United States Government Accountability Office

Report to Congressional Requesters

July 2017

INTERNET OF THINGS

Communities Deploy Projects by Combining Federal Support with Other Funds and Expertise

Accessible Version

GAO-17-570

July 2017

INTERNET OF THINGS

Communities Deploy Projects by Combining Federal Support with Other Funds and Expertise

GAO Highlights

Highlights of GAO-17-570, a report to congressional requesters

Why GAO Did This Study

Communities are increasingly deploying IoT devices generally with a goal of improving livability, management, service delivery, or competitiveness. GAO was asked to examine federal support for IoT and the use of IoT in communities. This report describes: (1) the kinds of efforts that selected federal agencies have undertaken to support IoT in communities and (2) how selected communities are using federal funds to deploy IoT projects.

GAO reviewed documents and interviewed officials from 11 federal agencies identified as having a key role in supporting IoT in communities, including agencies that support research or community IoT efforts or that have direct authority over IoT issues. GAO interviewed a non-generalizeable sample of representatives from multiple stakeholder groups in four communities, selected to include a range of community sizes and locations and communities with projects that used federal support. GAO also reviewed relevant literature since 2013 and discussed federal efforts and community challenges with 11 stakeholders from academia and the private sector, selected to reflect a range of perspectives on IoT issues.

GAO requested comments on a draft of this product from 11 federal agencies. Five agencies provided technical comments, which GAO incorporated as appropriate. Six agencies did not provide comments.

View GAO-17-570. For more information, contact Mark Goldstein at (202) 512-2834 or goldsteinm@gao.gov or Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov.

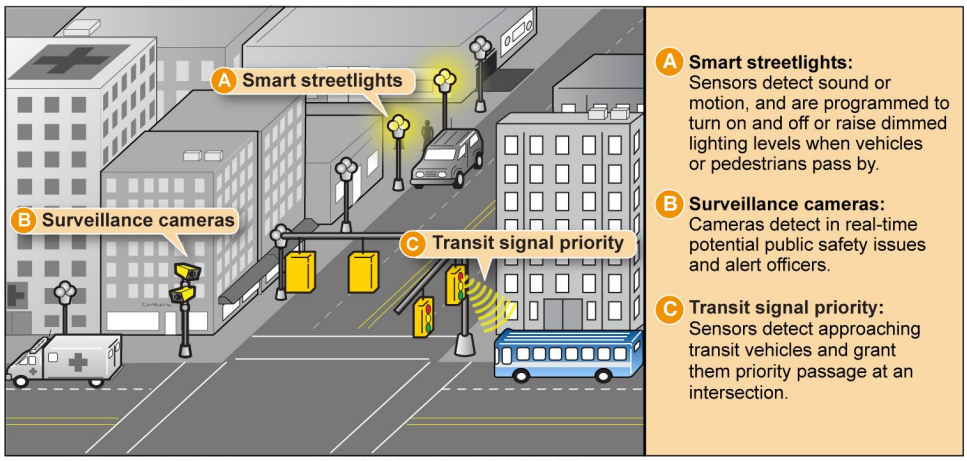
What GAO Found

The internet of things (IoT) generally refers to the technologies and devices that allow for the network connection and interaction of a wide array of devices, or "things." Federal agencies that GAO reviewed are undertaking two kinds of efforts that support IoT in communities:

- *Broad federal research and oversight of IoT-related technologies and issues:* For example, 8 of the 11 agencies GAO reviewed are involved in broad research efforts, often on communication systems—both wired and wireless network systems. In addition, nine agencies have oversight efforts that include providing IoT-related guidance, often on data security and privacy.
- *More direct efforts to support communities, including funding community IoT projects (see figure) and fostering collaboration among the agencies and communities:* For example, DOT recently awarded $40 million in federal funds to a community for a suite of "smart" projects related to improving surface transportation performance, and EPA awarded $40,000 each to two communities to develop strategies for deploying air quality sensors and managing the data collected from them. To foster such collaboration, in July 2016, the White House formed an interagency task force that has developed a draft *Smart Cities and Communities Federal Strategic Plan*. A final plan will be released in summer of 2017, according to federal officials.

All four of the communities that GAO reviewed are using federal funds in combination with other resources, both financial and non-financial, to plan and deploy IoT projects. For example, one community used the $40 million DOT award to leverage, from community partners, more than $100 million in additional direct and in-kind contributions, such as research or equipment contributions. Communities discussed four main challenges to deploying IoT, including community sectors (e.g., transportation, energy, and public safety) that are siloed and proprietary systems that are not interoperable with one another.

Examples of Internet of Things Projects in Communities



Source: GAO analysis of federal agency and industry information. | GAO-17-570

Contents

Abbreviations

ATCMTD	Advanced Transportation and Congestion Management Technologies Deployment
Commerce	Department of Commerce
DHS	Department of Homeland Security
DOE	Department of Energy
DOJ	Department of Justice
DOT	Department of Transportation
DSRC	dedicated short-range communications
EAGER	EArly-concept Grants for Exploratory Research
EIP-SCC	European Innovation Partnership on Smart Cities and Communities
EPA	Environmental Protection Agency
EPB	Electric Power Board (of Chattanooga)
EU	European Union
FCC	Federal Communications Commission
FTC	Federal Trade Commission
GCTC	Global City Teams Challenge
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
IoT	Internet of Things
MOU	memorandum of understanding
NIST	National Institute of Standards and Technology
NITRD	Networking and Information Technology Research and Development
NSF	National Science Foundation
NTIA	National Telecommunications & Information Administration
OSTP	Office of Science and Technology Policy
TIGER	Transportation Investments Generating Economic Recovery

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

July 26, 2017

Congressional Requesters

The Internet of Things (IoT) generally refers to the technologies and devices that allow for the network connection and interaction of a wide array of devices, or "things," throughout such places as buildings, vehicles, transportation infrastructure, or homes. IoT devices, or "smart" devices, are increasingly being used to communicate and process information to an extent that was not possible before. For example, a "smart" thermostat may allow a homeowner not only to remotely adjust the home's temperature, but also gather data on motion, temperature, and light, and analyze those data to automate the thermostat to respond to changes in the home's environment and use. Recent advancements in IoT-related technologies, such as the decreasing cost and size of electronics and the expansion of connectivity (e.g., broadband networks and Wi-Fi) have allowed not only individuals and businesses, but also governments and communities, to use connected objects to gather and communicate new types and quantities of information.

As a result of these advances, communities—both at home and abroad—are increasingly deploying projects with IoT devices, generally with a goal of improving livability, management, service delivery, or competitiveness. These projects can be targeted to specific community goals. For example, "smart" traffic lights may collect and evaluate real-time traffic information to update traffic signals' timing to reflect current traffic conditions, with the goal of improving traffic flow by easing congestion and reducing vehicles' emissions. IoT-enabled garbage cans can signal waste removal teams when cans are full, streamlining the routes that garbage trucks take and reducing wear and tear on roads due to unnecessary trips by these heavy trucks.

Researchers and industry stakeholders have noted that integrating technologies and projects so that they work in concert with one another is key to realizing the full potential of IoT applications.[1] The goals of different

[1] See, for example, McKinsey Global Institute, *The Internet of Things: Mapping the Value Beyond the Hype* (June 2015) and OECD, *The Internet of Things: Seizing the Benefits and Addressing the Challenges, 2016 Ministerial Meeting on the Digital Economy, Background Report* (May 2016).

sectors of the community—such as energy efficiency, mobility for underserved populations, or improved public health—are often interconnected in such a way that integrating IoT projects and systems may save resources and enable solutions that address multiple goals at once. In the example above, the smart traffic lights that are deployed by communities to improve traffic flow may also lead to reduced vehicle emissions, targeting a secondary goal of improving air quality and public health.

The U.S. government has shown increased interest in supporting IoT in communities, in part to harness the economic potential; help address anticipated challenges, such as risks to privacy or security; and promote replicability—that is, make it easier for projects in one community to be deployed in other communities. Over the past 22 months, the White House announced more than $240 million in federal investments for research and technology to support making communities "smarter." And on January 12, 2017, the former administration issued for public comment a draft federal strategic plan for smart cities and communities that provides a high-level framework to guide and coordinate federal efforts supporting IoT in communities. The European Union (EU) and some foreign governments also have made investments in supporting IoT projects in communities. For example, the EU, in 2015, funded three large-scale pilot projects with the aim of identifying and deploying integrated community solutions—that is, projects or technologies that aim to meet community goals.

You asked us to examine federal support for IoT and the impact of IoT on communities. In this report we describe the following:

1. The kinds of efforts selected federal agencies have undertaken to support IoT in communities, such as cities or counties.
2. How selected communities are using federal funds to deploy IoT projects, including any challenges they face in integrating those projects.

To identify the kinds of efforts that selected federal agencies have undertaken to support IoT in communities, we reviewed documents and interviewed officials from 11 selected federal agencies that we identified as having a key role in providing such support, including those that support research or community IoT efforts, oversee privacy or security protections and threats, or have direct authority over IoT issues. The 11 selected agencies include the following: the Departments of Commerce (Commerce), Energy (DOE), Health and Human Services (HHS),

Homeland Security (DHS), Justice (DOJ), and Transportation (DOT), as well as the Environmental Protection Agency (EPA), Federal Communications Commission (FCC), Federal Trade Commission (FTC), National Science Foundation (NSF), and Office of Science and Technology Policy (OSTP). We collected and synthesized information on current or recent major efforts these agencies identified as supporting the application of IoT in communities. The efforts discussed in this report are not an exhaustive list of such federal efforts.

