and local levels.

"If Seattle and Bellevue go down the Internet of Things route, they're going to sign deals with different vendors, and those vendors are likely to be incompatible," said Dr. Joseph Williams, Information and Communication Technology Industry Sector Lead in Washington state. "And both cities reside in King County. So how does King County do a smart county initiative, if all 49 cities in the county do their own thing?"

"There's no one single agency who is in charge of IoT regulations. I'm not sure that would even make sense to have one, but it is something we'll need to think about," said Rhee.

Barkakati agreed, citing his recent GAO report, which noted a big challenge for government is that when adopting IoT devices and systems, they must be able to communicate easily. Technical standards to enable this communication will need to be developed and implemented effectively.

One other challenge facing those who realize the need for regulation and standardization? The fact that those very regulations could end up restricting the sector and slowing down innovation and adoption.

"Recently in Washington state, we had legislators propose everything on smart car technology from crazy requirements on insurance to banning the use of any photography inadvertently collected in the navigation of the vehicle," Williams said. "They also wanted to put regulations and restrictions on drones, where they could go and what data they could collect." Williams pointed out that any legislation like that, while understandable, would actually restrict the development and data collection so critical to the development of IoT.

> **"Interoperability and related standards development will be important to the success of IoT from a technical perspective."**
>
> *NTIA green paper, "Fostering the Advancement of the Internet of Things"*

OVERCOMING REGULATION & STANDARDIZATION CHALLENGES

This tension between regulation and innovation is at the forefront of IoT issues in government. A recent green paper by National Telecommunications and Information Administration (NTIA) explained, "Commenters have urged the U.S. Government to avoid over-regulation that could stifle IoT innovation. The risk of premature and excessive regulation is notable given the size of the potential economic benefits to U.S. producers and consumers."

One model government has already adopted for a particular technology could work as inspiration here, said New: FedRAMP.

"The federal government should establish a process similar to the Federal Risk and Authorization Management Program designed to facilitate federal agency cloud adoption, to expedite federal agency adoption of the Internet of Things," New writes in his report for the Center for Data Innovation.

One other thing the government should consider doing for now in terms of regulation? Nothing.

"There's no department of IoT as of today," Rhee said. "And there's no department of smart cities. For where we are, it would be almost silly to create a U.S. federal department to work on something that's not even an industry, it's a concept. We need to wait and see what the private sector does, and what happens."

FAST TRACK

IT COST SAVINGS

Save up to 30% on infrastructure costs and invest in innovative solutions

http://www.bmc.com/it-solutions/industry-public-sector.htmls

bmc

INDUSTRY SPOTLIGHT

Evolving the Digital Workplace with the Internet of Things

An interview with Jeremy A. Wilson, Federal CTO, BMC

It's no secret that the pace of digital transformation is impacting every aspect of our society, including government. And as the public sector looks to the future, they're figuring out how to best serve citizens more efficiently, as well as to hire and retain workers by providing better technology and a more modern work environment.

That's where the concept of a digital workplace comes in. The digital workplace is where people, technology, and the workplace converge to improve agility, productivity, and engagement. This environment enables employees to find the same type of consumer-oriented experiences they enjoy in their personal lives, with one-stop-shopping for the technology tools to do their work more effectively and effortlessly.

But the digital workplace doesn't happen without having the right technology in place – particularly as it relates to managing the Internet of Things (IoT) and leveraging cloud-based analytics platforms. To understand how government agencies can create a digital workplace with IoT, GovLoop spoke with Jeremy A. Wilson, Federal CTO, at BMC, a leader in software solutions that helps organizations transform into digital enterprises.

Wilson explained that as government organizations strive to become digital enterprises, they need to make the best use of their existing assets and infrastructure, while introducing new technology and tools that drive their missions forward and keep their resources secure.

More than one-third of federal workers will be eligible for retirement by September 2017, and many government agencies are having difficulty attracting younger personnel. To address these issues, government IT leaders are working to create this "digital-first" workplace. The rapid adoption of digital technology in the commercial world is driving government agencies to fundamentally rethink how they deliver services to their internal users and external constituents. This provides the platform to vastly improve cross-collaboration between government agencies and maximize employee agility, productivity, and engagement.

