CENTER FOR DATA INNOVATION

How Is the Federal Government Using the Internet of Things?

By Daniel Castro, Joshua New & Alan McQuinn | July 25, 2016

There are many opportunities for federal agencies to use the Internet of Things to operate more efficiently and effectively, but few agencies are pursuing these opportunities. There are a number of challenges preventing greater adoption of the Internet of Things among federal agencies. These include a lack of leadership, skills, and funding, as well as cumbersome procurement policies and a risk-averse culture. Agency adoption of the Internet of Things will likely remain low unless important changes are made to encourage adoption across the federal government.

The Internet of Things (IoT)—a term used to describe the set of physical objects embedded with sensors or actuators and connected to a network—offers numerous opportunities for the federal government to cut costs and improve citizen services. Moreover, because the Internet of Things generates positive network externalities, widespread adoption by the government will spur commercial adoption. While early adopters in the federal government have already demonstrated the potential of this technology with projects that improve public safety, reduce energy use, enhance military capabilities, and improve worker health, overall adoption across federal agencies is still very low.

While early adopters in the federal government have already demonstrated the potential of this technology, overall adoption across federal agencies is still very low.

The federal government faces a number of challenges that have slowed the adoption of the Internet of Things in the public sector. First, there is a lack of strategic leadership at the federal level about how to make use of the Internet of Things. Second, federal agencies do not always have workers with the necessary technical skills to effectively use data generated by the Internet of Things. Third, federal agencies do not have sufficient funding to modernize their IT infrastructure and begin implementing IoT pilot projects. Fourth, even when funding exists, federal procurement policies often make it difficult for agencies to quickly and easily adopt the technology. Finally, risks and uncertainty—about privacy, security, interoperability, and return on investment—

delay federal adoption as potential federal users wait for the technology to mature and others to adopt first.

The federal government should make a number of reforms to address these challenges:

- The Federal CIO Council should establish an IoT taskforce to provide much needed cross-government leadership and coordination to support adoption and deployment of this technology.

- Each federal agency should develop an IoT action plan to identify how it will use IoT solutions to cut costs and improve services.

- Agencies should employ a chief data officer to ensure that they establish the necessary technical infrastructure to make effective use of data generated by the Internet of Things.

- GSA should establish an "IoT Corps"—a team of government employees who can be assigned to work on high-impact IoT projects for the government.

There are also a number of steps that the federal government can take to support the broader development of the Internet of Things. Federal agencies should:

- Fund and support large-scale state and local IoT pilot projects.

- Engage with the private sector to encourage industry-led voluntary standards and best practices to improve privacy, security, and interoperability.

- Expand R&D funding for key technologies that support the development of the Internet of Things.

This report concludes that adoption of the Internet of Things will likely remain low across the federal government unless changes are made to encourage adoption across federal agencies.

METHODOLOGY

In order to assess current use of the Internet of Things in the federal government we interviewed 22 experts from the U.S. federal government and private sector, including 8 current and former government officials (primarily chief information officers, chief technology officers, or the equivalent) and 14 senior private-sector leaders involved in developing or providing IoT solutions to government officials. Participants were asked questions about the opportunities and challenges federal agencies face to adoption and use of the Internet of Things. To encourage candor, all interviews were conducted on a non-attribution basis. Of the non-government participants, respondents included employees with the following organizations: Amazon, AT&T, Boeing, CGI, Cisco, GE, Google, IBM, the Industrial Internet Consortium, Intel, IT Alliance for the Public Sector, Lockheed Martin, Oracle, and VMWare.

FEDERAL GOVERNMENT USES OF THE INTERNET OF THINGS

The majority of respondents in our interviews said that U.S. federal agencies are just beginning to explore how to use the Internet of Things.[1] While there are some interesting examples of federal agencies using the Internet of Things, overall adoption rates are still low, especially outside of the defense agencies. Where federal agencies have begun deploying IoT solutions, it is typically to pursue one of two main goals: reduce costs and offer new services.

REDUCE COSTS

The primary motivation for federal agencies to use the Internet of Things is to be more efficient and reduce costs. Major projects include a smart-buildings initiative to reduce energy costs, a telematics program to increase the efficiency of government vehicles, an effort to improve asset management, and automating manual data-collection processes.

Smart Buildings

The foremost example of cost cutting in the federal government is in the form of smart-building applications. For example, the General Services Administration's (GSA) Smart-Buildings initiative aims to modernize federal government buildings in large part through connected technologies, thereby making them more energy efficient. Launched in May 2012, the initiative is an attempt to fulfill President Obama's 2009 executive order to reduce the energy consumption of federal buildings 30 percent by 2015.[2] The first phase of the project installed thousands of low-cost connected sensors into 50 of the government's most energy-intensive buildings, totaling over 30 million square feet, to collect a minimum of 1,000 data points related to energy use and operational efficiency per building. GSA has estimated this initiative to have resulted in $15 million of annual savings.[3] These technologies include a broad array of connected systems, ranging from simple motion sensors that turn off lights when employees leave their desks to more advanced systems that automatically raise and lower shades based on the amount of sunlight coming through windows to save on heating and cooling costs.[4] As of August 2014, GSA had expanded the program to 80 of a targeted 200 federal buildings and, by analyzing data from these sensors, had identified over 10,000 inefficiencies in federal buildings.[5] The U.S. Department of State has followed suit by setting up smart metering at many of its posts worldwide to analyze energy and water consumption in real time, improve efficiency, and benchmark building designs to improve performance for future buildings in its missions around the world.[6]

GSA continues to explore opportunities to use data from these smart systems to increase efficiency. For example, in June 2013, GSA partnered with IBM to implement GSA Link, an analytics program that monitors smart-building data in real time to identify inefficiencies. With this data, GSA learned that large amounts of equipment remained running over federal holidays, prompting managers to proactively encourage employees to turn off their computers before they leave.[7] The granularity of the data allows managers to solve subtler efficiency problems as well, such as when the system reported irregular air flow data from a particular building vent that was later found to be obstructed by a dead pigeon.[8] Though this strained the building's ventilation system, no human would have likely noticed the change; but thanks to a robust sensor network, managers can identify exactly when and where such problems arise.[9] Similarly, the U.S. Coast Guard (USCG) has deployed a suite of automated monitoring tools and networked sensors throughout its primary data center to collect data on environmental factors and system utilization. These tools provide staff with detailed performance dashboards and have allowed USCG to reduce energy costs in its data center by 25 percent.[10]

Furthermore, in July 2014, GSA connected its desk-reservation system, called BookIt, to its security system, so that whenever an employee scans an identification badge to enter a building, his or her desk powers up and turns on lighting once the employee sits down.[11] GSA uses data gathered from this reservation system as part of its connected hoteling strategy—where certain office resources are treated as shared assets, rather than assets assigned to a specific individual—to efficiently allocate space in its main building, an approximately 800,000 square foot building that houses as many as 4,400 federal workers.[12]

Fleet Telematics

One growing use of the Internet of Things is for fleet telematics—the use of sensors to remotely monitor the location, performance, and behavior of vehicles within a fleet. GSA, which provides vehicles and fleet management services to over 75 federal agencies, has begun to use telematics to improve the efficiency of government vehicles.[13] In December 2015, GSA began to implement a program to use telematics devices, which include location tracking, navigation systems, and emissions sensors, to help ensure that the 204,000 vehicles in GSA's fleet comply with the March 2015 executive order (E.O. 13693) to reduce government vehicle greenhouse gas emissions 4 percent by 2017, 15 percent by 2021, and 30 percent by 2025.[14] When a federal agency obtains GSA vehicles, which range from sedans to ambulances and heavy trucks, it can choose to retrofit the vehicles with either of two telematics systems: GPS only or both GPS and vehicle diagnostics.[15]

The GPS-only system records and transmits data on vehicle speed, location, utilization, and time spent idling, while the system that includes vehicle diagnostics also reports on maintenance issues, fuel consumption, and emissions.[16]

Although all federal agencies will eventually have to collect and report all of this data, even those that choose to use only the GPS tracking system can increase their efficiency, lower costs, and avoid redundant expenditures by improving route planning, protecting against unauthorized vehicle usage, and providing timely information on the availability and whereabouts of agency vehicles.[17] By adding vehicle diagnostics technologies however, telematics can increase efficiency and cost benefits dramatically. For example, real-time data about engine performance can indicate potential problems before they arise and allow for preventative maintenance, which can be significantly cheaper than repairing an engine after it breaks down; this also avoids downtime.