To identify how selected communities are using federal funds to deploy IoT projects and any challenges they face in integrating those projects, we conducted semi-structured interviews by telephone or in person with representatives from multiple stakeholders groups in four communities that are using federal efforts to implement IoT projects—Chattanooga, Tennessee; Chicago, Illinois; Columbus, Ohio; and Portland, Oregon. We selected these four communities to include a range of city sizes and locations and communities with projects that used federal support and involved multiple community sectors (e.g., energy, transportation, public safety), as well as experience in successfully and unsuccessfully seeking federal funds. The experiences of the selected communities are not generalizeable to those of all U.S. communities; however, we believe that the information provides a balanced and informed perspective on the topics discussed.

We also reviewed information on the European Commission's efforts supporting IoT in communities and selected European communities' experiences with deploying IoT projects. We reviewed available documents from and conducted interviews by telephone or in person with representatives from European Union (EU) to better understand how its efforts align with the United States' efforts, given the EU's experience with supporting IoT in communities. We selected the European Union and select member states based on criteria that included the relative maturity of efforts compared to the United States; similarity to U.S. governance structure; and the availability of information about projects and governmental support. Specifically, we interviewed multiple stakeholder groups in three selected European communities—Eindhoven, The Netherlands; Gothenburg, Sweden; and Stockholm, Sweden. We also interviewed officials from the European Commission (Directorate-General for Communications Networks, Content, and Technology) and Sweden's Ministry of Enterprise and Innovation.

In addition, we interviewed 11 representatives from industry associations, consulting companies, academia, and industry vendors to obtain

perspectives on domestic and foreign efforts to support IoT in communities and any challenges faced by communities in using these efforts. We selected these representatives, based on our review of background material and recommendations from others, concerning their expertise and involvement in IoT efforts. We also reviewed literature from the last 4 years in peer-reviewed journals, trade publications, and conferences, among other professional resources, to identify federal and international efforts related to IoT in communities, as well as any analyses of communities' projects.

We conducted this performance audit from November 2015 to July 2017 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

IoT has no generally accepted, all-inclusive definition. Instead, IoT is generally described as a concept referring to how connected devices interact and process information. The devices themselves are generally not computers, but have embedded components that connect to a network.[2] We define IoT for the purposes of our report as the concept of connecting and interacting with a wide array of objects through a network.[3] An IoT-enabled object is often referred to as a "smart" or a "connected" device, which allows that object to communicate and potentially process information and thereby provide capabilities and functionality beyond what that object would normally provide. For example, connected vehicles—vehicles that "talk" to infrastructure and other vehicles—provide the capability to identify threats and hazards on the roadway and allow drivers to receive notifications and alerts of dangerous situations, potentially reducing the number of accidents.

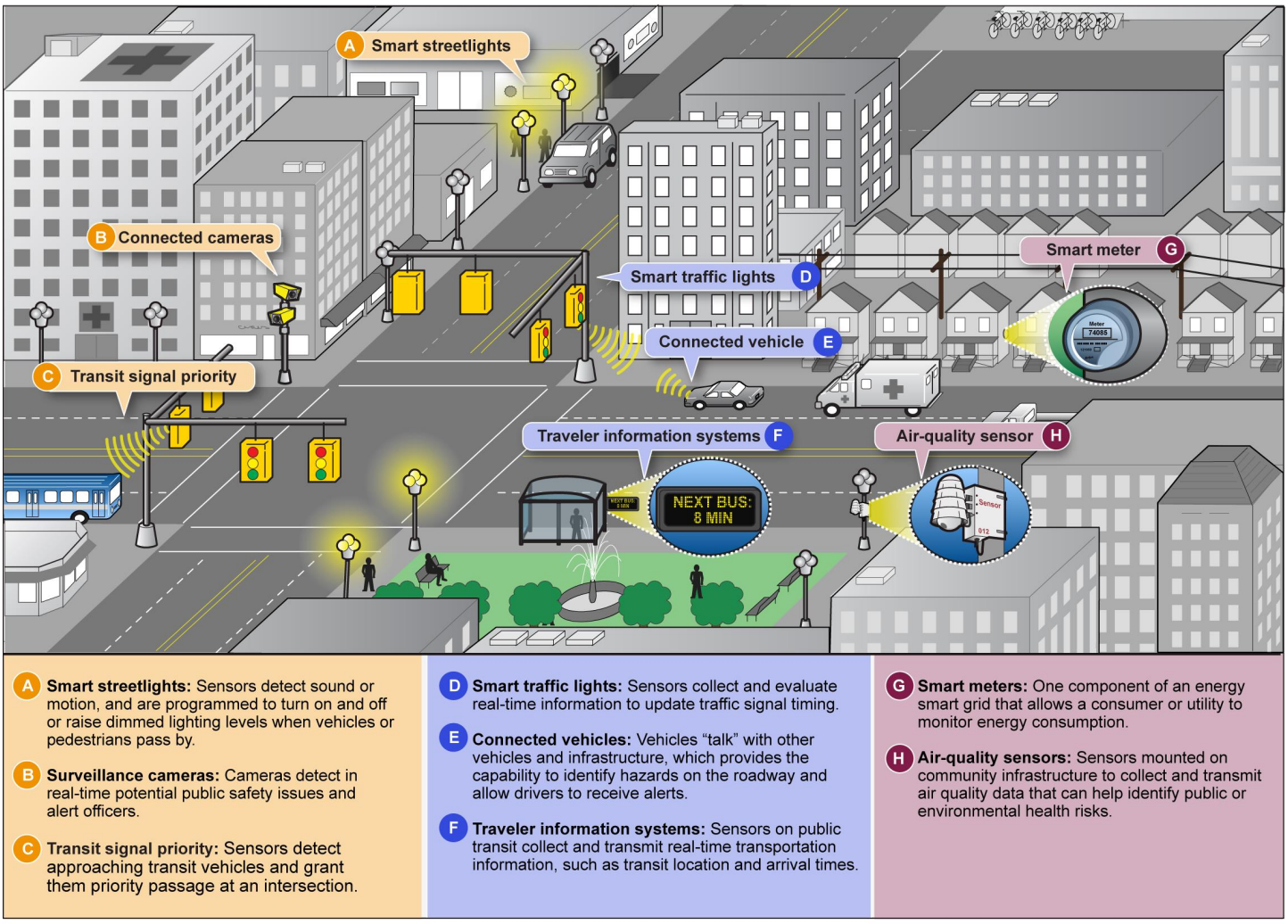
[2] Other connected devices include personal computers and laptops, tablets, and mobile phones, but these devices are generally not included in the term IoT.

[3] Although the term IoT implies the Internet is the mode of communication, other networks can also transmit information collected by sensors. For the purposes of this report, IoT includes information collected and transferred both by the Internet and other networks.

IoT devices are used in a variety of settings, such as the home (e.g., smart appliances), manufacturing (e.g., predictive maintenance), or a health care setting (e.g., remote patient monitoring).[4] In this report, we focus on the application of IoT within a community setting—often referred to as a "smart city" or "smart community"—with the aim to generally improve the livability, management, or service delivery of that community. For example, a community may deploy streetlights with embedded sensors that detect sound or motion and that are programmed to switch on and off or raise dimmed lighting levels when vehicles or pedestrians pass. By managing the level of streetlight use, communities seek to improve energy efficiency and costs, as well as reduce maintenance costs by reducing service trips to replace burned-out lights. Figure 1 illustrates other examples of how IoT technologies may be used in a community. More indirectly, these technologies can drive economic growth by generating demand for new products, new companies, and new skilled jobs, according to literature and industry experts.

[4] Remote patient monitoring uses technology to monitor patients outside of conventional settings, and can be used to monitor patients with chronic conditions, such as those with congestive heart failure or diabetes, or as a diagnostic tool, such as for some heart conditions. See GAO, *Health Care: Telehealth and Remote Patient Monitoring Use in Medicare and Selected Federal Programs*, GAO-17-365 (Washington, D.C.: Apr. 14, 2017).

Figure 1: Examples of Types of Internet of Things Projects in Communities



Source: GAO analysis of federal agency and industry information. | GAO-17-570

While the idea of connecting objects is not new, recent advancements in technologies that support IoT—such as the decreasing cost and size of electronics and the expansion of connectivity (e.g., broadband networks and Wi-Fi), are driving a proliferation in the number and types of uses of connected devices. One projection puts the future number of IoT devices (excluding computers, mobile phones, and tablets) at over 10 billion in 2020. This would represent an increase of more than 200 percent between 2015 and 2020, at which point the number of connected things would outpace the number of computers, tablets, and smartphones currently connected.

There are also, however, hurdles that may impede widespread use of IoT devices. Security and privacy risks can originate from unintentional threats, such as equipment failures, or intentional threats, such as from hackers. As noted in a Commerce green paper on IoT, published in January 2017,[5] while these risks are generally not unique to IoT, ubiquitous connectivity and growth in IoT devices raise new challenges. As new and more "things" become connected, they increase not only the opportunities for security and privacy breaches, but also the scale and scope of any resulting consequences. For example, in October 2016, a cyberattack that involved the hacking of thousands of unsecured IoT devices interrupted Internet access to a number of major websites across the United States for hours. These hurdles demonstrate the need for strategies to respond to concerns about safety and increased risks to privacy and security. We have reviewed and continue to review some of these issues; for example, we recently issued a report that discusses the specific implications of IoT technologies, including safety, security, and privacy issues.[6]

IoT projects are also complex, crosscutting, and require expertise to design and deploy.[7] IoT projects involve the deployment of rapidly evolving technologies and also often collect and store vast amounts of data that must be analyzed before they can be used to develop community solutions. For example, as we have previously reported,[8] when local transportation departments deploy IoT-enabled sensors on traffic lights to monitor and collect data on traffic flow to help manage congestion, they may need assistance in developing the system requirements; collecting, analyzing, and protecting the vast amounts of

[5] Department of Commerce, *Fostering the Advancement of the Internet of Things*, (Washington, D.C.: January 2017).