But a workplace cannot be truly digital first without the support of the right technology – particularly as it relates to the data and insights that IoT can offer.

"There will be nearly 21 billion IoT connected devices worldwide by 2020," Wilson explained. "IoT is transforming the 'traditional' environment and is paving the way for a modern digital workplace." With this transformation, it is important that government agencies begin to break down some of the barriers between people, technology and the workplace, while also keeping necessary process enforcement and governance.

Aggregating, managing, delivering, and analyzing hardware, software, and services from multiple cloud and on-premises vendors that workers choose isn't easy. Each offering may have its own interface, which can be confusing and frustrating to use. Additionally, unless government organizations have the proper analytics tools in place when collecting data generated by IoT they will not be able to maximize the potential value of this data. Most importantly, it's critical to keep that data secure.

"As the workplace becomes more digital centric, there is an ever-increasing number of ways devices can be compromised," Wilson said. "Government needs to take steps to establish a comprehensive defense methodology and security infrastructure to identify and mitigate these threats."

Agencies also need to have the right cloud-based, big data analytics platform in place. The right solution will help agencies collect and analyze machine, business, and operational data – from virtually any source, in real time – as well automatically learn behavior of machine data, the service desk, business activities, and social metrics.

"The more devices that you have connected in this modern digital workplace, the more data you have to analyze," Wilson said. "This is one of the biggest problems we have today, there is too much data and not enough people. Government agencies must start looking at new methods to visualize and consume data as we make this shift. They must become more efficient in keeping data secure and in analyzing it for trends."

BMC can help government agencies power their digital workplaces. With IoT, BMC provides security and operations with greater insights to quickly identify, prioritize, and remediate threats, along with a secure cloud-based analytics platform. The digital service management platform from BMC empowers IT to drive digital innovation, with exceptional IT service management capabilities that help organizations scale and automate IT processes.

Leveraging data and the right technology can help government organizations meet the challenges of rising citizen demands and attract new talent. The digital workplace will require sophisticated, intuitive technology, comprehensive service offerings, and a partner like BMC with the solutions and expertise to help agencies drive change.

CHALLENGE # 4

Workforce

IoT can only reach its full potential with the buy-in of top leadership and a workforce who has the skills to advance it. But there's a lack of education for employees about how to deploy IoT, and agencies do not always have workers with the necessary technical skills to effectively use data generated by sensors and other devices.

The challenge of hiring and retaining talented technical workers in the U.S. government is not limited to IoT. Because the private sector offers higher pay and more flexibility, it has long been difficult for the government to hire the best and the brightest in IT.

But this challenge will be particularly important to overcome if the public sector wants to expand and deploy critical IoT technology, because it will need a skilled and well-trained workforce to operate in this emerging field.