Furthermore, as emissions vary by vehicle make and model, granular data about the emissions of an entire fleet can allow administrators to make more informed decisions about purchasing and vehicle utilization, as well as flag specific problematic vehicles to be phased out or repaired. Though estimates for the total cost and energy savings of this program do not exist, the effectiveness of similar programs in the private sector indicates that they are quite substantial, particularly given the large scale of GSA Fleet. For example, UPS implemented tracking and diagnostic telematics technology into many of its delivery vehicles and was able to cut the number of scheduled maintenance inspections by 50 percent, eliminate 3.43 million hours of idling time and 13,000 metric tons of carbon emissions per year; the technology also improved route efficiency to save 39 million gallons of fuel and avoid 364 million miles of driving since 2001.[18]

Improve Asset Management

Some federal agencies are also rolling out IoT applications to increase asset monitoring, utilization, productivity, and reliability. The Department of Defense (DoD), for example, is using the Internet of Things to more efficiently manage how it tracks military supplies, such as clothing, construction materials, and medical supplies.[19] In 2011, the Defense Logistics Agency and the U.S. Transportation Command designed a system to monitor the 3.5 billion transactions per month generated by 67 DoD logistics systems and 250 commercial transportation carriers.[20] While much of this data comes from the RFID tags that all contractors are required to use, data also comes from connected devices such as sensors embedded in fuel tanks at distribution hubs.[21] This data gives managers real-time insight into the availability and location of supplies and allows them to better manage inventory and shipments, as well as make more informed purchasing decisions.

Automate Manual Processes

Some agencies are using the Internet of Things to automate manual processes, which can substantially reduce costs. For example, the Department of Agriculture's National Agricultural Statistics Services (NASS) employs thousands of individuals to collect information from private farms across the country in order to produce the agricultural statistics used for production, marketing, and distribution. NASS has begun to collect some of this data automatically from connected farm technologies, such as soil moisture sensors and networked combines, to improve how it gathers its statistics on private farms.[22] Also, the Department of Transportation (DOT) has partnered with Sidewalk Labs, a subsidiary of Alphabet Inc. focusing on urban innovation, for a project called Flow to create a monitoring and management system for public transportation. This system will allow both federal and local transportation planners to better understand how people navigate cities to tackle transportation challenges and increase engagement with citizens.[23]

Many respondents to our interviews anticipate that automating manual processes will be an important opportunity for federal agencies to use the Internet of Things in the near future.

CREATING NEW SERVICES

Several federal agencies have used the Internet of Things as an opportunity to create services in support of their missions. Major new projects that use the Internet of Things include improving national defense, monitoring the natural world, and enhancing safety and public health.

Enhance Military Capabilities

The leading adopters of the Internet of Things are U.S. defense agencies, which use connected technologies on the battlefield to train soldiers, to improve care for injured troops, and to safeguard military supply chains.

The Internet of Things allows the U.S. military to provide a shared awareness of the battlefield for U.S. forces, a concept known as network centric warfare.[24] Military IoT deployments are designed to accommodate the specific operational needs of the different branches of the military.[25] Military bases collect data using a wide variety of connected technologies, including cameras, infrared sensors, and radiation and chemical detectors; and a wide variety of platforms, including drones, surveillance satellites, ship and ground stations, and soldiers in the field.[26] For example, the Navy operates a network of connected buoys that use sonar technology to detect the presence of submarines.[27] The Air Force combines surveillance data and sensor data from fight jets to provide pilots with detailed threat and target data in real time.[28] The Army combines data from environmental sensors and satellite imagery to help soldiers better navigate unfamiliar terrain.[29]

One particularly interesting use of the Internet of Things for military purposes is the connected aircraft. The F-35 Joint Strike Fighter—the nation's most advanced fighter jet—is a fully networked aircraft that is outfitted with an array of sensors designed to collect a variety of data to improve situational awareness.[30] The on-board systems analyze and synthesize all of this data to create a personalized dashboard displaying the most relevant information the pilot needs to complete a mission.[31] Defense contractors are also researching the next generation "smart skin" designed to cover the fuselage of an aircraft with thousands of sensors to relay a wide variety of information from the aircraft to a command post in real time.[32] Data from the F-35 are eventually merged with other data about other aircraft, ships, and vehicles in the field to provide a better picture of what is happening on the battlefield.

The Internet of Things not only makes the military supply chains more efficient, it also ensures that military equipment does not fall into the wrong hands. In response to high risk of theft and pilferage of military supplies headed through Pakistan to U.S. troops in Afghanistan, DoD's U.S. Transportation Command installed container detection intrusion devices (CIDDs) on military containers traveling through the area.[33] CIDDs use sensors placed on each container to detect and alert military personnel of any unauthorized intrusions; combined with satellite surveillance and truck location tracking in the event of unusual delays, this substantially reduces theft of military cargo.[34]

DoD has also developed several IoT applications designed to improve infantry performance. The Army's Multiple Integrated Laser Engagement System (MILES) training program simulates live combat by equipping soldiers with sensor-laden clothing and weapons loaded with blank cartridges and mounted with special lasers.[35] Sensors in the clothing register when a solder has been "killed" by a laser and trainers can monitor these simulations in real time to provide feedback.[36] Similarly, "shoot houses" rely on acoustic sensors, motion sensors, and video cameras to monitor soldiers in live-fire exercises to provide trainers with detailed data about soldier performance.[37]

The military is also using smart devices to provide better care to injured troops. For example, the Army has equipped thousands of soldiers' helmets with the Headborne Energy Analysis and Diagnostics System (HEADS), an array of sensors that record data about blows to the head to study how troops sustain traumatic brain injuries.[38] And the Defense Health Agency (DHA) is researching how to use wearable technologies to collect data that can determine what kind of injury a soldier has sustained, the injury's severity, evacuation time, treatment information, and whether surgery is needed, long before the soldier even reaches the hospital.[39] For example, biosensors placed inside clothing can monitor a soldier's vital signs, activities, and sleep quality.[40]

DHA believes that these efforts will improve quality of care through accurate patient identification, reduction of medical errors, and by providing comprehensive treatment information. Similarly, the Air Force has piloted the BioStampRC Wearable Sensing Platform, a series of Bluetooth-connected sensors embedded in a wearable patch that monitors biometric data, which can help doctors better evaluate an injured pilot's health and prioritize care.[41] The Defense Advanced Research Projects Agency's (DARPA) Warrior Web program has worked with Harvard University to develop smart clothing that monitors joint movement and provides targeted support to reduce fatigue and the risk of musculoskeletal injury.[42] The Department of Defense is also partnering with a consortium of manufacturers, universities, and non-profit organizations to establish the Revolutionary Fibers and Textiles Manufacturing Innovation Institute, part of the Obama Administration's National Network for Manufacturing Innovation, to develop futuristic fabrics and textiles that incorporate sensors and other technology.[43]

Monitor Weather and the Environment

The National Oceanic and Atmospheric Administration (NOAA) produces geospatial data for a variety of valuable applications, including coastal mapping, flood-risk evaluation, land-use management, and supporting environmental health, and it is exploring how to improve its services using the Internet of Things.[44] For example, NOAA's Ocean Explorer program is using and deploying a global network of hydrophones—underwater acoustic sensors—that can help researchers study ecological and environmental phenomena, such as whale migrations and underwater volcanic activity. NOAA's National Centers for Environmental Information is the world's largest provider of weather and climate data, operating advanced networks of environmental sensors on land stations on every continent, as well as satellites, buoys and ocean platforms, and weather balloons.[45] This data supports a wide variety of public and private-sector services, including resource management, transportation planning, weather forecasting, and insurance pricing.[46]

Protect Public Health and Safety

Many federal agencies are using the Internet of Things to protect public health and safety.