[6] GAO, *Technology Assessment: Internet of Things: Status and Implications of an Increasingly Connected World*, GAO-17-75 (Washington, D.C.: May 15, 2017). We also recently issued a report that highlights security issues associated with IoT devices that the Department of Defense faces. See *Internet of Things: Enhanced Assessments and Guidance Are Needed to Address Security Risks in DOD,* GAO-17-514SU (Washington, D.C.: June 7, 2017.

[7] For more information on IoT projects, generally, see, for example, GAO-17-75 and Internet Society, *The Internet of Things: An Overview Understanding the Issues and Challenges of a More Connected World,* (October 2015).

[8] GAO, *Intelligent Transportation Systems: Urban and Rural Transit Providers Reported Benefits but Face Deployment Challenges*, GAO-16-638 (Washington, D.C.: June 21, 2016).

data collected; and identifying interdependent goals for the community, such as improving air quality. As such, the local transportation department may hire consultants to help with procurement and deployment of a system; purchase the system from a vendor; partner with academia for support in data analysis and innovative solutions; collaborate with other local-government departments to identify interdependent goals; and collaborate with other entities, such as transit operators or regional planning departments, to leverage outcomes, among other activities.

As noted earlier, researchers and industry stakeholders have noted that successful integration of technologies and projects—including across sectors (e.g., transportation, energy, or public safety)—is key to realizing the full potential of IoT. That is, when systems are interoperable—or work in concert with one another—they may support interdependent goals. For example, sensors deployed in community infrastructure to report on traffic conditions or environmental conditions such as air quality can also, if equipped with audio or visual capability, provide real-time traffic information to public-safety or emergency-response persons, to help determine the fastest route to an emergency. Government departments that work with each other to build integrated systems can help optimize resource expenditures and maximize services to community residents.[9] One research institute estimated in 2015 that IoT applications in cities could have a global economic impact between $930 billion to $1.6 trillion per year in 2025, with systems that are interoperable enabling more than 40 percent of that value.[10]

No single federal agency addresses all aspects of IoT. We identified at least 11 federal agencies that have a key role in supporting IoT in communities, either because they support research or communities, oversee privacy or security protections and threats, or have direct authority over IoT issues. The 11 key federal agencies that we identified include Departments of Commerce (Commerce), Energy (DOE), Health and Human Services (HHS), Homeland Security (DHS), Justice (DOJ), Transportation (DOT), as well as the Environmental Protection Agency (EPA), Federal Communications Commission (FCC), Federal Trade Commission (FTC), National Science Foundation (NSF), and Office of Science and Technology Policy (OSTP). See appendix I for more

[9] See, for example, Smart Cities Council, *Smart Cities Readiness Guide* (2014).

[10] McKinsey Global Institute, *The Internet of Things*.

information on selected agencies' missions and examples of relevant support for communities' IoT applications.

The EU also has made investments in supporting IoT projects in communities. For example, in 2013 the EU adopted a research and innovation framework program for 2014 to 2020 (Horizon 2020) that includes cross-cutting focus areas in both:

- IoT, which aims to enable the emergence of an IoT environment that is supported by open (i.e., publicly available) technologies and platforms, and
- "Smart cities and communities," which aims to bring together cities, industry, and citizens to demonstrate solutions and business models that can be scaled up and replicated.

These focus areas are supported by bi-annual funding strategies. The European Commission, similarly to the U.S. government, is divided into departments and executive agencies that have varied responsibilities. For example, the European Commission has departments for Energy; Mobility and Transport; and Communications Networks, Content, and Technology that each have responsibility in carrying out the European Commission's policies related to the respective industry sector that the departmental entity oversees. With support from the EU, as well as local initiatives, European communities are increasing investments in IoT projects, and according to literature we reviewed and some U.S. and European industry experts we interviewed, some of those communities are generally recognized as having more advanced and mature IoT projects than communities in the United States.

In Addition to Broad IoT Research and Oversight, Federal Agencies More Directly Support Communities by Funding IoT Projects and Fostering Collaboration

Broad Federal IoT Research and Oversight Provide Underlying Support for IoT in Communities

Research

Many of the federal agencies we reviewed are conducting or funding broad research in IoT-related technologies. As communities increasingly deploy IoT devices, they are more dependent on the underlying communications systems—both wired and wireless network systems—that enable those devices to communicate with each other and with other systems. And with wireless systems likely playing an increased role in supporting IoT, demand for access to spectrum[11]—a limited resource already in high-demand—will also rapidly increase.[12] Recognizing the increasing demand for connectivity and spectrum access, 8 of the 11 federal agencies are conducting or funding research on communication systems and the related impacts of those systems—such as privacy, security, and demand for spectrum access—that could subsequently support communities' IoT projects. For example:

- NSF awarded 19 universities over $8 million over 3 years beginning in 2016, through its US Ignite program, for fundamental research in networking technologies to further both the capabilities and understanding of high-speed networking infrastructure to meet the demands of future applications, including community applications. NSF also awarded in 2016 more than $6 million over 2 years for exploratory research in connecting networked computing systems with

[11] Radio frequency spectrum is a natural resource that makes possible wireless communication and supports an array of government and commercial wireless services, like mobile voice and data and public safety activities. In the United States, the National Telecommunications & Information Administration (NTIA) manages the federal government's use of spectrum, and FCC manages spectrum use for nonfederal users, including commercial, private, and state and local government users.

[12] Department of Commerce, *Fostering the Advancement of the Internet of Things*.

physical devices through NSF's EArly-concept Grants for Exploratory Research (EAGER) funding mechanism.

- Commerce's National Telecommunications & Information Administration (NTIA) has a research lab that is developing an IoT testbed for testing the potential of interference posed by new IoT-related spectrum use to existing spectrum users in a dense environment, such as a city. The growth in wireless communications has increased the potential for harmful interference—an action that interrupts or obstructs communication service—when two systems use the same or adjacent spectrum frequencies in the same geographic area. NTIA officials also told us that this lab is also supporting DOT's efforts to investigate the potential interference of unlicensed wireless devices operating in the licensed spectrum for dedicated short-range communications (DSRC)—the wireless technology that, according to DOT, is expected to be used in a connected vehicle environment.[13]
- FTC's Office of Technology Research and Investigation researches and evaluates the impact of IoT technologies on consumers, including issues related to privacy and security. In addition, in January 2017, the FTC announced a prize competition that challenges the public to develop a tool that consumers can deploy to guard against security vulnerabilities in IoT devices. And while the challenge is not directed to communities, FTC staff noted that it is possible that some of the proposed submissions could help address security issues related to IoT devices in communities.
- In late 2016, DOJ formed a threat analysis team to study the potential national-security threats posed by IoT devices as part of a broader effort to assess the next -generation of cyber threats. According to DOJ officials, the team has focused on how IoT devices may be exploited by terrorists or others to cause loss of life or disrupt the nation's increasing reliance on IoT technologies, which included surveying other federal agency efforts and non-government experts on this issue. DOJ hopes in the future to support an interagency approach to this issue.

[13] In a connected vehicle environment, data are expected to be shared wirelessly among vehicles or between vehicles and infrastructure using dedicated short-range communications (DSRC), a technology similar to Wi-Fi that offers a link through which vehicles and infrastructure can transmit messages over a range of about 300 to 500 meters.

In addition to networked communications systems, federal agencies are conducting or funding broad technical research on IoT devices that support communities, such as sensors and intelligent transportation systems technologies,[14] as described in the examples below.

- DHS awarded three $100,000 small business innovation research contracts in January 2016 for research and development of modular (i.e., composed of standardized units), low-cost, integrated, IoT-enabled flood inundation sensors. These sensors would (1) monitor flood-prone areas in real-time across large geographic areas and (2) allow emergency responders to predict, detect, and react to flood conditions, among other things. All three awardees received follow-on awards to test and evaluate the sensors in the field, beginning in April 2017. The final phase of the awards involves commercialization of the sensors, and while not funding commercialization directly, DHS plans, among other things, to help bridge relationships between the awardees (sensor developers) and potential buyers (such as first responders).
- EPA's Office of Research and Development formally coordinates with two universities on research related to management and analysis of data collected through sensor networks. This research has included collaborating to develop a freely available data-hosting and visualization tool, as well as analyzing high-resolution air pollution emissions data.
- DOE established the Grid Modernization Initiative to support modernization, including ensuring the resiliency and security, of the nation's electricity grid—commonly referred to as a smart grid.[15] Under this initiative, DOE not only makes funding available but also supports research projects related to IoT technologies, such as sensors, which, according to the initiative's multi-year program plan, are necessary to assess the health of the grid in real time, predict its

[14] Intelligent transportation systems refer to the collection of various wireless and wireline communications-based information and electronic technologies used in transportation.

[15] This modernization effort includes incorporating information technology systems and networks and two-way communication into existing infrastructure (e.g., electricity networks including power lines and customer meters) to automate actions that system operators formerly had to make manually. These efforts are designed to, among other things, improve transmission of electricity from power plants to consumers, provide grid operators with more information about conditions on the electricity system, integrate new and improved technologies into the grid, and allow consumers to receive more information about electricity prices and availability from the electricity system.

behavior, and respond to events effectively. According to DOE officials, the initiative's projects are in their first year, so no reported results are available, but a peer review panel was held in April 2017 to provide lessons learned and share best practices. DOE officials also told us that they anticipate the initiative to continue through at least 2018.