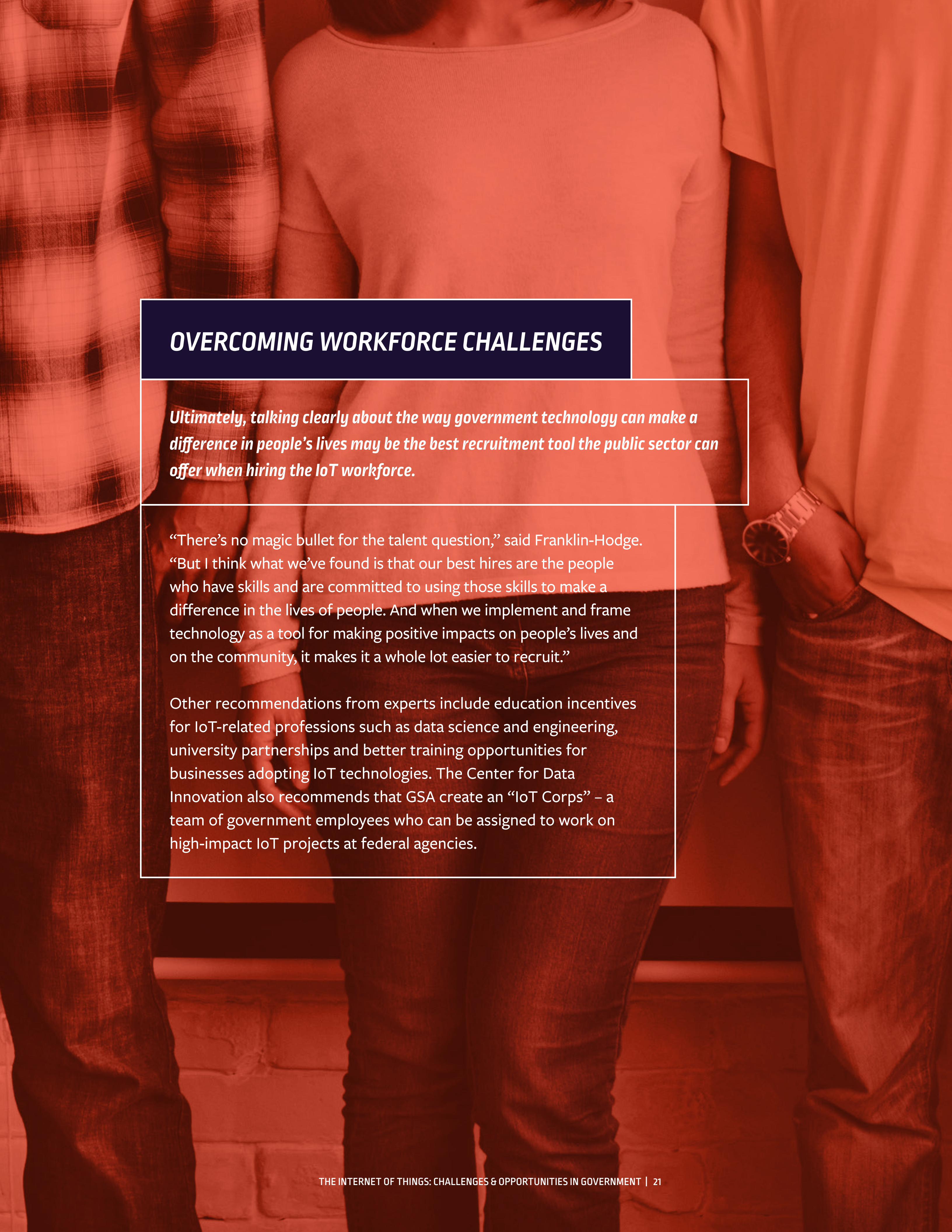
According to NTIA, "In order for the United States to take full advantage of developments in an IoT economy, the U.S. Chamber of Commerce Center for Advanced Technology and Innovation suggests that the Department will need to prepare U.S. workers for a shift in workforce education and training needs." But this will be difficult for a variety of reasons.

Bonaparte cited one example of the kind of skilled employee needed for an IoT initiative, a mining company that operates driverless trucks in its mines. These are huge vehicles that collectively haul millions of tons of material each month. Generally, driverless vehicles are controlled from a remote location by technically skilled employees working in a state-of-the-art operations center hundreds of miles away. Training for these sorts of jobs, however, is not at the level Bonaparte believes it should be.

The other fact is that the development of IoT will automate some fields and cause potential job loss. "Robotics has displaced workers in various sectors, and progress in IoT technologies will increase the threat to some types of jobs," acknowledges the GAO report.

This reality can cause a reluctance to train workers for future IoT jobs, as some sectors would rather not acknowledge the eventuality of this happening. But refusing to prepare and train the workforce for IoT will only cause a shortage later on.

> **"There's a huge data science skills gap in the United States government. Right now, there's way more demand for data center workers than we're producing."**
>
> Joshua New,
> *Center for Data Innovation*



OVERCOMING WORKFORCE CHALLENGES

Ultimately, talking clearly about the way government technology can make a difference in people's lives may be the best recruitment tool the public sector can offer when hiring the IoT workforce.

"There's no magic bullet for the talent question," said Franklin-Hodge. "But I think what we've found is that our best hires are the people who have skills and are committed to using those skills to make a difference in the lives of people. And when we implement and frame technology as a tool for making positive impacts on people's lives and on the community, it makes it a whole lot easier to recruit."