Several federal agencies have successfully leveraged the Internet of Things to improve disaster-response efforts, substantially reducing the potential economic and human cost of both natural and manmade disasters. For example, the Department of Veterans Affairs has equipped some of its hospitals with sensors that monitor the buildings' structural integrity during an earthquake and notify hospital administrators if they need to evacuate patients and staff.[47] Also to protect against earthquakes, the U.S. Geological Survey (USGS) has deployed a functioning prototype of ShakeAlert, an early warning system for earthquakes that relies on hundreds of sensors spaced 6-12 miles apart that report earthquake activity to a control center in real time.[48] When ShakeAlert detects the initial shock of an earthquake, USGS can then issue warnings up to several minutes before the more destructive, slower-traveling earthquake waves arrive.[49]

The Department of Homeland Security (DHS) runs several research and development projects that are exploring how the Internet of Things can provide solutions to the agency's operational needs.[50] For example, the Next Generation First Responder program, launched in January 2015, includes 40 projects working to develop connected technologies that protect emergency responders, reduce response time, and improve decision making.[51] One technology that DHS is piloting for first responders is clothing embedded with sensors that collect first responders' vital signs and transmits them to headquarters to improve situational awareness during emergencies.[52]

Also, the Centers for Disease Control and Prevention (CDC) is developing a pilot project to research what existing and emerging technologies, including the Internet of Things, are available for monitoring underground mining environments to safeguard miners' health.[53] Additionally, the Federal Emergency Management Agency (FEMA) is exploring ways it can use data from Internet of Things devices, such as fitness monitors, home appliances, smart smoke detectors, and security cameras, to gain insights and provide assistance during disasters.[54] Emergency managers want to be able to use data from these private networks of sensors to help during emergencies.[55]

NASA has developed several methods to use imaging and thermal sensors on its Earth observation satellites to predict, detect, and track wildfires.[56] For example, lightning imaging sensors aboard the Tropical Rainfall Measuring Mission can detect 90 percent of lightning strikes in the world, which can help researchers identify which areas might be prone to wildfire outbreaks; the Geostationary Operational Environmental Satellites provide continuous coverage of the northern hemisphere and transmit images and infrared scans that can reveal small wildfires every 15-30 minutes.[57] In 2003, NASA developed software that links these efforts—when one satellite detects a potential fire as it passes over a particular location, it can automatically direct a different satellite with more sensors to observe that area to collect additional data, confirm if it is actually a fire, and notify ground controllers.[58] And in partnership with NASA, the Forest Service operates the Active Fire Mapping Program, which combines satellite and sensor data to provide firefighting authorities with near real-time maps of wildfires across the United States and Canada.[59]

The Environmental Protection Agency (EPA) uses the Internet of Things to protect against other kinds of dangerous environmental hazards. For example, EPA's Air Quality System aggregates air pollution data collected by EPA, state, local, and tribal air pollution sensors. And EPA's NEUBrew program measures solar radiation with ultraviolet ray and ozone sensors at six stations across the country. EPA has also developed the Remote Sensing Information Gateway (RSIG) as a portal to access these and other environmental sensor networks throughout the federal government.[60] Similarly, in 2008 the U.S. Department of State started using air-quality-detection systems in its five missions in China to detect air pollution concentration and automatically send out notices to U.S. citizens in the region via smart phone apps and social media.[61] As a result of the success of the program, the U.S. Department of State has partnered with the EPA to replicate the program in other missions in areas like Mongolia, Vietnam, Kosovo, Indonesia and India, posting the data online on the EPA's AirNow website.[62]

CHALLENGES

Although there are a number of important examples that show the federal government is beginning to use the Internet of Things, overall adoption remains limited. There are a number of challenges that are holding back broader adoption of the technology, including: lack of strategic vision and leadership; lack of skills; lack of funding; inadequate procurement policies; and an unwillingness to take on the associated risk.

LACK OF STRATEGIC LEADERSHIP

One challenge limiting federal government adoption of the Internet of Things is the lack of a comprehensive vision for how to use the technology across federal agencies. The U.S. government does not have a strategic plan for how it will adopt and deploy the Internet of Things across federal agencies, and individual agencies are unprepared for how they will leverage the technology internally. In 2015, the Brookings Institute reviewed the strategic plans of all federal agencies and found that none so much as mentioned the Internet of Things.[63] As of May 2016, we still could not find a federal agency that addresses how it will use the Internet of Things in its strategic plan.[64]

While some federal agencies are pushing forward on IoT projects, many senior government IT leaders, including some chief information officers (CIOs), lack a complete understanding both of the technology and its potential benefits. This lack of support from senior government officials has permeated throughout the federal government, perpetuating a general lack of awareness and enthusiasm when it comes to the Internet of Things. Past surveys of federal agencies reinforce this point. One 2014 survey of federal employees found that only 9 percent thought their agency was actively exploring or using the Internet of Things, and only 14 percent said their agency would be using the technology in some way in the next three years.[65] In another survey, conducted in 2016 with 464 senior federal employees familiar with information security, 20 percent of respondents said that their agency was leveraging or moving to leverage the Internet of Things.[66] Surprisingly, this figure represents a 10 percent drop from the same survey conducted two years earlier.[67]

This lack of strategic vision hinders adoption of the Internet of Things within agencies. Project managers who wish to use the Internet of Things for a particular project may find that their own IT departments are unable or unwilling to provide the backend IT infrastructure needed to collect, store, and analyze new streams of data. Fragmented authority means that while a particular project may have the funding and support for the necessary hardware components, project managers have to work separately to get buy-in from the agency's IT department to run the software components.[68] As a result, office managers in federal agencies cannot even buy a "smart" coffee maker for the breakroom without getting their IT departments involved. It is no surprise that agencies will tend to default to "dumb."

When office managers in federal agencies cannot even buy a "smart" coffee maker for the breakroom without getting their IT departments involved, it is no surprise that agencies will tend to default to "dumb."

LACK OF SKILLS

The federal government will not be able to adopt the Internet of Things if it does not have access to the necessary technical skills to make use of the data generated by these systems. Unfortunately, there is a shortage of IT workers in the United States, especially of those skilled at working with data. By 2018, the United States will face a shortage of up to 190,000 workers well-educated in data science and 1.5 million managers and analysts able to use data to make better decisions.[69] A survey of 497 businesses in the China, France, Germany, India, the United Kingdom, and the United States found that this shortage of skilled data workers is a global concern, with only one-third of companies reporting they have the human capital necessary to effectively use new data.[70] While the talent shortage is not limited to the federal government, the public sector will likely feel the impact of this skills shortage more severely than the private sector because executives at federal agencies report that they have difficult recruiting and retaining the highest quality employees and even more difficulty terminating those employees who perform badly.[71] As demand for skills related to data and the Internet of Things continue to grow, the private sector will be able to offer more competitive salaries, while federal agencies may struggle to attract comparable talent. The Federal Chief Information Officers (CIO) Council has recognized this challenge and it has begun to study how best to hire and retain the federal IT workforce.[72]

Our interviews with public and private-sector IT leaders suggest that these workforce issues will likely impact adoption of the Internet of

Things. The majority of respondents thought that the federal workforce lacked the necessary skills to adopt and deploy IoT solutions.[73] In addition, many agencies lack the senior-level leaders needed to take full advantage of the data that they collect now or to lay the groundwork for future data collection. Chief data officers are responsible for establishing an organization's data management strategy, ensuring effective use of information assets, and creating the technical architecture necessary to make use of data. However, only 8 federal agencies—the Departments of Agriculture, Commerce, Health and Human Services, Homeland Security, and Transportation, as well as the General Services Administration, Nuclear Regulatory Commission and the U.S. Agency for International Development—employ a full time Chief Data Officer.[74] Thus many agencies are not likely to have the capacity in the future to adopt IoT technologies that will generate substantial amount of data.

A prerequisite to an agency having the technical capacity to handle new sources of data is a mature data-management strategy.