- NSF, through its Smart and Connected Communities program, anticipates awarding about $18.5 million in grants under a 2016 program. This program solicits projects that support interdisciplinary research activities to improve understanding of smart and connected communities and enable sustainable change to enhance community functioning. Also, in 2015, NSF's $3 million grant awarded through its Major Research Instrumentation program supported the development of a new tool for a project known as the Array of Things. The project's goal is to install a sensor platform in the City of Chicago that collects data on a variety of community factors, including air quality and traffic, and makes these data publicly available to encourage innovative community solutions from third parties.
- Finally, DOT's Intelligent Transportation Systems Joint Program Office conducts a variety of research and demonstration projects that, according to its current strategic plan, includes the testing of ideas that might be developed into intelligent transportation systems technologies and subsequently deployed to advance transportation.

Oversight

The federal government is also engaged in overseeing IoT-related issues. In doing so, all but two of the federal agencies we reviewed are developing and distributing IoT-related guidelines, seeking input on and making policy recommendations, and convening or participating on working groups that support the development of voluntary consensus standards. As communities continue to deploy IoT devices and analyze the increasing amount of resulting data, federal policies and guidance can help them better understand the benefits of using IoT-related technologies, and help them address the challenges. Notably, Commerce issued a paper in January 2017 that, among other things, sought input on the role of the federal government in fostering IoT and related policy recommendations. The paper also discusses both benefits, such as improvements in safety and efficiency for consumers and governments,

and challenges of IoT, including risks to security and privacy.[16] Other examples include:

- *Safety:* DOT issued an Automated Vehicles Policy in September 2016 in order to speed the delivery of an initial regulatory framework and best practices to guide the safe design and deployment of automated vehicles.[17]
- *Security:* In October 2016, through public meetings, NTIA convened a multi-stakeholder process on IoT security upgradability and patching with a goal of fostering a marketplace that offers devices and systems that support security upgrades through increased consumer awareness and understanding, among other things. And, in November 2016, DHS issued a set of industry-neutral, non-binding principles to provide stakeholders with suggested practices that help to account for security and other challenges as stakeholders develop, implement, or use IoT devices.[18]
- *Privacy:* FTC staff issued a report in January 2015 that both summarized a 2013 staff-hosted workshop discussion on benefits and risks of IoT and provided an update on post-workshop developments, including a report on data privacy issued by the President's Council of Advisors on Science and Technology.[19], [20] The report also included the FTC staff's recommendations on privacy and security, which continued to recommend that Congress enact broad-based privacy legislation. Also, HHS published a report in July 2016 that highlighted what it referred to as gaps in regulation, as well as confusion among consumers on privacy of health data collected by entities not regulated by the Health Insurance Portability and Accountability Act (HIPAA).[21],[22]

[16] Department of Commerce, *Fostering the Advancement of the Internet of Things*.

[17] U.S. Department of Transportation, *Federal Automated Vehicles Policy*, (Washington, D.C.: September 2016).

[18] U.S. Department of Homeland Security, *Strategic Principles for Securing the Internet of Things (IoT) Version 1.0*, (Washington, D.C.: November, 2016).

[19] President's Council of Advisors on Science and Technology, *Report to the President: Big Data and Privacy: A Technological Perspective* (May 2014).

[20] Federal Trade Commission staff, *The Internet of Things: Privacy and Security in a Connected World* (Washington, D.C.: January 2015).

[21] Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

- *Interoperability:* Commerce's National Institute of Standards and Technology (NIST) participates in international standards-setting organizations. NIST has convened an international public working group to help develop a consensus framework to enable interoperable community IoT solutions and plans to publish a draft consensus framework in late 2017.[23] This effort (and others at NIST) provides the technical basis for NIST contributions to work in international standards-setting organizations. DHS contracted with an international consortium of more than 500 companies, government agencies, and universities[24] to demonstrate how proprietary systems, specifically sensors used by first responders, could be made interoperable using open standards—that is, standards that are publicly available and maintained by a collaborative and consensus-driven process.

Selected Federal Agencies Directly Support Communities by Funding IoT Projects

In addition to broad research and oversight of IoT issues, we identified three federal agencies (Commerce, DOT, and EPA) that are more directly supporting communities through expanded funding for community IoT projects. In December 2015, DOT launched a two-phase prize competition, the Smart City Challenge, which, to date, included the largest single award amount ($50 million[25]) made available by the federal government to support IoT in communities. According to DOT, it had unprecedented community interest, attracting 78 mid-sized cities to apply for the first phase. According to DOT, it was one of the first times, if not the first, that federal funds were made available to explicitly encourage communities to integrate systems across sectors to achieve

[22] U.S. Department of Health and Human Services, *Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA* (Washington, D.C.: July 2016).

[23] National Institute of Standards and Technology (NIST) launched the International Technical Working Group on IoT-enabled Smart City Framework through its first workshop in March 2016.

[24] The consortium is named the Open Geospatial Consortium. http://www.opengeospatial.org/

[25] This amount included $40 million in Department of Transportation (DOT) funds, combined with an additional $10 million provided by Vulcan, Inc., a private company that supports innovative approaches to build sustainable communities.

interdependent goals.[26] As of April 2017, the challenge winner—Columbus, Ohio—is still finalizing its project schedule and details. DOT officials noted that it is challenging to identify measurements that define success and ensure that the projects provide adequate data to inform any evaluation, but that DOT officials are working with Columbus representatives and an independent evaluator to develop a strategy to do so. DOT officials also noted that they provided seven finalist communities $100,000 each and that some communities have used that money to revise their original proposals and bid on other available federal funds.

Two other federal agencies also recently announced funding for deployment of community IoT projects.

- In August 2016, EPA launched prize competition—called the Smart City Air Challenge—for the purpose of learning how communities would deploy hundreds of air quality sensors, manage high volumes of data, and make the data public. EPA awarded $40,000 each to Baltimore, Maryland, and Lafayette, Louisiana, to develop innovative strategies for deploying sensor platforms and managing the data collected from 300 sensors, as well as sharing lessons learned with other communities. According to EPA officials, as of April 2017, the communities are testing and deploying the sensors and will meet quarterly throughout 2017 with EPA officials to share knowledge and will participate in webinars with other communities to share best practices. EPA will evaluate the projects at the end of 2017 to determine whether it will award a second round of funding of $10,000 each.
- Commerce's NIST awarded, in September 2016, a total of $350,000 to four communities to collaborate and deploy replicable smart solutions to address community issues. These grants include such projects as using Wi-Fi-enabled sensors to alert first responders to emergencies in a senior community and developing computer models to predict urban flood events. In September 2017, the awardees are expected to submit final reports that include evaluation of the projects against specific criteria including evidence of effective use of existing

[26] Specifically, DOT's notice of funding opportunity described the challenge's vision as one to demonstrate and evaluate a holistic, integrated approach to improving surface transportation performance within a city and integrating this approach with other community sectors, such as public safety, public services, and energy. DOT also noted that the challenge intended to address how emerging transportation data, technologies, and applications can be integrated with existing systems in a city to address transportation challenges.

standards for interoperability across systems and clear and quantifiable performance goals with measurement capabilities incorporated into the system design. NIST officials noted that communities may find it challenging to meet these criteria during a 1-year, small-scale project but noted that regular bi-weekly meetings and continuing interaction between NIST and the communities is intended to help.

DOT also provides funds through other federal grant programs that do not specifically target IoT, but can still be used to support IoT projects. For example, DOT published a guide for communities that identifies existing funding programs or initiatives, such as its Advanced Transportation and Congestion Management Technologies Deployment (ATCMTD) initiative and DOT's Transportation Investments Generating Economic Recovery (TIGER) grant program that could be used towards funding IoT projects, according to the DOT guide.[27] The guide provides examples of IoT technologies that meet eligibility criteria under these programs, such as the ability of sensor-based infrastructure as an eligible technology for maintenance and monitoring under the ATCMTD Initiative. DOT officials reported that DOT announced for fiscal year 2016, nine ATCMTD and TIGER grants supporting IoT projects, such as a project in the city and county of Denver, Colorado that includes deploying technologies to support its connected freight program with a goal of reducing freight congestion.

[27] The ATCMTD Initiative and TIGER grant program support surface transportation infrastructure, including local innovative transportation projects. The FAST Act directs the DOT to establish the ATCMTD initiative to provide grants to state and local governments to develop model deployment sites for large scale installation and operation of advanced transportation technologies to improve safety, efficiency, system performance, and infrastructure return on investment. 23 U.S.C. §503(c)(4)(A). The TIGER program aims to support innovative and collaborative projects, including multi-modal and multi-jurisdictional projects.

EPA's Smart City Air Challenge

In August 2016, EPA launched the Smart City Air Challenge to encourage communities to deploy hundreds of air quality sensors and make the data publicly available. The challenge emphasizes that the communities share their data management practices with other communities to help them build capacity. The awards are intended to be seed money, so communities are encouraged to leverage opportunities with sensor manufacturers, data management companies and others. Also, the challenge requires local governments to be part of the project teams to ensure that their perspectives are part of the solution.

In December 2016, EPA awarded two communities—Baltimore, MD, and Lafayette, LA—$40,000 each, and recognized four projects for honorable mention.

After a year, EPA plans to evaluate the accomplishments and collaboration of the two communities and award each up to an additional $10,000.