Other recommendations from experts include education incentives for IoT-related professions such as data science and engineering, university partnerships and better training opportunities for businesses adopting IoT technologies. The Center for Data Innovation also recommends that GSA create an "IoT Corps" – a team of government employees who can be assigned to work on high-impact IoT projects at federal agencies.

INDUSTRY SPOTLIGHT

Communicating with the Public Through Sensors and Technology

An interview with Richard Fong, Technical Implementation Consultant, Granicus

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 Granicus, a leading company in the public sector digital software 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 decade, 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 us.”

Granicus 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 Granicus with the alert, who will in turn send the message to that specific monitoring site distribution list.

“In essence,” Fong continued, “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.”

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 our platform with APIs, we can expose various resources so a government agency’s system or application can communicate back with us 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.”

“As the world continues to evolve,” said Fong, “so does the way we serve government and thus, how government communicates with citizens. Just imagine where we’ll be in another 15 years.”

CHALLENGE # 5

Broadband & Infrastructure

IoT will depend on both public and private communications networks, and will use various wireline and wireless modes, including satellite, often in combination or on an interdependent basis. The need for seamless connectivity will require robust broadband and infrastructure for interconnecting devices. How can governments meet this challenge?

If IoT technologies and sensors are, in an analogy, the cars of the future, solid broadband and infrastructure networks are the roads they need to drive on. IoT cannot truly be successfully deployed without robust broadband and a secure, safe infrastructure.

The numbers support this reality. According to NTIA, internet traffic will be 22 times greater in 2018 than 2013. This traffic growth will dictate the need for greater overall network capacity – and smarter use of the bandwidth that is available for IoT projects.

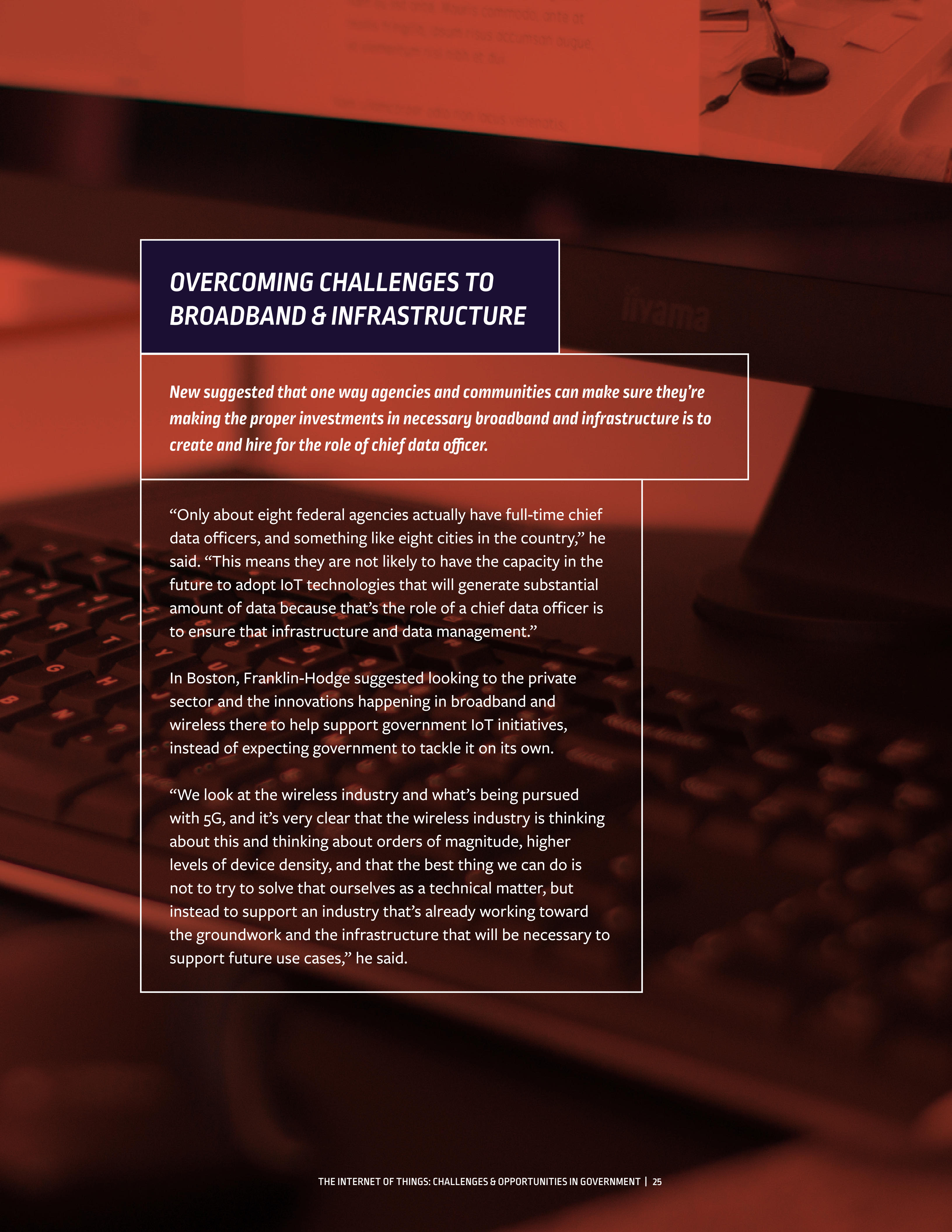
Additionally, explained New, agencies that do not have the technical infrastructure to manage massive amounts of data are going to be unable to adopt the IoT.