LACK OF FUNDING

Federal agencies generally lack the necessary funding to adopt and deploy IoT solutions, even if these solutions have a positive return on investment.[75] This reflects a broader problem of insufficient funds available for IT projects. In 2015, the federal budget for IT investments was approximately $87 billion, and it is expected to grow to $89.9 billion by 2017.[76] But the growth rate of federal IT budgets has dramatically decreased over the last few years. From 2001 to 2009, the annual rate of growth in IT spending was 7.1 percent, but it shrunk to remain at 1.8 percent annually since 2009.[77]

Much of the federal spending on the Internet of Things is through the defense budget.[78] In 2015, federal spending on sensors and other connected devices to collect data totaled $4.1 billion, with $1.6 billion of this spent on sensors. Of the spending on sensors, defense agencies accounted for 88 percent of the total. Most of these contracts are with the U.S. Army and U.S. Navy which spent $779 million and $653 million, respectively, between 2011 and 2015 on sensors for surveillance and situational awareness to protect soldiers and supply chains.

Federal modernization efforts have also lagged, contributing to slower adoption of new and innovative technologies. Much of federal IT infrastructure is aging or out of date, and approximately 75 percent of the 2015 federal IT budget was spent to operate and maintain older systems, according to the U.S. Government Accountability Office.[79] While certain programs, such as the Federal Cloud Computing Strategy, have led to more efficient use of these funds, additional funding is necessary to modernize IT systems. To address this challenge, President

Barack Obama has requested a $3.1 billion IT modernization fund from Congress to give agencies the funds to improve or retire outdated IT systems.[80] In the meantime, OMB has begun efforts to promote the adoption of newer systems to replace legacy ones.[81] Unfortunately, since these legacy systems do not involve the Internet of Things, these efforts will likely have little impact on adoption.

INADEQUATE PROCUREMENT POLICIES

Another challenge facing federal adoption and deployment of the Internet of Things is the outdated and burdensome rules and practices governing how federal agencies can purchase technologies. Standard federal procurement practices are designed to purchase tested and mature technologies, not new and promising ones.

First, the federal procurement process makes it difficult to buy and deploy the latest technologies. There are a few methods by which the government can make procurements, including contracts—such as GSA Multiple Award Schedule (MAS) contracts—and open-market acquisition.[82] GSA awards MAS contracts, also known as GSA schedule contracts, which allow federal agencies to acquire 11 million commercial goods and services from contractors.[83] Using these contracts, federal agencies establish Blanket Purchase Agreements (BPAs) with contractors to fill repetitive needs for supplies and services. Unless federal IT vendors are able to establish an IoT solution on an existing BPA, federal procurers cannot buy it—except through open market acquisition.[84] Open-market acquisition allows agencies to purchase commercial products and services not on any federal contract. However, open-market acquisition is a slower process subject to additional determinations—such as whether a purchase is "fair and reasonable"—before agencies can purchase new goods or services.[85] Furthermore, because it can take six months to a year to update BPAs, by the time the procurement process has resulted in the purchase of a particular product, the next generation of that product has already hit the market. This is especially true with the Internet of Things as the technology is rapidly evolving.

Standard federal procurement practices are designed to purchase tested and mature technologies, not new and promising ones.

Second, the federal government's procurement habits are rigid, tending to make large capital expenditures on technology rather than purchasing services or technology in flexible and innovative ways. Some federal agencies are trying to address this challenge through new acquisition programs. For example, DHS created the Homeland Security Innovation Programs (HSIP) that uses a more flexible purchasing method than the lengthy traditional procurement process; this more flexible method, known as Other Transaction Solicitation, allows the agency to request ideas and guide research efforts towards areas that benefit the government the most.[86] The first award this program announced was a $200,000 prize to a California company to help produce "advance detection capability and security monitoring of networked systems, collectively known as the Internet of Things."[87] The federal government broadly will likely need to use flexible mechanisms such as this to make procurement decisions for innovative IoT products and services.

Finally, the federal IT procurement process is more likely to purchase technology hardware, software, and services rather than issue a contract to achieve specific business outcomes—even if the former is riskier and more expensive. For example, suppose an agency wanted to use smart building technology to increase the energy efficiency of its headquarters. It could purchase the technology to create a sensor network and hire contractors to build and install the hardware, create the infrastructure it needs to operate on, and design and operate the underlying analytics platform. At the end of the day, the federal agency alone would bear the risk of failure, such as if the project did not actually achieve the desired energy efficiency savings. Alternatively, the agency could issue a contract for the specific outcomes it wanted, such as a 10 percent reduction in energy use, and shift much of this risk to the private sector. However, since government agencies are not accustomed to operate in this manner, they tend to avoid this approach.

UNWILLINGNESS TO TAKE ON ASSOCIATED RISKS

Because many uses of the Internet of Things by the federal government are relatively new and untested, federal agencies may be inclined to delay adoption until the technology is more mature and others have tested it. Adopting technology can be risky, and the leaders in federal agencies have little incentive to take on this risk since, unlike in the private sector, there is little payoff for success and a substantial downside to failure.

There are five primary categories of risk associated with the Internet of Things for federal adopters: privacy; security; interoperability; data governance; and return on investment.

Privacy

One risk federal agencies face is failure to properly protect the privacy of personal data collected through their use of the Internet of Things. The federal government gathers a lot of data about government workers and the public, and government projects that make use of the Internet of Things will necessarily involve collecting more data. The public sector has important responsibilities when it comes to protecting the confidentiality of the information that it collects and shares between different agencies. Without careful consideration of privacy, the government can invite the accusation that it is violating the privacy of the public, creating mistrust and resistance to the adoption of new technology. Some agencies are trying to address potential concerns early on by limiting what information they collect and ensuring that the data collected is stored securely. For example, in 2013 the Federal Communications Commission (FCC) experimented with an open-source mobile app that allowed users to monitor their broadband connection speeds; if they wanted to share that result anonymously, the app would pass the data to the agency to inform evidence-based decisionmaking.[88] To ensure a high degree of user trust, the FCC used strong privacy controls, so that it did not know who the users were or their location within a 5-mile radius.

Security

Another risk for federal agencies is that they will not properly secure their uses of the Internet of Things. The federal government already struggles with securing its IT systems, suffering a number of high-profile data breaches in the past few years. The Internet of Things represents a new set of technologies that need to be secured.[89] Each new device that is connected to the network could potentially introduce new vulnerabilities. Moreover, connected devices can have a number of properties that make them more useful and convenient, but that also make them a greater security risk. For example, mobile devices may use low-power processors to conserve battery power, which limits the device's ability to perform computationally complex operations, such as encrypting data.

The Internet of Things also has unique security consequences that do not exist in purely digital systems. In particular, industrial control systems, including supervisory control and data acquisition (SCADA) systems, which are used to remotely monitor and manage complex industrial processes such as electric power generation and wastewater treatment, present serious security risks that should be managed properly. Vulnerabilities in these systems can put physical infrastructure itself at risk if the system fails or is sabotaged by attackers. The result can be a disruption of essential services to millions of individuals.[90]

Interoperability

Interoperability—the ability of different IT systems to communicate, exchange data, and cooperatively use that data—is a necessary component of large-scale IoT deployments, both in the public and private sector. Interoperability requires not only that systems be networked together, but that data from each system be interoperable. Without interoperability, the federal government cannot fully use the information it gathers from sources like the Internet of Things.

Data Governance

Similarly, the federal government needs to be able to store, process, and analyze the data it collects in order to gain value from it.[91] Unfortunately, most federal agencies are ill-equipped to process and analyze the new streams of data that would result from IoT adoption. As a result, some federal IT leaders may even see collecting large amounts of data from the Internet of Things to be a liability, because if they do not know how to put this data to good use and manage it responsibly, they may be found at fault for not acting on this information in the event of an emergency.[92]

Return on Investment

Another uncertainty that affects public-sector deployment of the Internet of Things is a lack of understanding of the costs and benefits of the technology. In many cases, the return on investment (ROI) for the Internet of Things has simply not been fully explored, making many federal IT decisionmakers hesitant to adopt the technology. This is generally because the technology has not had a chance to mature, and there are relatively few federal-use cases to demonstrate its value. Those that do exist, such as smart metering and connected buildings, have demonstrated their ROI potential and are more likely to be adopted by federal agencies.