Source: GAO's analysis of EPA information. | GAO-17-570

Some federal agencies are also working to maximize those federal funds by encouraging or requiring grant recipients to leverage private funds. For example, both DOT's Smart City Challenge and EPA's Smart City Air Challenge strongly encouraged communities to leverage funding from the private sector and others. DOT officials told us that Columbus, Ohio, the winner of the DOT Smart City Challenge, was able to leverage an additional $350 million or more from community partners beyond DOT's $40 million contribution. The EPA challenge solicitation specifically noted that the two community awards of $40,000 each were intended to be seed money for communities to leverage other resources.

Furthermore, federal agencies are promoting project replicability, so that solutions in one community can be more easily deployed in other communities. Due to the complexity of IoT projects and communities' limited resources, two representatives from industry and academia highlighted that communities are hesitant to be the first adopters of these projects without models or leading practices to follow. In recognizing this hesitance, some federal agencies are promoting the design of projects that are replicable to other communities. Most notably, NIST launched its Global City Teams Challenge (GCTC) program—a collaborative platform for the development of "smart cities"—to encourage collaboration and the development of technology standards. In doing so, NIST recognized that IoT projects tend to be isolated and customized—that is, not interoperable with other projects or replicable to other communities. According to NIST, many custom-designed systems are not cost effective, and the growth of the smart cities market is also hindered by deployments that are customized. And, with standards-based solutions—or replicable projects—communities can build on each other's work and make their solutions available to other communities that may lack resources. For example, the multi-stakeholder team that is deploying the sensor and computer research platform, called the Array of Things, in the City of Chicago first began as a partnership between the City of Chicago, University of Chicago, and Argonne National Laboratory. This partnership participated in the GCTC program and also received an NSF research instrumentation grant, as discussed above. The team has had inquiries from nearly 90 cities around the world, and is preparing to deploy the IoT technology in an initial set of pilot cities, including Seattle, Washington, and Amsterdam, the Netherlands.

Highlights of Chicago's Array of Things project

- ***Federal Support:*** GCTC project team and $3.1 million award through NSF's major research instrumentation program and more than $1 million from DOE's Argonne National Laboratory.
- ***Non-federal support:*** $150,000 provided by Chicago Innovation Exchange. Installation and information technology services from the City of Chicago. Technical advice and support from multiple universities, research institutes, and industry partners, such as Cisco, Microsoft, and Intel.
- ***Project description:*** Chicago's Array of Things project plans to install hundreds of interactive, modular sensor boxes across the city to collect real-time data on the city's environment, infrastructure, and activity for research and public use, essentially measuring factors that impact livability such as climate, air quality and noise. The project also reserves space for additional sensors in support of future data collection in other areas and industry sectors.

Source: David Carhart/PDT & Urban Center for Computation and Data. | GAO-17-570

Finally, DOE has provided in-kind technical support to IoT projects. In-kind contributions can be equipment and services that are provided to a project and that, while not directly providing funds, still benefit and assist in financing the project, as described below:

- As part of DOT's Smart City Challenge, DOE is providing an estimated $10 million in in-kind contributions to the winner of the challenge—Columbus Ohio—which includes a technical staff-in-residence in Columbus who can provide expertise to the community as it deploys its IoT projects.
- Under an October 2014 memorandum of understanding with the Electric Power Board (EPB) of Chattanooga, the owner and operator of the region's smart grid,[28] staff from DOE's Oak Ridge National Lab use their expertise to test new technologies and develop new analyses, among other things, to help EPB to use its electricity data to improve its operations.

DHS officials also told us that while in the past they have not provided in-kind support, they are currently drafting a contract in which they will be providing in-kind support, including drones and some open-source software, to a quasi-governmental organization that works to advance community IoT projects.

[28] A smart grid refers to the increased use of information technology systems and networks and two-way communication to automate actions that system operators formerly had to make manually.

Federal Government Also Supports Communities' IoT Projects by Fostering Interagency and Community Collaboration

Interagency Collaboration

Issues related to IoT in communities cut across multiple sectors and government agencies—that is, no single government agency addresses all aspects of IoT or communities' IoT efforts. And similar to other cross-cutting federal efforts, achieving meaningful results requires collaborative efforts of multiple programs and agencies spread across the federal government and often more than one sector or level of government. Both Congress and the executive branch have recognized the need for improved collaboration across the federal government.[29] We also have previously reported that agencies face challenges when attempting to work collaboratively and that the agencies can enhance and sustain their collaborative efforts by engaging in such practices as establishing mutually reinforcing or joint strategies designed to help achieve a common outcome and identifying and addressing needs by leveraging resources to support common outcomes.[30]

To promote government-wide collaboration in supporting deployment of IoT in communities, the White House created an interagency Smart Cities and Communities task force in July 2016—co-chaired by representatives from DOT, NIST, and NSF—that is coordinated through the Networking and Information Technology Research and Development (NITRD) program.[31] Twenty-two federal departments and agencies have participated on the task force as of January 2017 with initial efforts focused on developing (1) a federal strategic plan and (2) a resource

[29] Collaboration can be broadly defined as any joint activity that is intended to produce more public value than could be produced when organizations act alone.

[30] GAO, *Results Oriented Government: Practices that Can Help Enhance and Sustain Collaboration Among Federal Agencies*, GAO-06-15 (Washington, D.C.: Oct. 21, 2005) and GAO, *Managing for Results: Key Considerations for Implementing Interagency Collaborative Mechanisms*, GAO-12-1022 (Washington, D.C.: Sept. 27, 2012).

[31] Federal officials told us that this task force was created in part in response to a recommendation made by the President's Council of Advisors on Science and Technology in its February 2016 report to the President titled: Technology and the Future of Cities.

guide for communities.[32] On January 12, 2017, the task force released for public comment a draft federal strategic plan that offers a high-level framework to guide and coordinate smart community-related federal initiatives, with an emphasis on local government and stakeholder engagement.[33] The draft plan highlighted five goals motivating the strategy, including accelerating innovation and infrastructure improvement and facilitating cross-sector collaboration and bridging existing silos. It also identified four strategic priorities and next steps that include promoting interagency collaboration and developing a road map for specific federal actions to execute the strategic priorities. According to federal officials who are chairing the efforts, the public comments will help inform a revised federal strategic plan, which, as of April 2017, is anticipated for publication in the summer of 2017. According to these officials, following the completion of the strategic plan, the task force will be dissolved, and the NITRD program's standing Cyber-Physical Systems interagency working group will identify and coordinate any additional action that is needed to support these efforts, such as any activities related to the execution of the federal strategic plan. The task force's second effort included the launching of an interactive website resource guide in March 2017 that describes federally funded research and development programs in smart cities and communities.[34] According to the task-force, the guide aims to facilitate collaboration and coordination among task force member agencies, academia, industry, local cities and communities, and other government entities. These officials noted that the guide will be reviewed and updated annually, and that they are using

[32] The 22 federal departments and agencies are: Department of Agriculture; Commerce's NIST, NTIA, International Trade Administration, and Census Bureau; Department of Defense's Defense Advanced Research Projects Agency; DOE's Office of Electricity Delivery and Energy Reliability, Office of Science, and Office of Energy Efficiency and Renewable Energy; HHS' National Institutes of Health and Centers for Disease Control and Prevention; DHS; Department of Housing and Urban Development's Office of Community Planning and Development; Department of State; DOT's Federal Highway Administration and Federal Aviation Administration; EPA; National Aeronautics and Space Administration; NSF; Office of Management and Budget; OSTP; and National Coordination Office for Networking and Information Technology Research and Development.

[33] National Science and Technology Council, Networking and Information Technology Research and Development Subcommittee, *Smart Cities and Communities Federal Strategic Plan: Exploring Innovation Together: Draft for Public Comment* (Washington, D.C.: January 2017).

[34] https://www.nitrd.gov/apps/smartcity/index.aspx.

aggregate data on use and search patterns to evaluate the effectiveness and usability of the guide.

At the same time, individual federal agencies are formally and informally collaborating at a program level on specific agency projects or efforts related to community IoT projects. Federal agency officials told us that this collaboration helps bridge issues that cut across agencies, as well as leverage expertise. For example, in 2016, DOT and DOE signed a memorandum of understanding (MOU) that recognizes their departments' mutual interest in realizing the economic, environmental, and national security benefits achieved by the growing use of smart transportation technologies. The MOU formally states their intention to coordinate actions to leverage DOE's traditional focus and expertise in transportation energy technology systems and DOT's traditional focus and expertise in transportation safety technology systems to accelerate the analysis and application of "smart" transportation systems. Under this MOU, and as mentioned above, DOE supports a national lab expert, as part of a technologist-in-cities pilot program, in Columbus, Ohio, who serves as a complement to DOT's Smart City effort and focuses on energy-related components of the planned projects. In addition, according to NTIA officials, its research lab also coordinates with DOT's Intelligent Transportation Systems Joint Program Office, including investigating the potential interference of unlicensed wireless devices operating in the licensed spectrum for DSRC—the wireless technology that, according to DOT, is expected to be used in a connected vehicle environment.