Clearly, broadband and smart infrastructure are the keys to successful IoT deployment. But executing and evolving in these areas can be a challenge for government, both in the creation of better infrastructure and the fact that many citizens don't have access to broadband, limiting their potential use of and benefits stemming from IoT.

In fact, the Federal Communications Commission reports that 19 million Americans (6 percent) do not have access to fixed broadband. In particular, rural providers can find it difficult to upgrade existing networks to keep pace with consumer demand and extend networks into parts of rural America still lacking access. According to the Rural Broadband Association, "Overcoming these challenges to availability and sustainability of broadband is the condition precedent to the widespread availability of IoT-enabled devices that can transform the lives and businesses, especially agricultural operations, for millions of rural Americans."

Another reality is that updating infrastructures has long been a true challenge for government at all levels. It will be relatively difficult to create and invest in the infrastructure needed to support IoT programs when so much of current government IT is invested in legacy technology and maintenance.

> **"We are asking ourselves, how do we lay the infrastructural groundwork for the evolving technology around broadband access?"**
>
> Jascha Franklin-Hodge,
> *Boston Chief Information Officer*



OVERCOMING CHALLENGES TO BROADBAND & INFRASTRUCTURE

New suggested that one way agencies and communities can make sure they're making the proper investments in necessary broadband and infrastructure is to create and hire for the role of chief data officer.

"Only about eight federal agencies actually have full-time chief data officers, and something like eight cities in the country," he said. "This means they are not likely to have the capacity in the future to adopt IoT technologies that will generate substantial amount of data because that's the role of a chief data officer is to ensure that infrastructure and data management."

In Boston, Franklin-Hodge suggested looking to the private sector and the innovations happening in broadband and wireless there to help support government IoT initiatives, instead of expecting government to tackle it on its own.

"We look at the wireless industry and what's being pursued with 5G, and it's very clear that the wireless industry is thinking about this and thinking about orders of magnitude, higher levels of device density, and that the best thing we can do is not to try to solve that ourselves as a technical matter, but instead to support an industry that's already working toward the groundwork and the infrastructure that will be necessary to support future use cases," he said.

Conclusion

It’s clear that the Internet of Things is becoming a reality in the public sector. Our questions: What role do we see government playing in this new arena and what obstacles are currently holding it back? There are significant challenges, but there are ways to overcome all of them. And that must be done, because IoT will have an impact on every vertical within the public sector, including training, transportation, technology and healthcare, just to name a few. With some efforts in innovation, problem-solving and creative uses of technology, the public sector can truly start to take advantage of IoT to create efficiencies, reduce costs, and ultimately help citizens live better lives.

About & Acknowledgments

ABOUT GOVLOOP govloop.com | @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.