Another factor contributing to the uncertainty around ROI is scale. Due to the smaller scale, ROI is easier to demonstrate in state and local government applications of the Internet of Things. For example, it is easier to launch a public smart-meter pilot in a single city and to monitor its impact, than it is to roll out that same program throughout the country.

RECOMMENDATIONS

Federal adoption of the Internet of Things can improve the efficiency and effectiveness of federal agencies, spur commercial innovation in related products and services, lower the costs for this emerging technology, and promote stronger security features for smart devices. Moreover, by being a lead adopter of the Internet of Things, the federal government can drive broader adoption of Internet of Things in the U.S. economy, thereby boosting U.S. competitiveness.[93] As such, the federal government should take a number of steps to overcome the broad array of challenges facing federal government adoption of the Internet of Things. In addition, there are a number of important steps the federal government should take to support the development of the technology as a whole, which will lead to both public and private sector benefits.

HOW TO IMPROVE FEDERAL GOVERNMENT USE OF THE INTERNET OF THINGS

Many of the challenges limiting the federal government's use of the Internet of Things would be greatly diminished with better guidance and management. However, considering that one of the biggest barriers to IoT adoption in the federal government is a general lack of in-depth knowledge about the technology, federal agency leaders must first improve their own understanding of how they can use the technology. There are several key steps the federal government should take to address this challenge.

First, the Federal Chief Information Officers Council should establish an Internet of Things taskforce responsible for providing cross-government leadership on this technology. The IoT taskforce should be charged with educating agency leadership about the technology, fostering collaboration across agencies, and developing and sharing best practices for deploying IoT applications in the federal government. An important part of the Council's work should be to identify how to reform procurement policies so that agencies can purchase IoT solutions more easily and with less delay. As successful adoption of the Internet of Things will also require a workforce equipped with the skills necessary to deploy connected technologies, ensure interoperability, and work with data generated by IoT applications, the IoT taskforce should also work with the Council's Workforce committee and the Office of Management and Budget to develop data skills training programs for federal employees.

Second, each major federal agency should develop its own action plan for how it will use the Internet of Things to both cut costs and improve the quality of its services. Agency action plans should focus on making "smart" the default for government operations, such as by requiring the use of connected technologies for customs inspections, integrating smart technologies into government-subsidized housing and agency buildings; and embedding sensor networks into infrastructure as part of modernization efforts.[94] These action plans should not only identify opportunities to use the Internet of Things, but also address any unique obstacles the agency faces to adopting and using the technology. In addition, IoT action plans should explain how agencies plan to realign their operations around the new opportunities presented by the Internet of Things and the data these technologies generate.

Importantly, agency IoT action plans should include strategies to reduce the risk and uncertainty of the Internet of Things, both of which substantially limit the federal government's willingness to adopt the technology. There are several promising ways agencies could approach this problem. Agencies should launch pilot projects to test various IoT use-cases that support low-risk, high-value, and mission-oriented projects that are relatively easy to implement and analyze. Once each pilot program has been implemented, the federal agency conducting the experiment should do cost-benefit analysis to establish the project's benefits and whether it can be rolled out in other areas. This information should be made public so that other agencies can evaluate whether they can adopt it as well. Projects in the near term may include, but are not limited to, smart-building applications, fleet tracking and asset management, managing commodities in intelligent ways, and automating routine or back-office processes to get more staff out into the field. By pursuing a multitude of IoT pilot projects, agencies can quickly identify the most valuable and beneficial ones for rapid scale-up. These lessons learned can quickly be shared across federal agencies through the proposed Federal CIO Council's IoT Task Force.

Agency action plans should also identify and pursue opportunities to use the Internet of Things to improve workplace accessibility. The federal government, which at the end of FY2014 employed 247,000 people with disabilities, has long been a leader in providing workplace accommodations for people with disabilities; IoT offers considerable potential to make federal agencies more accessible to these workers.[95] For example, Bluetooth beacon technology dispersed throughout a building can provide audio cues via a smartphone app to help people with vision impairments navigate physical spaces or provide contextual information.[96]

The federal government should also establish a process similar to the Federal Risk and Authorization Management Program (FedRAMP), designed to facilitate federal agency cloud adoption, to expedite federal agency adoption of the Internet of Things. FedRAMP certifies cloud products and services based on standardized security assessments, saving federal agencies substantial amounts of time and money by reducing the need for them to carry out their own assessments. It also provides a clear signal to private-sector vendors about federal security requirements.[97] A FedRAMP-style program designed for the Internet of Things could offer similar security assessments, as well as address other risk factors limiting IoT adoption, including privacy and interoperability issues.

Third, every major federal agency that has not done so already should employ a chief data officer that works in tandem with the agency chief information officer to inject valuable data expertise into agency decisionmaking about how to use the Internet of Things. Agencies that do not have the technical infrastructure to manage massive amounts of data are going to be unable to adopt the Internet of Things. The fact that so few agencies have chief data officers undoubtedly contributes to the slow adoption rates, risk of non-interoperable systems, and other impediments to the federal government's use of the Internet of Things.[98] By creating a leadership position specifically focused on data use and management, federal agencies could increase their ability to understand how the Internet of Things can help mission delivery and substantially improve policies and practices governing how agencies procure, deploy, and use IoT technologies.

Fourth, GSA should establish an "IoT Corps"—a team of government employees who can be assigned to work on high-impact IoT projects at federal agencies. The goal of the IoT Corps would be to develop a strong federal workforce with the skills needed to deploy the Internet of Things, without locking these employees into working at a particular agency. Instead, members of the IoT Corps could rotate to new assignments every couple of years based on new projects, agency needs, and available funding. This model of government service would build off some of the successful aspects of 18F and the U.S. Digital Service.

HOW FEDERAL AGENCIES SHOULD SUPPORT THE DEVELOPMENT OF THE INTERNET OF THINGS

There are several challenges facing the growth of the Internet of Things as a whole that the private sector alone cannot solve; by addressing these challenges the federal government will create substantial secondary benefits with regard to its own use of the Internet of Things. As noted previously, by becoming an early adopter of the Internet of Things, the federal government can promote broader adoption of the Internet of Things throughout the economy. Thus, federal agencies should consider more than how they alone will use the Internet of Things.

Federal agencies should fund and support large-scale state and municipal pilot projects that focus on scalable and replicable IoT applications. If a city has the opportunity to receive federal assistance to experiment with the Internet of Things, not only would it be more likely to carry out such projects, but other cities would then be able to look to these efforts to learn best practices and replicate their successes. This would also have the added benefit of signaling to the private sector that there will be a viable market for these technologies, encouraging firms to scale up production and thus lowering costs. By making strong security practices a pre-requisite for participation in these projects, the government can also push the private sector to invest more in security for the Internet of Things.

Federal agencies should prioritize funding for projects with high social or economic impact, such as those that address expensive chronic health issues, as well as those with the potential to scale nationally. Many of these projects will have value to certain federal agencies. For example, military bases—which function like small cities, operating independently with residences, hospitals, police stations, and grocery stores—are looking to use proven IoT solutions that result from DOT's Smart Cities Challenge to improve their energy efficiency and reduce costs.[99] Just as federal agencies should carry out their own pilot projects to reduce the risk associated with the Internet of Things, encouraging state and local governments to do the same will have a similarly beneficial effect.

Though interoperability is an immediate concern for the federal government's own use of IoT, it is also a concern for a much broader group of stakeholders, particularly private firms. Though industry should lead standards development, the federal government should use its ability to bring together disparate market players, local governments, standards bodies, and other groups to encourage the adoption of common standards and promote interoperability where needed.