Community Collaboration

Some federal agencies have undertaken efforts to support collaboration at the community level, across local governments, academia, and the private sector. NIST's GCTC program, as discussed earlier, enables local governments, nonprofit organizations, academic institutions, technologists, and private corporations from all over the world to form project teams, or "action clusters," to work on community IoT projects and facilitate interoperability, according to NIST officials.[35] And since the GCTC program launched in September 2014, GCTC has recruited and supported over 160 project teams, with participation from over 150 cities and 400 companies or organizations from urban and rural communities

[35] In the 2017 Global City Teams Challenge round, NIST has emphasized the formation of "superclusters," teams of action clusters formed around community goals, such as transportation, public safety, or public broadband access.

across the United States and their counterparts in other countries.[36] The White House also has supported collaboration at the community level through promotion of the MetroLab Network—a networking consortium of city-university partnerships that seeks to bring interested cities and universities together to share expertise and lessons learned across municipalities.[37] According to a 2016 MetroLab Network report, the membership consists of more than 35 partnerships and has developed a library of more than 120 research, development, and deployment projects that are currently under way across its membership. The library resource, as well as knowledge-sharing and networking events convened as part of the consortium, enables collaboration with, and the sharing of lessons from communities that have deployed innovative community solutions. For example, according to an official from the Portland Bureau of Planning and Sustainability, a meeting at a MetroLabs event resulted in a partnership between Portland and a stakeholder leading Chicago's Array of Things project to share information and leverage resources in testing sensors and a sensor platform for an air quality project.

European Union Efforts Are Generally Similar to the United States, Although in Some Cases More Formalized

Broad Research and Oversight

In the European Union (EU), the European Commission directs research on IoT-related technologies and oversees IoT policy-related issues, similar to the U.S. federal government.

- Within the EU's Horizon 2020's 7-year research program, the European Commission developed an initiative to support innovation, which includes a specific focus area for IoT that is cross-cutting. The focus area aims to enable an IoT environment that is supported by technologies and technology platforms that are open (i.e., publicly available). Funds for the 2016-2017 programs are to be used to

[36] According to NSF officials, in 2015 and 2016, NSF's combined investment of over $3 million to 17 university-community teams has enabled research in coordination with GCTC.

[37] The White House, *Fact Sheet: Administration Announces New "Smart Cities" Initiative to Help Communities Tackle Local Challenges and Improve City Services*, p. 8 (Washington, D.C.: Sept. 14, 2015) and the White House, *Fact Sheet: Announcing Over $80 million in New Federal Investment and a Doubling of Participating Communities in the White House Smart Cities Initiative*, (Washington, D.C.: Sept. 26, 2016) 12-13.

demonstrate scientific progress that enables advanced IoT applications.

- The EU also has taken legislative steps related to IoT oversight. For example, the EU adopted the General Data Protection Regulation in spring 2016, which, according to European Commission officials, seeks to simplify protection for individuals' data, including data from IoT devices, by providing a single set of rules that apply to all EU member states.[38] It is scheduled to be implemented over the next 2 years. At the country level, according to community representatives in Sweden with whom we spoke, policy makers are also investigating potential regulatory changes. For example, in one instance, the Swedish government created "policy labs" (also sometimes called a "regulatory holiday,") specifying some geographic locations or a specific time frame that is free of regulation so that project partners can test what policies are needed in that environment—such as a connected vehicle environment—to make the solution successful.

Funding and Collaboration

The EU also directly supports IoT applications in communities through direct funding. Sometimes it does so through formalized programs, such as joint-departmental funding that is focused on "smart cities and communities."

- Specifically, the Horizon 2020 research program includes a cross-cutting focus area on "smart cities and communities"—which aims, in part, to bring together cities, industry, and citizens to demonstrate community solutions and business models that can be scaled up and replicated, and that lead to measurable benefits in energy and resource efficiency, new markets, and new jobs. The supporting funding program combines funds from multiple departments—the European Commission's departments on energy, transportation, and communications technology—to support IoT projects in communities that span these sectors. Under this program, the EU has funded three different large-scale pilot projects since 2015 that focus on replicability and support IoT projects. For each pilot project, three European cities were selected as "lighthouse cities," with up to five different follow-on cities in which successful projects are to be replicated. The lighthouse cities design and implement their smart projects, and when successful, the follow-on cities begin deployment.

[38] Regulation (E.U.) 2016/679.

- We also found examples where individual countries supported community deployment of IoT projects and encouraged those communities to leverage resources from private industry and others. For example, according to community representatives in Sweden, the Drive Sweden project—focused in part on local and national traffic management and deployment of autonomous vehicles and fleets—is jointly funded by three Swedish government agencies: the Swedish Energy Agency, the Swedish Research Council, and Sweden's Innovation Agency. The project has to leverage private funds, as it is part of a program supporting nationally funded projects that require private industry cost-sharing.

European Commission departments and countries also collaborate in administering programs for community IoT projects and support collaboration among other stakeholders. For example, in 2012, recognizing that IoT technologies span all sectors of the economy and society, the European Innovation Partnership on Smart Cities and Communities (EIP-SCC) was launched. The partnership is a stakeholder group that aims to significantly accelerate the deployment of smart city solutions integrating technologies from energy, transportation, and communications technology. The EIP-SCC is jointly administered by three European Commission departments with jurisdiction over the energy, transportation, and communications technology sectors. It has a mechanism called a stakeholder platform that serves as a collaborative, networking, and knowledge-sharing tool for communities, collecting and analyzing input from all stakeholders. According to its agenda, it seeks to provide bottom-up contributions, such as those from communities, to ensure that EU policy on smart communities reflects the needs and engagement of communities. Also, at the country level, Sweden announced in June 2016 a formal program that supports collaboration among government, private, and academic stakeholders to create innovative solutions for specific societal challenges, one of which is "smart cities."

Selected Communities Use Federal Funds with Other Resources to Deploy IoT Projects but Face Various Challenges Integrating Projects

Communities Are Using Federal Funds in Conjunction with Other Funding and Expertise to Deploy IoT Projects

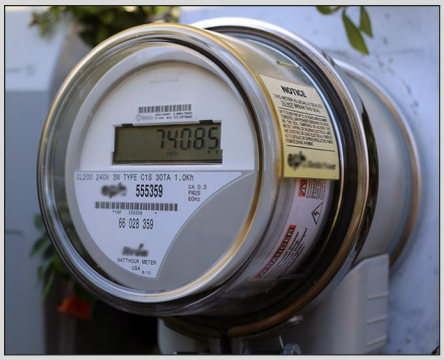
Financial Support

In planning and deploying IoT projects, all of the communities we reviewed are using federal funds with other direct funding and in-kind support. As described previously, grant recipients are sometimes required by federal agencies to leverage private funds. For example, the Chattanooga Electric Power Board leveraged more than $115 million in nonfederal investment as part of its federal award of $111.6 million through DOE's smart grid investment grant program in 2010.[39] Chattanooga used these federal and nonfederal funds to expand its fiber optic network to support communication of its smart grid equipment, which includes smart meters for more than 170,000 energy utility customers.

[39] This grant program was funded through the American Recovery and Reinvestment Act of 2009 (Recovery Act). According to a DOE Funding Opportunity Announcement for Financial Assistance under the Recovery Act, a cost share or match must be at least 50% of the total allowable costs of these projects (i.e., the sum of the recipient's allowable costs and the federal government share equals the total allowable costs of the projects) and must come from non-federal sources.

Highlights of Chattanooga's Smart Grid Infrastructure Project

- ***Federal Support:*** $111.6 million award through DOE smart grid investment grant program
- ***Non-federal Support:*** $115.1 million in other contributions
- ***Project Description:*** Chattanooga installed a fiber based gigabit internet infrastructure to improve efficiency and resiliency in its utility energy distribution The project included installation of more than 170,000 smart meters for utility customers. Since this project was completed, Chattanooga is making this fiber infrastructure available to other community stakeholders for other IoT projects, including deploying a network of air quality sensors to detect asthma-aggravating particulate matter and pollen in metropolitan Chattanooga.



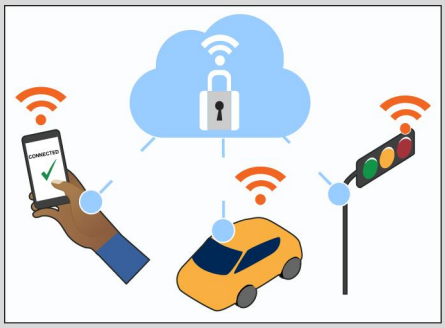
Source: EPB-Chattanooga. | GAO-17-570

According to community representatives we interviewed, without a federal cost-sharing requirement, federal funds alone may not be sufficient to cover all project costs. For example, according to City of Columbus representatives, it used its $50 million award from DOT's Smart City Challenge[40] to leverage about an additional $90 million in support from community partners. Some of the support has come in direct funding while other support has been in-kind, such as research, programmatic support, or equipment contributions.

[40] This amount includes $40 million from DOT and $10 million from Vulcan, Inc.

Highlights of Columbus's Smart City Challenge Projects

- ***Federal Support:*** $40,000,000 award through DOT's Smart City Challenge
- ***Non-federal support:*** More than $100 million in direct funds and in-kind contributions, including a $10 million grant from Vulcan, Inc.
- ***Project description for one of several projects:*** The Integrated Data Exchange is an open data environment that will: (1) contain data from many different sources; (2) generate performance metrics for program monitoring and evaluation; (3) transparently serve the needs of public agencies, researchers, and entrepreneurs; and (4) provide practical guidance and lessons learned to other potential deployment sites.



Source: GAO analysis of City of Columbus documents. | GAO-17-570

Local government officials from two of the communities that we reviewed discussed beginning to leverage value from public assets, making public infrastructure available in exchange for financial support, such as in-kind donations of technology equipment. For example, representatives from two communities highlighted their use of community-based "technology incubators." In these cases, a technology incubator is generally an entity that supports the collaboration of public, private, and oftentimes academic partners and provides public assets—such as data, resources, and infrastructure—to test technologies and develop innovative solutions to community needs. For example, Chattanooga provides access to its fiber network for use as a test bed to a variety of partners and a variety of projects. One project involves deploying and connecting a network of air quality sensors to detect asthma-aggravating particulate matter and pollen in the community with a goal of providing real-time alerts to end users, such as asthma patients, health institutions, and others affected by elevated pollen levels. Representatives from three of the communities we reviewed, as well as four other industry and academic stakeholders that we spoke with, discussed that developing such business models where local governments leverage value from public assets can help finance the project, and in some cases help sustain the project after initial grant funding runs out.

