CENTER FOR DATA INNOVATION

Everything the U.S. Government Is Doing to Help the Private Sector Build the Internet of Things

By Daniel Castro and Joshua New | December 12, 2016

The Internet of Things (IoT) offers a host of potential benefits to many sectors of the economy, including agriculture, manufacturing, transportation, and health care.[1] While the U.S. federal government has undertaken an array of important activities to support the development of the Internet of Things in the private sector, these efforts are mostly uncoordinated and the government lacks a strategic vision. In the coming years, the federal government should better organize its support of widespread IoT use in America by establishing a national strategy for the Internet of Things.

The U.S. federal government has a significant opportunity to support private sector efforts at building the Internet of Things.

As the Center for Data Innovation has written previously, because the Internet of Things—physical objects embedded with sensors or actuators and connected to a network, which can include everything from home appliances to automated factories to connected cars—offers so many important economic and social benefits, countries should develop national strategies to promote its adoption and use.[2] Among other benefits, creating a national strategy would help coordinate existing initiatives and allow government agencies to better plan future projects. One way to accelerate development and adoption of the Internet of Things is for the U.S. federal government to be an early adopter.[3] However, in addition to being an early adopter, the U.S. government has a significant opportunity to support private-sector efforts at building the Internet of Things through other activities, including programs to provide technical resources; strengthen cybersecurity; develop industry-friendly regulations; ensure spectrum availability; support research, development, and demonstration; and coordinate stakeholders. Many of these programs are underway, although they often lack the coordination and scale necessary to support the Internet of Things as completely as possible. The purpose of this report is to shine a light on these activities, so policymakers have a better understanding of what is being done today and where gaps exist.

PROVIDING TECHNICAL RESOURCES

Several U.S. federal agencies are providing technical resources to support the Internet of Things largely by providing guidance on standards development and interoperability. In May 2016, the National Institute of Standards and Technology (NIST) Cyber-Physical Systems Public Working Group (CPS PWG) published the *Framework for Cyber-Physical Systems*.[4] The framework provides comprehensive technical information, definitions, and taxonomies on five categories of issues related to the Internet of Things: reference architecture, cybersecurity and privacy, timing and synchronization, data interoperability, and use cases.[5] NIST's framework helps guide the development of solutions to a variety of technical challenges associated with the Internet of Things.[6] CPS PWG also manages an array of projects at NIST labs to produce technical research related to a variety of IoT applications, including smart manufacturing, disaster resilience, and smart grid.[7]

NIST's Engineering Lab runs multiple initiatives to advance metrology (i.e., scientific measurement) that benefit the Internet of Things.[8] For example, its Sensing and Perception Systems Group produces metrological research related to smart manufacturing and construction applications, and its Advanced Metering in Smart Distribution Grids project focuses on improving the accuracy of smart-meter sensor technology.[9] NIST also published a *Research Roadmap for Smart Fire Fighting* in 2015 to provide guidance on overcoming technical challenges related to connected technologies that can improve firefighting and fire-protection efforts.[10]

To promote interoperability, in September 2015, NIST published its "Big Data Interoperability Framework," which provides exhaustive technical and taxonomical information as well as standards information for data technologies, particularly the Internet of Things.[11] NIST has also published the third iteration of its *Framework and Roadmap for Smart Grid Interoperability Standards*, and is currently developing its "IoT-Enabled Smart City Framework."[12] Additionally, the Department of Transportation's (DOT's) Intelligent Transportation Systems (ITS) Standards Program is conducting a variety of activities to support interoperable ITS standards and architectures, including testing, providing technical assistance to local and state stakeholders, and developing deployment guidance.[13]

STRENGTHENING CYBERSECURITY

To address cybersecurity needs, NIST published its "Framework for Improving Critical Infrastructure Cybersecurity" in early 2014.[14] Though its focus is far broader than just the Internet of Things, the framework provides valuable recommendations and cybersecurity best practices that apply to all connected technologies. In May 2016, NIST released the second draft of its *Systems Security Engineering*, which provides additional technical guidance for securing connected technologies.[15]

Several agencies have taken steps to develop and promote general IoT cybersecurity best practices. In January 2015, the Federal Trade Commission (FTC) published high-level guidance for businesses about how to build security into IoT products.[16] The National Telecommunications and Information Administration (NTIA) has committed to hosting a series of public meetings to convene IoT stakeholders and discuss issues related to security upgradability and patching, and it held its first meeting in October 2016.[17] And in November 2016, the Department of Homeland Security (DHS) published "Strategic Principles for Securing the Internet of Things," a whitepaper that details the security risks of IoT devices and establishes nonbinding principles for responsible cybersecurity practices.[18]

For sector-specific issues, NIST published extensive guidelines for smart-grid cybersecurity in 2014, and the FCC's Technological Advisory Council (TAC) Cybersecurity Working Group published a white paper in December 2015 detailing the technical considerations of cybersecurity for consumer IoT devices.[19] Additionally, in January 2016, the Food and Drug Administration (FDA) issued draft guidance for medical-device manufacturers focusing on post-market cybersecurity challenges for networked medical devices.[20] Finally, the National Highway Traffic Safety Administration (NHTSA), an agency within DOT, has published "Cybersecurity Best Practices for Modern Vehicles," an overview of voluntary guidelines to improve security in connected vehicles.[21]

In addition to providing guidance, some federal agencies have taken steps to encourage the development of new technologies to improve cybersecurity for the Internet of Things since many kinds of connected devices lack the computing power to use traditional cybersecurity approaches. For example, the Defense Advanced Research Projects Agency (DARPA) launched the "Leveraging the Analog Domain for Security" program in September 2015 to fund research into technology that can analyze electromagnetic, acoustic, thermal, and other kinds of emissions from connected devices to detect the presence of malicious software.[22] Malicious software can cause connected devices to function differently than intended, causing changes in the emissions these devices produce.[23] DARPA has allocated up to $36 million for the first phase of the project, which will run for 18 months.[24]

DEVELOPING INNOVATION-FRIENDLY REGULATIONS

Several federal agencies have completed or are working on regulatory and policy efforts that will substantially influence the development and adoption of the Internet of Things.