Similarly, federal agencies should engage with the private sector to encourage the development of industry-led voluntary standards and best practices around issues such as privacy and cybersecurity, as well as seek opportunities to promote international collaboration on industry-led, consensus-based standards adoption. The federal government should also push back against other countries' efforts to implement nation-specific standards for connected technologies or limit how data from these devices can flow across borders.[100]

While federal agencies have been slow to adopt IoT technologies, a number of them have already established R&D projects and devoted a considerable amount of research funding for the Internet of Things. The federal government should encourage these efforts, focusing on key underlying technological challenges of the Internet of Things, such as improving cybersecurity and developing low-cost battery technologies. For example, the National Science Foundation could establish one or more Engineering Research Centers focused on particular applications of the Internet of Things. These efforts would benefit all market players and support the development of new IoT applications, including public sector ones.

Another promising method of funding R&D initiatives that generate significant value is a government-backed venture capital program targeted specifically for firms developing innovative IoT applications. For example, the Central Intelligence Agency's venture capital arm In-Q-Tel invests in companies developing cutting-edge technologies that can enhance the capability of federal intelligence agencies, many of which have also generated significant private-sector value, such as touch-screen technology used in many consumer smartphones and the satellite imaging technology that went on to become Google Earth.[101] A similar venture capital project could accelerate the development and commercialization of federal IoT applications.

Finally, while federal agencies have taken several steps to examine the spectrum needs of IoT and free up additional spectrum, they should remain vigilant about monitoring spectrum availability as the number of connected devices rapidly increases to avoid any bottlenecks that could lead to device failure.[102]

CONCLUSION

There are many opportunities for the federal government to use the Internet of Things to make government services better and more efficient. While the federal government has launched a number of projects to use the Internet of Things, overall adoption, especially in non-defense applications, remains low. In addition, federal agencies face a number of challenges to adoption. These findings suggest that federal government adoption of the Internet of Things will likely continue to lag behind that of the private sector unless changes are made to encourage adoption across federal agencies.

REFERENCES

1. Interviews conducted by authors with relevant experts in May and June 2016. See methodology section for additional notes.

2. "New Smart Building Technology to Increase Federal Buildings Energy Efficiency," *General Services Administration*, news release, May 14, 2012, http://www.gsa.gov/portal/content/135115; "GSA to Increase Energy Efficiency and Reduce Costs in Federal Buildings," *General Services Administration*, news release, May 17, 2012, http://gsablogs.gsa.gov/gsablog/2012/05/17/gsa-to-increase-energy-efficiency-and-reduce-costs-in-federal-buildings/.

3. Tom Shircliff and Rob Murchison, "GSA BuildingLink Leverages a Minimum of 1,000 Data Points Per Building," *Realcomm*, February 21, 2013, http://www.realcomm.com/advisory/571/1/gsa-buildinglink-leverages-a-minimum-of-1000-data-points-per-building.

4. Mohana Ravindranath, "At GSA, an 'Internet of Things' experiment," *Washington Post*, August 31, 2014, https://www.washingtonpost.com/business/on-it/at-gsa-an-internet-of-things-experiment/2014/08/30/403c620c-2e10-11e4-994d-202962a9150c_story.html.

5. Ravindranath, "At GSA, an 'Internet of Things' experiment"; Shircliff and Murchison, "GSA BuildingLink Leverages a Minimum of 1,000 Data Points Per Building."

6. Interviews conducted by authors with relevant experts in May and June 2016. See methodology section for additional notes.; Caroline D'Angelo, "The Greening Diplomacy Initiative: Capturing Innovation," *American Foreign Service Association*, April 2014, http://www.afsa.org/greening-diplomacy-initiative-capturing-innovation; "2014 Strategic Sustainability Performance Plan," *U.S. Department of State*, June 28, 2014, http://www.state.gov/documents/organization/233777.pdf.

7. Ravindranath, "At GSA, an 'Internet of Things' experiment."

8. Ibid.

9. Ibid.

10. Heather Hayes, "Agencies Tap Automation Tools for Greater Data Center Efficiencies," *FedTech*, July 28, 2015, http://www.fedtechmagazine.com/article/2015/07/agencies-tap-automation-tools-greater-data-center-efficiencies.

11. Ravindranath, "At GSA, an 'Internet of Things' experiment."

12. Natalie Grasso, "GSA Video and Case Study: Work is What You Do, Not Where You Are," *Work Design Magazine*, January 11, 2016, http://workdesign.com/2016/01/gsa-case-study-and-video-work-is-what-you-do-not-where-you-are/; "10 Keys to Office Hoteling Success," *General Services Administration*, accessed July 21, 2016, http://www.gsa.gov/graphics/admin/Successful-Hoteling-Tips_Final.pdf.

13. Carten Cordell, “GSA offers telematics data sharing on fleet vehicles,” *Federal Times*, December 2, 2015, http://www.federaltimes.com/story/government/acquisition/gsa-gwac/2015/12/02/gsa-offers-telematics-data-sharing-fleet-vehicles/76657862/; “GSA Fleet - Leading the Way,” *General Services Administration*, accessed May 31, 2016, http://www.gsa.gov/portal/content/104624.

14. “GSA Fleet - Leading the Way,” *General Services Administration.*

15. General Services Administration (GSA), “GSA Fleet – Telematics” (Washington, DC: GSA, 2016), http://www.gsa.gov/portal/mediaId/123678/fileName/telematics_fact_sheet_26Jan2016.action.

16. General Services Administration (GSA), “GSA Fleet – Telematics.”

17. General Services Administration (GSA), “GSA Fleet – Telematics”; Robert Prime, “The Main Benefits of Fleet Tracking,” *Telematics.com*, October 29, 2013,http://www.telematics.com/main-benefits-fleet-tracking/.

18. Michael Frank, “How Telematics Has Completely Revolutionized the Management of Fleet Vehicles,” *Entrepreneur*, October 20, 2014, https://www.entrepreneur.com/article/237453; “Big Data = Big Wins for the Environment,” United Parcel Service (UPS), 2013, http://sustainability.ups.com/media/UPS-Big-Data-Infographic.pdf.

19. “Passive Radio Frequency Identification,” *Office of the Under Secretary of Defense for Acquisition, Technology and Logistics*, October 2010, http://www.acq.osd.mil/dpap/dars/dfars/html/current/252211.htm#252.211-7006.

20. “Lockheed Martin Selected To Maintain In-Transit Visibility Program To Ensure Accurate And Timely DOD Shipments,” *Lockheed Martin*, September 8, 2014, http://www.lockheedmartin.com/us/news/press-releases/2014/september/isgs-igc-0908.html.

21. Denise Zheng and William Carter, “Leveraging the Internet of Things for a More Efficient and Effective Military,” *Center for Strategic and International Studies*, September 2015, https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/150915_Zheng_LeveragingInternet_WEB.pdf.

22. “Sowing the Internet of Things into agriculture,” *GCN*, January 15, 2015, https://gcn.com/blogs/emerging-tech/2015/01/agriculture-iot.aspx.

23. Jonathan Shieber, “US DOT and Alphabet’s Sidewalk Labs aim to create new public transit and Wi-Fi networks,” *TechCrunch*, March 17, 2016, http://techcrunch.com/2016/03/17/u-s-dot-and-sidewalk-labs-hustle-and-flow/.

24. Interviews conducted by authors with relevant experts in May 2016. See methodology section for additional notes; “The Internet of Things

for Defense," Wind River, 2015, http://www.windriver.com/whitepapers/iot-for-defense/wind-river_%20IoT-in-Defense_white-paper.pdf; David Alberts, John Garstka, and Frederick Stein, "Network Centric Warfare," *CCRP*, February 2000, http://www.dodccrp.org/files/Alberts_NCW.pdf.

25. Zheng and Carter, "Leveraging the Internet of Things for a More Efficient and Effective Military."

26. Zheng and Carter, "Leveraging the Internet of Things for a More Efficient and Effective Military."

27. Phuong Lee, "Navy wants to increase use of sonar-emitting buoys off Pacific Coast," *Navy Times*, January 25, 2015, http://www.navytimes.com/story/military/tech/2015/01/25/navy-wants-to-increase-use-of-sonar-emitting-buoys-off-pacific-coast/22315829/.