Highlights of Sweden's technology incubators

Sweden has 33 science parks, which are described as a stimulating meeting place for academia, research, the public sector, and industry.

Stockholm Science Park:

Kista Science City (KSC) is operated by a not-for-profit foundation that includes public, private, and academic organizations, for the purpose of facilitating collaboration among these stakeholders.

An open testbed—the Urban ICT Arena—will serve as the testbed and co-creation arena for developing, testing, and showcasing community IoT solutions. For example, the City of Stockholm will provide access to a fiber optic network for industry and academics to test community technology solutions, including solutions for clean water and efficient transportation.

Source: GAO analysis of Kista Science City and Urban ICT Arena information. | GAO-17-570

Representatives from all three of the European communities that we visited also reported having technology incubators where public, private, and academic entities partner to test innovative community solutions. While incubator-like entities can be found all over the world, Sweden has 33 formal technology incubators across the country, called Science Parks, which are jointly funded by industry, universities, and the local governments. These science parks facilitate collaboration among these stakeholders to develop community solutions. Representatives from three science parks that we met with in Gothenburg and Stockholm highlighted the importance of collaboration of public, private, and academic entities—typically referred to as the "triple-helix" model—to the success of the projects. For example, at a science park open testbed in Stockholm, the local and regional government, an industry partner, among others, have provided access to wired and wireless communications networks for other entities to use in developing innovative community solutions, such as improving water quality and transportation efficiency.

Non-financial Support

Representatives from communities we reviewed and industries we spoke with discussed the importance of collaboration among public, private, and academic entities to make the best use of the unique expertise that each member group brings to the table.

- Representatives from two communities discussed that local governments can provide a policy framework and help ensure that the solutions are based in the community's needs, as opposed to driven by the latest technology invention.
- A Columbus representative discussed its "culture of collaboration" and how private partners have brought invaluable resources to its DOT Smart City Challenge projects, particularly expertise on technologies and connections to other industry players for innovative ideas and solutions.
- Representatives from two of the communities we spoke with have active "convener" organizations that bring public, private, and academic stakeholders together on an on-going basis to discuss collaborative opportunities to address community problems.

While representatives from all of the communities discussed the benefits of collaboration, an industry representative also highlighted that maintaining well-functioning partnerships takes time and resources.

Representatives from all three European communities also discussed the value of collaboration for providing a variety of expertise, and in some cases, independence. For example, in The Netherlands, a non-profit organization oversees part of Eindhoven's "smart city" projects. Representatives from this organization highlighted this as advantageous to providing government and commercial independence—that is, to best balance the government's oversight needs with private industry interests. In Stockholm, a local government representative highlighted that the role of some academics is to independently evaluate the IoT projects' success, both in meeting environmental sustainability goals and economic goals.

Several Factors May Hinder Communities in Integrating IoT Projects

Although integrated projects can help maximize the potential of IoT applications, communities can face challenges in integrating projects. All of the domestic communities we reviewed are planning or have deployed discrete IoT projects—projects that, at least initially, generally focus on addressing a singular issue, such as traffic congestion on a particular corridor. Domestic and foreign community representatives that we spoke with pointed to four main factors that can hinder the deployment of integrated projects, and in some cases, offered perspectives on solutions to these challenges.

Siloed Community Sectors

Siloed community sectors can make it challenging to integrate IoT projects. A variety of representatives that we spoke with—representatives from three of the domestic communities and two of the foreign governments, as well as seven academic and industry representatives—highlighted that local government departments and federal grants tend to be focused on one sector (e.g., transportation, energy, public safety) of a community, inhibiting IoT project integration. An industry representative who works with communities on IoT projects said that community projects tend to be planned and deployed in isolation, in part because it is difficult to leverage resources and benefits across the silos created by government departments. A local government representative from a domestic community noted that there is no sense of a single organization at the federal level when pursuing grants and that while federal grants are helpful, tracking opportunities and developing proposals are a lot of work, and consumes both time and resources. Representatives from one

domestic community noted that collaboration between transportation, energy, and environmental monitoring appears be most advanced, in part because these industries have recognizable synergies.

Domestic and industry representatives that we spoke with offered perspectives on how internal or external leadership and a federal strategy could help overcome silos and promote integration.

- *Leadership:* Representatives from a domestic community, as well as four industry representatives, noted that an individual or department within the local government could serve as a mechanism to bridge silos. For example, an industry representative that works with communities on IoT projects noted that some domestic communities are using a Chief Information Officer or Chief Data Officer as a leader who can help integrate projects across departments. And according to local representatives from three domestic communities and two industry representatives, entities that are external to the local government, such as the community's technology incubator or other consortium, could help convene various stakeholders. For example, in one domestic community, a consortium of public, private, and academic entities helped identify how to leverage a past investment in traffic sensors to expand the capacity to evaluate air quality.
- *Federal Strategy:* While collaboration is helpful to integrating projects, representatives from three communities, three industry and academic representatives, and officials from two federal agencies noted that some kind of federal strategy or guidelines could be helpful. For example, a representative from one community noted the desire for a federal vision or framework that organizes multiple industries and agencies and supports strategies and resources for working together to achieve common goals. As discussed above, through the White House's NITRD program, a task force that consists of 22 federal agencies, recently issued a draft federal strategic plan that includes a high-level framework to guide and coordinate smart community-related federal initiatives, with an emphasis on local government and stakeholder engagement. Federal officials working on the task force anticipate that the final plan, which will be informed by public comments, will be published in summer 2017.

Proprietary Systems

Representatives from three of the domestic communities and one of the foreign communities, as well as four industry stakeholders we interviewed, identified challenges related to proprietary vendor systems in

deploying integrated projects. For example, while private industry can provide communities with needed financial support and expertise, representatives from two communities noted that private interests also encourage the development of proprietary systems that are solely owned by a vendor. Representatives from two communities also noted that proprietary systems risk making the community dependent on one vendor that could go out of business or raise maintenance costs. The use of proprietary systems raises confidence that the components within a system will work together, but challenges arise when communities seek to integrate systems from different vendors, perhaps across sectors.[41] We also recently reported on similar challenges experienced by transit providers, including difficulties changing vendors after an intelligent transportation system has been deployed and getting vendors to work with one another to integrate systems amid concerns about making changes to those systems.[42]

Representatives from all of the domestic and foreign communities we reviewed, as well as four academic and industry stakeholders, said that standards-based and open data platforms could help support integrated projects and innovative solutions. Some federal agencies—such as NIST, EPA, and DHS—are taking steps to address interoperability issues, including promoting consensus-based standards that would encourage proprietary systems to at least be designed to be interoperable. For example, NIST recognized that IoT projects are generally based on custom systems that are not interoperable, portable across cities, or cost-effective. Subsequently, NIST is helping convene an international public working group to develop a consensus framework to enable smart city solutions.[43] Representatives from one foreign community told us that they are working to create an "umbrella" platform to unify all of the diverse systems developed by different projects with different business plans and timelines. Representatives from all three of the foreign communities noted that publicly funded projects often require that data collected be open—that is, available for others to use, including the public or other vendors. Representatives from two of these communities, as well as representatives from three of the domestic communities, noted that open

[41] See, for example, Internet Society, *The Internet of Things*.

[42] GAO-16-638.

[43] NIST and its partners are convening an international public working group called the IoT-Enabled Smart City Framework collaboration project.

data allow third-party entities access to information they can use to develop innovative solutions.

Resource Constraints

Communities with limited resources—both financial and staff expertise—can face challenges integrating IoT projects due, in part, to the complexity and cross-cutting nature of these projects. As two academic representatives who work to support community projects noted, it is less resource-intensive for communities to deploy singular, discrete IoT projects than to deploy integrated projects that require time and resources to develop a holistic vision and business plan. Industry representatives from two communities and three other industry representatives, however, highlighted that leveraging value from public assets could help finance communities' IoT projects, as well as help financial sustainability. For example, as discussed above, some communities are making public infrastructure available in return for payment or in-kind donations of technology equipment. Representatives from one of the foreign communities discussed a government push to design projects that are financially sustainable, in such a way that they would be financially viable after grant funding runs out. U.S. federal efforts to support community collaboration have helped communities share their lessons learned on developing new business models, a process that also helps communities invest their funds more efficiently and effectively, by reducing the unknowns and subsequently the risk of investment.

These rapidly developing technologies often also require new and unique expertise, particularly across sectors or disciplines, to deploy and maintain. A local transportation department representative from one community noted that his department's responsibilities are no longer confined to technical engineering skills but also involve expertise in information technology and data management, which requires additional training. Representatives from two domestic and three foreign communities discussed efforts to create new staff positions or retrain staff in existing positions. Representatives from a foreign community discussed creating a chief digital officer whose responsibilities include using data to improve efficiency for citizens and combining knowledge in data analytics with public policy.