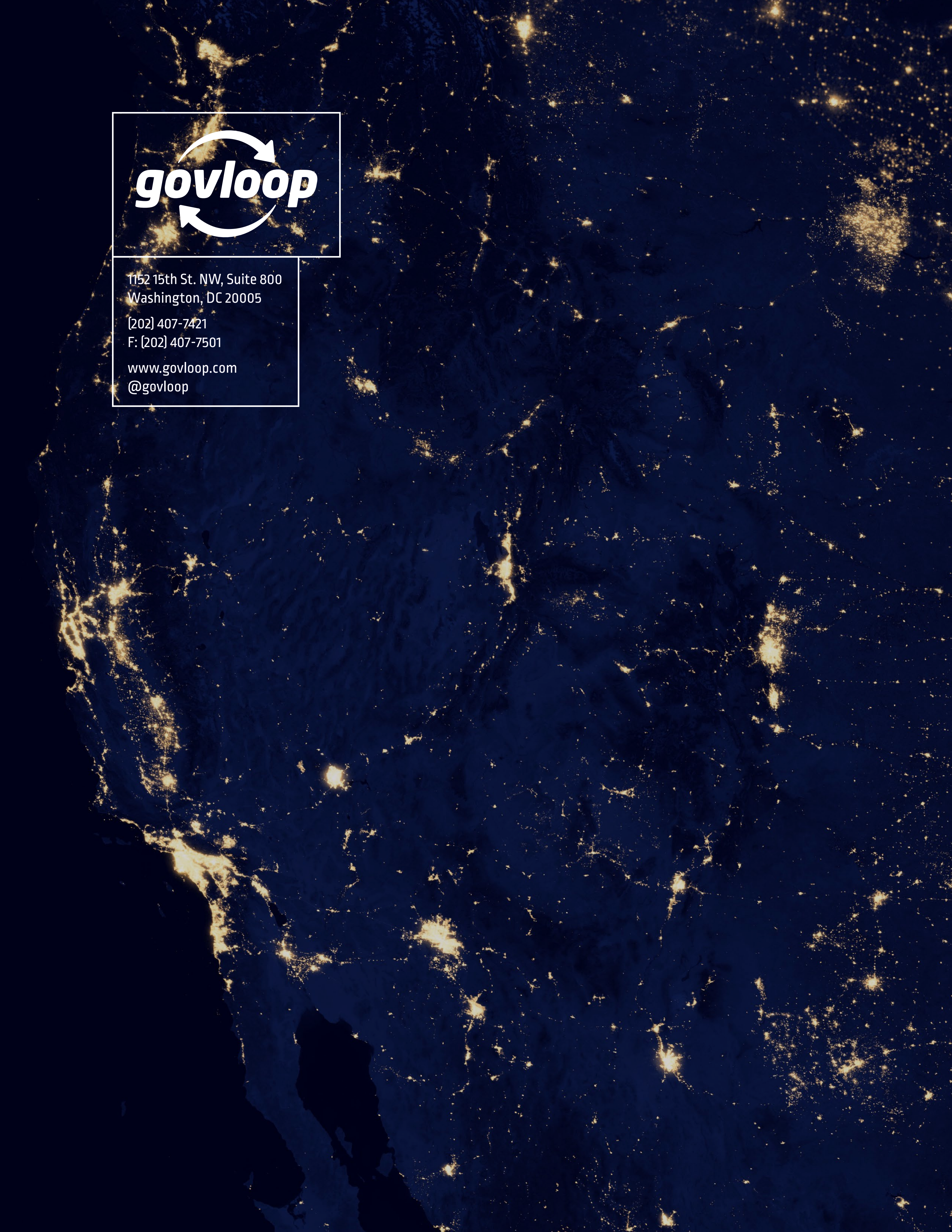
For more information about this report, please reach out to info@govloop.com.

THANK YOU

Thank you to Amazon Web Services, BMC, Microsoft and Granicus for their support of this valuable resource for public sector professionals.

AUTHOR Catherine Andrews, Senior Director, Editorial & Production

DESIGNER Kaitlyn Baker, Lead Graphic Designer



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

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

www.govloop.com
@govloop