28. Zheng and Carter, "Leveraging the Internet of Things for a More Efficient and Effective Military."

29. "About DCGS-A," *Distributed Common Ground System – Army*, accessed May 31, 2016, https://dcgsa.army.mil/about/.

30. "Multi-Mission Capability for Emerging Global Threats," *F35*, 2016, https://www.f35.com/about/capabilities.

31. Lockheed Martin, "The F-35. How it Works," *Washington Post*, accessed May 31, 2016, http://www.washingtonpost.com/sf/brand-connect/the-f-35-how-it-works/.

32. Kris Osborn, "Pentagon Unveils Program to Help Build 6th Generation Fighter," *DoD Buzz*, January 28, 2015, http://www.dodbuzz.com/2015/01/28/pentagon-unveils-new-program-to-help-develop-6th-generation-fighter/.

33. Claire Swedberg, "RFID Plays Crucial Military Role in Middle East," *RFID Journal*, April 29, 2009, http://www.rfidjournal.com/articles/view?4837/; "RFID Technology: Keeping Track of DoD's Stuff," *Defense Industry Daily*, July 13, 2010, http://www.defenseindustrydaily.com/rfid-technology-keeping-track-of-dods-stuff-05816/.

34. Swedberg, "RFID Plays Crucial Military Role in Middle East."

35. Zheng and Carter, "Leveraging the Internet of Things for a More Efficient and Effective Military."

36. Zheng and Carter, "Leveraging the Internet of Things for a More Efficient and Effective Military."

37. Zheng and Carter, "Leveraging the Internet of Things for a More Efficient and Effective Military."

38. Kevin Sablan, "Helmet sensors help Army study brain injury," *The Orange County Register*, August 21, 2013, http://www.ocregister.com/articles/brain-496474-sensors-helmet.html.

39. "DHA Health IT uses the Internet of Things to monitor health, improve readiness," *U.S. Defense Health Agency*, June 29, 2015,

http://www.health.mil/News/Articles/2015/06/29/DHA-Health-IT-uses-the-Internet-of-Things-to-monitor-health-improve-readiness.

40. "Self-Powered Biosensors," *U.S. Defense Health Agency*, accessed May 24, 2016, http://www.health.mil/Reference-Center/Fact-Sheets/2015/12/01/Self-Powered-BioSensors.

41. Mark Pomerleau, "Air Force successfully tests wearable biometric sensors," *GCN*, October 6, 2015, https://gcn.com/articles/2015/10/06/biostamprc.aspx.

42. David McNally, "Army evaluates DARPA's futuristic soft exosuit," *U.S. Army*, October 28, 2014, https://www.army.mil/article/135272/Army_evaluates_DARPA_s_futuristic_soft_exosuit/.

43. "Office of the Press Secretary, "FACT SHEET: Obama Administration Announces New Revolutionary Fibers and Textiles Manufacturing Innovation Hub in Cambridge, MA and New Report on $2 Billion in Manufacturing R&D Investments," The White House, *press* release, April 1, 2016, https://www.whitehouse.gov/the-press-office/2016/04/01/fact-sheet-obama-administration-announces-new-revolutionary-fibers-and.

44. "What is remote sensing?" *U.S. National Oceanic and Atmospheric Administration*, accessed May 31, 2016, http://oceanservice.noaa.gov/facts/remotesensing.html.

45. "Data Access," *U.S. National Oceanic and Atmospheric Administration*, accessed May 31, 2016, https://www.ncdc.noaa.gov/data-access.

46. "About Us," *U.S. National Oceanic and Atmospheric Administration*, accessed May 31, 2016, https://www.ncdc.noaa.gov/about.

47. "Data Processing," *U.S. Geological Survey*, February 13, 2012, http://nsmp.wr.usgs.gov/processing.html.

48. "Earthquake Early Warning," *U.S. Geological Survey*, last modified April 6, 2016, http://earthquake.usgs.gov/research/earlywarning/.

49. "Earthquake Early Warning," *U.S. Geological Survey.*

50. "Apex Programs," Department of Homeland Security, n.d., https://www.dhs.gov/science-and-technology/apex-programs.

51. "Next Generation First Responder Apex Program," *Department of Homeland Security*, n.d., https://www.dhs.gov/science-and-technology/ngfr.

52. Reginald Brothers, "S&T's Internet of Things Pilot Demonstrates 'State of the Practical'," *U.S. Department of Homeland Security*, January 25, 2016, https://www.dhs.gov/science-and-technology/blog/2016/01/25/st-internet-things-pilot-demonstrates-state-practical. Greg Otto, "DHS funds smart shirts for first responders," *Fedscoop*, February 1, 2016, http://fedscoop.com/dhs-funded-project-helps-smart-shirts-save-first-responders.

53. "Mining Project: Industrial Internet of Things (IIoT) Applications in Underground Coal Mines," *Centers for Disease Control and Prevention*,

December 10, 2015, http://www.cdc.gov/niosh/mining/researchprogram/projects/project_IndustrialInternet.html.

54. Tim Moyniham, "The New Tech of Disaster Response, from Apps to Aqua-Drones," *Wired*, August 29, 2015, http://www.wired.com/2015/08/fema-disaster-tech/.

55. "Crisis Response and Disaster Resilience 2030: Forging Strategic Action in an Age of Uncertainty," *FEMA*, January 2012, http://www.fema.gov/media-library-data/20130726-1816-25045-5167/sfi_report_13.jan.2012_final.docx.pdf.

56. "NASA Satellites Eye Forest Fires," *National Aeronautics and Space Administration*, August 13, 2003, http://www.jpl.nasa.gov/news/news.php?release=2003-113.

57. "Global Fire Monitoring," *National Aeronautics and Space Administration*, accessed May 31, 2016, http://earthobservatory.nasa.gov/Features/GlobalFire/fire_5.php.

58. "NASA Satellites Eye Forest Fires," *National Aeronautics and Space Administration*.

59. Catherine Andrews et al., "What the IoT Means for the Public Sector," *GovLoop*, 2015, http://www.isaca.org/Groups/Professional-English/cybersecurity/GroupDocuments/IoT%20in%20the%20Public%20Sector.pdf.

60. "Remote Sensing Information Gateway," *U.S. Environmental Protection Agency,* last updated May 12, 2016, https://www.epa.gov/hesc/remote-sensing-information-gateway.

61. "Guide to Green Embassies," *U.S. Department of State*, accessed April 21, 2016, http://overseasbuildings.state.gov/sites/admin-overseasbuildings.state.gov/files/pdfs/green_guide_-_final_for_posting_01142014_upload.pdf; "Mission China," *State Air*, accessed May 24, 2016, http://www.stateair.net/web/post/1/1.html.

62. U.S. Department of State, "U.S. Environmental Protection Agency Launch Innovative International Air Quality Program," news release, February 18, 2015, http://www.state.gov/r/pa/prs/ps/2015/02/237573.htm; "AirNow Department of State," *AirNow*, accessed May 31, 2016, https://airnow.gov/index.cfm?action=airnow.global_summary#Indonesia$Jakarta_Central.

63. "Kena Fedorschak, Kevin C. Desouza and Gregory Dawson, "Federal agencies behind the curve: IoT and BYOD," *Brookings Institution*, March 16, 2015, http://www.brookings.edu/blogs/techtank/posts/2015/03/16-iot-byod-government-computers.

64. The Government Performance and Results Modernization Act of 2010 requires every federal agency to produce a strategic plan every four years that describes the long-term goals of the agency, how it will realize those goals, and the challenges and risks that the agency faces

to achieve those goals. For more, see “Section 230—Agency Strategic Planning,” *White House*, 2016, https://www.whitehouse.gov/sites/default/files/omb/assets/a11_current_year/s230.pdf.

65. Catherin Andrews, “The Internet of Things: Preparing yourself for a Connected Government,” *GovLoop*, 2014, https://www.vion.com/assets/site_18/files/gl_guide_iot_final%20(3).pdf

66. “Achieving Holistic Federal Cybersecurity: A Candid Survey of Federal Managers,” *Government Business Council*, April 2016, http://www.govexec.com/insights/reports/achieving-holistic-cybersecurity-2016-progress-report/127435/.