Evolving Technologies

Representatives from two domestic communities we reviewed highlighted the fact that IoT-related technologies are constantly evolving, an evolution that ultimately makes integrating projects even more challenging. And, as we have reported in the past, integrating technologies often requires multiple phases of testing, which requires time and resources, and ultimately may require changes to the system or technology and re-testing.[44] Communities with limited resources may prefer to focus on discrete projects, rather than risk investment in integrated projects with uncertain results. For example, representatives from two of the domestic communities spoke about project integration as the "next step" after they deploy the discrete projects. And representatives from two domestic communities, as well as three other industry and academic representatives, said that it is risky to develop a holistic, integrated project when the specific technology is not proven to be effective or could be completely different in 5 or 10 years. Selected federal efforts [45] seek to help communities design replicable IoT projects and reduce the risk for subsequent communities. These and other efforts, while under way, are likely to take several years or longer to fully implement and measure success.

Agency Comments

We requested comments on a draft of this product from Commerce, DOE, HHS, DHS, DOJ, DOT, EPA, FCC, FTC, NSF, and OSTP. Commerce, DOE, FTC, NSF, and OSTP provided technical comments, which we incorporated as appropriate. HHS, DHS, DOJ, DOT, EPA, and FCC did not provide comments.

[44] GAO, *Positive Train Control: Additional Authorities Could Benefit Implementation*, GAO-13-720 (Washington, D.C.: Aug. 16, 2013).

[45] For example, in September 2016, NIST announced $350,000 in four grants enabling four communities to work together on innovative smart city solutions. These Replicable Smart City Technologies grants that are awarded to teams of communities focus on the development and deployment of interoperable technologies to address important public concerns regarding air pollution, flood prediction, rapid emergency response, and improved citizen services through interoperable smart city solutions that can be implemented by communities of all types and sizes.

We are sending copies of this report to the appropriate congressional committees, relevant federal agencies, and other interested parties. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or members of your staff have questions about this report, please contact Mark Goldstein at (202) 512-2834 or goldsteinm@gao.gov or Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix II.

Mark Goldstein
Director, Physical Infrastructure

Nabajyoti Barkakati
Director, Center for Science, Technology, and Engineering

List of Requesters

The Honorable Elijah E. Cummings
Ranking Member
Committee on Oversight and Government Reform
House of Representatives

The Honorable Brian Schatz
Ranking Member
Subcommittee on Communications, Technology, Innovation, and the Internet
Committee on Commerce, Science, and Transportation
United States Senate

The Honorable Cory A. Booker
United States Senate

The Honorable Deb Fischer
United States Senate

The Honorable Cory Gardner
United States Senate

Appendix I: Information on Selected Federal Agencies

Table 1: Selected Federal Agencies, Mission, and Example of Relevant Support for IoT Applications in Communities

Selected federal agency	Mission	Example of relevant support for IoT applications in communities
Department of Commerce's National Institute of Standards and Technology (NIST)	NIST works to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.	• Serves as focal point for conducting scientific research and developing measurements, standards, and related technologies in the federal government. • Supports the development and application of standards, guidelines, and related tools to improve the cybersecurity of connected devices and the environments in which they are deployed. • Collaborates with stakeholders across government, industry, international bodies, and academia, via the NIST IOT Cybersecurity program in order to cultivate trust and promote U.S. leadership in IoT.
Department of Commerce's National Telecommunications & Information Administration (NTIA)	NTIA is the Executive Branch agency principally responsible by law for advising the President on telecommunications and information policy issues.	• Manages federal spectrum and identifies potential commercial spectrum. • Develops policy on issues related to the Internet economy, including online privacy and cybersecurity. • Performs research and engineering to support telecommunications policy and spectrum management.
Department of Energy (DOE)	DOE works to ensure America's security and prosperity by addressing its energy, environmental and nuclear challenges through transformative science and technology solutions.	• Supports fundamental scientific research for energy and is the nation's largest supporter of basic research in the physical sciences, including the use of IoT technologies in helping ensure a resilient, reliable, and flexible electricity system. • Supports applied research and development on energy efficient buildings, building equipment, and mobility systems.
Department of Health and Human Services (HHS)	HHS is the federal government's principal department responsible for protecting the health of Americans and providing essential human services.	• Promotes awareness of and mitigate risks to network-enabled medical devices.
Department of Homeland Security (DHS)	DHS is lead federal agency for securing civilian government computer systems, and works with industry and state, local, tribal, and territorial governments to secure critical infrastructure and information systems, among other things.	• Works to analyze and reduce cyber threats and vulnerabilities; • Coordinates the response to cyber incidents to ensure that our computers, networks, and cyber systems remain safe.

Selected federal agency	Mission	Example of relevant support for IoT applications in communities
Department of Justice (DOJ)	DOJ enforces the law and defends the interests of the United States according to the law; ensures public safety against threats foreign and domestic; provides federal leadership in preventing and controlling crime; seeks just punishment for those guilty of unlawful behavior; and works to ensure fair and impartial administration of justice for all Americans.	• Investigates and prosecutes cybercrimes where the exploitation of IoT vulnerabilities cause communal harm. • Recommends precautions to shield IoT devices from cyber intrusions and to prevent their use in disruptive cyber attacks. • Formed a threat analysis team to study the security of IoT.
Department of Transportation (DOT)	DOT is the principal department responsible for implementing national transportation policy and administering most federal transportation programs.	• Conducts research, development, and outreach activities to facilitate the adoption of information and communication technology to enable society to move safely and efficiently
Environmental Protection Agency (EPA)	EPA works to protect health and the environment.	• Awards grants, conducts research, challenges, and education activities in areas relating to public health and environmental monitoring, such as air quality sensors.
Federal Communications Commission (FCC)	FCC is an independent U.S. government agency overseen by Congress. It is the United States' primary authority for administering communications laws and regulating use of spectrum and communications technology, except with respect to the operations of other federal entities.	• Identifies and allocates spectrum to support evolving service needs including IoT. • Formed a technological Advisory Council, which has produced position statements, recommendations, forecasts, and related materials on IoT technologies. • Participates with industry to understand evolving needs for IoT deployment.
Federal Trade Commission (FTC)	FTC works to prevent business practices that are anticompetitive or deceptive or unfair to consumers; to enhance informed consumer choice and public understanding of the competitive process; and to accomplish this without unduly burdening legitimate business activity.	• Recommended a series of concrete steps that businesses can take to enhance and protect consumers' privacy and security when using IoT devices.
National Science Foundation (NSF)	NSF works to promote the progress of science; to advance the national health, prosperity, and welfare; to secure the national defense; and for other purposes.	• Supports research and education across all fields and disciplines of science and engineering and at all levels of education, including IoT technologies.
Office of Science and Technology Policy (OSTP)	OSTP works to help coordinate science and technology policy across the government; build partnerships among federal, state, and local governments and the private sector; and develop policies related to science and technology activity.	• Oversees the Networking and Information Technology Research and Development program, which is a multiagency effort that seeks to provide the research and development (R&D) foundations for assuring continued U.S. technological leadership and meeting the needs of the Federal Government for advanced information technologies.

Source: GAO analysis of federal agency documents | GAO-17-570

Appendix II: GAO Contacts and Staff Acknowledgments

GAO Contacts

Mark Goldstein, (202) 512-2834 or goldsteinm@gao.gov

Nabajyoti Barkakati, (202) 512-4499 or barkakatin@gao.gov

Staff acknowledgments

In addition to the contacts named above, Susan Zimmerman (Assistant Director), Gretchen Snoey (Analyst in Charge), Eli Albagli, Edward Alexander, Jr., Ana Ivelisse Avilés, Brett Caloia, Joseph Cook, John de Ferrari, Camilo Flores, Sara Ann Moessbauer, Christopher Murray, Amy Rosewarne, and Andrew Stavisky made key contributions to this report.

Tommy Baril, Jennifer Beddor, Leia Dickerson, Karen Doran, Lawrance Evans, Jr., Philip Farah, John Neumann, Malika Rice, Stephen Sanford, and Sarah Veale also made contributions to this report.

Related GAO Products

Internet of Things: Enhanced Assessments and Guidance Are Needed to Address Security Risks in DOD. GAO-17-514SU. Washington, D.C.: June 7, 2017.

Technology Assessment: Internet of Things: Status and implications of an increasingly connected world. GAO-17-75. Washington, D.C.: May 15, 2017.

Health Care: Telehealth and Remote Patient Monitoring Use in Medicare and Selected Federal Programs. GAO-17-365. Washington, D.C.: April 14, 2017.

Cybersecurity: Actions Needed to Strengthen U.S. Capabilities. GAO-17-440T. Washington, D.C.: February 14, 2017.

Data Analytics and Innovation: Emerging Opportunities and Challenges. GAO-16-659SP. Washington, D.C.: September 20, 2016.

Intelligent Transportation Systems: Urban and Rural Transit Providers Reported Benefits but Face Deployment Challenges. GAO-16-638. Washington, D.C.: June 21, 2016.

Critical Infrastructure Protection: Measures Needed to Assess Agencies' Promotion of the Cybersecurity Framework. GAO-16-152. Washington, D.C.: December 17, 2015.

Intelligent Transportation Systems: Vehicle-to-Infrastructure Technologies Expected to Offer Benefits, but Deployment Challenges Exist. GAO-15-775. Washington, D.C.: September 15, 2015.

Critical Infrastructure Protection: Cybersecurity of the Nation's Electricity Grid Requires Continued Attention. GAO-16-174T. Washington, D.C.: October 21, 2015.

Spectrum Management: FCC's Use and Enforcement of Buildout Requirements. GAO-14-236. Washington, D.C.: February 26, 2014.

Intelligent Transportation Systems: Vehicle-to-Vehicle Technologies Expected to Offer Safety Benefits, but Deployment Challenges Exist. GAO-14-13. Washington, D.C.: November 1, 2013.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, LinkedIn, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov and read The Watchblog.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: http://www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548