67. Please note the 2014 survey had on 424 participants, a decrease of 40. “Achieving Holistic Federal Cybersecurity: A Candid Survey of Federal Managers,” *Government Business Council*, June 2014, http://cdn.govexec.com/media/gbc/docs/gbc_dell_cybersecurity_insightreport_final.pdf.

68. Interviews conducted by authors with relevant experts in May and June 2016. See methodology section for additional notes.

69. James Manyika et al., “Big Data: The Next Frontier for Innovation, Competition, and Productivity,” *McKinsey Global Institute*, May 2011, http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation.

70. “Data Science Revealed: A Data-Driven Glimpse into the Burgeoning New Field,” *EMC*, 2011, http://www.emc.com/collateral/about/news/emcdata-science-study-wp.pdf.

71. “Survey on the Future of Government Service,” *Center for the Study of Democratic Institutions*, July 16, 2015, http://www.vanderbilt.edu/csdi/research/sfgs.php.

72. “CIO Council Looks to Data to Optimize IT Workforce,” *CIO Council*, February 17, 2015, https://cio.gov/cio-council-looks-data-optimize-workforce/.

73. Interviews conducted by authors with relevant experts in May and June 2016. See methodology section for additional notes.

74. “Chief Data Officers,” *Project Open Data*, accessed May 29, 2016, https://project-open-data.cio.gov/chief-data-officers/.

75. “Information Technology,” *White House*; Interviews conducted by authors with relevant experts in May and June 2016. See methodology section for additional notes.

76. See budget information. “Information Technology,” *White House*, accessed May 29, 2016, https://www.whitehouse.gov/sites/default/files/omb/budget/fy2017/assets/ap_17_it.pdf

77. “Information Technology,” *White House.*

78. “The Internet of Things: Sensors and Data Collectors,” *Govini*, 2016, http://www.govini.com/research-item/internet-of-things-sensors/.

79. “Federal Agencies Need to Address Aging Legacy Systems,” *U.S. Government Accountability Office*, May 25, 2016, http://gao.gov/products/GAO-16-468.

80. Jason Miller, “White House raises cyber stakes with request for 35 percent increase in 2017,” *Federal News Radio*, February 9, 2016, http://federalnewsradio.com/budget/2016/02/white-house-raises-cyber-stakes-request-35-percent-increase-2017/

81. Jason Miller, “OMB draft policy begins IT modernization with or without Congress,” *Federal News Radio*, February 29, 2016, http://federalnewsradio.com/omb/2016/02/omb-draft-policy-begins-modernization-without-congress/.

82. “GSA Schedules Frequently Asked Questions,” *U.S. General Services Administration*, accessed May 31, 2016, http://www.gsa.gov/portal/content/203021.

83. Ibid.

84. Interviews conducted by authors with relevant experts in May and June 2016. See methodology section for additional notes.

85. “GSA Schedules Frequently Asked Questions,” *U.S. General Services Administration.*

86. Aaron Boyd, “DHS calls on Silicon Valley to help secure the IoT,” *Federal Times*, January 7, 2016, http://www.federaltimes.com/story/government/dhs/2016/01/06/dhs-silicon-valley-iot/78357474/.

87. DHS Science & Technology, “DHS S&T Awards $200K for Internet of Things Systems Security,” *U.S. Department of Homeland Security*, news release, February 22, 2016, https://www.dhs.gov/science-and-technology/news/2016/02/22/st-awards-200k-internet-things-systems-security.

88. “FCC Speed Test App Tip Sheet,” *Federal Communications Commission*, September 4, 2013, https://www.fcc.gov/consumers/guides/fcc-speed-test-app-tip-sheet

89. Gregory Wilshusen, “Recent Data Breaches Illustrate Need for Strong Controls across Federal Agencies,” *U.S. Government Accountability Office*, June 24, 2015, http://www.gao.gov/assets/680/670935.pdf; James Eng, OPM Hack: Government Finally Starts Notifying 21.5 Million Victims,” *NBS News*, October 1, 2015, http://www.nbcnews.com/tech/security/opm-hack-government-finally-starts-notifying-21-5-million-victims-n437126.

90. Robert Atkinson, Daniel Castro, Stephen Ezell, Alan McQuinn, and Joshua New, “A Policymaker’s Guide to Digital Infrastructure,” *Information Technology and Innovation Foundation,* May 2016, http://www2.itif.org/2016-policymakers-guide-digital-infrastructure.pdf.

91. Interviews conducted by authors with relevant experts in May and June 2016. See methodology section for additional notes.

92. Interviews conducted by authors with relevant experts in May and June 2016. See methodology section for additional notes.

93. Joshua New and Daniel Castro, "Why Countries Need National Strategies for the Internet of Things," *Center for Data Innovation*, December 16, 2015, http://www2.datainnovation.org/2015-national-iot-strategies.pdf.

94. Robert D. Atkinson et al., "A Policymaker's Guide to Digital Infrastructure," *Information Technology and Innovation Foundation*, May 2016, http://www2.itif.org/2016-policymakers-guide-digital-infrastructure.pdf.

95. Meredith Somers, "Record number of people with disabilities in federal workforce," *Federal News Radio*, October 13, 2015, http://federalnewsradio.com/workforce/2015/10/record-number-people-disabilities-federal-workforce/ and "Disabilities," *White House*, accessed May 29, 2016, https://www.whitehouse.gov/issues/disabilities.

96. Liz Stinson, "Guiding the Blind Through London's Subway with Estimote Beacons," *Wired*, http://www.wired.com/2015/03/blind-will-soon-navigate-london-tube-beacons/.

97. "Program Overview," *FedRAMP*, accessed May 29, 2016, https://www.fedramp.gov/about-us/about/.

98. "Chief Data Officers and Chief Data Scientists," *Project Open Data*, accessed May 29, 2016, https://project-open-data.cio.gov/chief-data-officers/.

99. Interviews conducted by authors with relevant experts in May and June 2016. See methodology section for additional notes.

100. Robert D. Atkinson, "Testimony Before U.S. House Ways and Means Subcommittee on Digital Trade," *Information Technology and Innovation Foundation*, July 13, 2016, https://itif.org/publications/2016/07/13/testimony-us-house-ways-and-means-subcommittee-digital-trade.

101. Steve Henn, "In-Q-Tel: The CIA's Tax-Funded Player In Silicon Valley," *NPR*, July 6, 2012, http://www.npr.org/sections/alltechconsidered/2012/07/16/156839153/in-q-tel-the-cias-tax-funded-player-in-silicon-valley.

102. Doug Brake, "5G and Next Generation Wireless: Implications for Policy and Competition," *Information Technology and Innovation Foundation*, June 30, 2016, https://itif.org/publications/2016/06/30/5g-and-next-generation-wireless-implications-policy-and-competition.

ABOUT THE AUTHORS

Daniel Castro is the director of the Center for Data Innovation and vice president of the Information Technology and Innovation Foundation.

Joshua New is a policy analyst at the Center for Data Innovation.

Alan McQuinn is a research analyst at the Information Technology and Innovation Foundation.

ACKNOWLEDGEMENTS

The authors wish to thank the experts who agreed to be interviewed for this report, and also note that the report's conclusions are the authors' and do not necessarily represent the views of either interviewees or their employers.

ABOUT THE CENTER FOR DATA INNOVATION

The Center for Data Innovation is the leading global think tank studying the intersection of data, technology, and public policy. With staff in Washington, DC and Brussels, the Center formulates and promotes pragmatic public policies designed to maximize the benefits of data-driven innovation in the public and private sectors. It educates policymakers and the public about the opportunities and challenges associated with data, as well as technology trends such as predictive analytics, open data, cloud computing, and the Internet of Things. The Center is a nonprofit, non-partisan research institute affiliated with the Information Technology and Innovation Foundation.

contact: info@datainnovation.org

datainnovation.org