The FDA's medical-device cybersecurity guidance, when finalized, will guide FDA's regulatory approach towards the security of medical IoT technologies.[25] In July 2016, FDA also issued guidance exempting low-risk devices from regulatory oversight in certain conditions.[26] For example, connected devices that collect health data, such as fitness trackers, will not be subject to regulatory scrutiny, provided that they only function to promote healthy behavior, and not diagnose or treat a specific disease.[27] Additionally, in February 2015, FDA finalized guidance exempting medical-device data systems—connected devices that store, transfer, display, or convert medical data—from regulatory oversight.[28]

In 2014, DOT issued an advance notice of proposed rulemaking (NPRM) mandating the use of vehicle-to-vehicle (V2V) communications, which rely on connected technologies to improve vehicle safety by sharing data such as speed and location, in new cars.[29] After soliciting feedback from industry and the public, DOT submitted the NPRM to the Office of Management and Budget in January 2016, with plans to issue the V2V mandate in mid-2016, though it had not done so as of October 2016.[30] Transportation Secretary Anthony Foxx has stated that the goal of the V2V mandate is to encourage the deployment of innovative connected technologies, rather than create burdensome restrictions.[31] And in September 2016, the National Highway Traffic Safety Administration (NHTSA) published its Federal Automated Vehicles Policy, which recommends policies that encourage the collection and sharing of large amounts of data from connected sensors in autonomous vehicles to accelerate the development of the technology.[32] Although the policy is largely supportive of innovative uses of connected sensors, it does include counterproductive and unnecessary recommendations related to consumer privacy that are not relevant to vehicle safety, have the potential to create duplicative or conflicting rules, and which are outside the immediate expertise of the agency.[33]

Other federal agencies are exploring how the Internet of Things impacts existing regulations. In January 2015, the Federal Trade Commission released a staff report summarizing a workshop it hosted to discuss the security and privacy considerations of the Internet of Things.[34] The report puts forth several best practices for businesses deploying the Internet of Things to adopt to mitigate security and privacy risks and earn consumer trust.[35] Similarly, though not explicitly focused on the Internet of Things, the FTC published another report in January 2016 examining the potential for businesses to use data, such as information collected by sensor networks, to discriminate or harm consumers.[36]

To guide future regulatory actions and identify the proper role of the federal government on issues related to the Internet of Things, in April 2016 NTIA issued a request for comments (RFC) on a broad array of benefits and challenges created by the Internet of Things.[37] After reviewing these comments, NTIA will produce a working paper identifying specific areas of focus for federal agencies to address issues limiting IoT deployment, overcome possible challenges such as consumer protection and spectrum availability, and promote private sector development of the Internet of Things.[38] Importantly, the RFC also seeks to address the value and viability of an overarching national strategy for the Internet of Things, an approach employed by several other countries.[39]

ENSURING SPECTRUM AVAILABILITY

The success of the Internet of Things relies on several public goods, including spectrum. The FCC has undertaken a number of proceedings to make additional wireless spectrum available for commercial use. While these efforts are not specifically aimed at the Internet of Things, additional spectrum, including licensed, unlicensed, and blended access models, will facilitate cheaper, more abundant connectivity that will support a broad array of connected technologies. The 2015 AWS-3 auction made 65 megahertz of licensed, flexible-use spectrum bands available to wireless network operators. The FCC is working to improve rules governing access to the 5 gigahertz (GHz) band and made considerable progress to ease access to an additional 100 megahertz (MHz) of unlicensed spectrum. The FCC is also experimenting with a new model of spectrum access for the 3.5 GHz band to better coordinate licensed and unlicensed users. The ongoing 600 MHz incentive auction will allow television broadcasters to sell their rights to these spectrum bands to wireless providers, and FCC is exploring how to free up more high-band spectrum above 24 GHz, which is expected to be an important component for next-generation 5G networks.[40]

SUPPORTING RESEARCH, DEVELOPMENT, AND DEMONSTRATION

Since the Internet of Things consists of many different technologies, such as batteries, sensors, and transmitters, it is difficult to clearly define all the federal government's R&D efforts that benefit the Internet of Things, either directly or indirectly, as many initiatives focus on a particular component, rather than the technology as a whole.

In September 2015, the White House launched its Smart Cities Initiative, to use connected technologies to solve municipal challenges and improve government services, and earmarked over $160 million in new funding to advance research in this space, ranging from connected vehicle pilot projects to developing advanced emergency-response technologies.[41] In September 2016, the White House announced $80 million in additional federal support for the Smart Cities Initiative, focusing specifically on projects related to climate, transportation, public safety, and transforming city services using connected technologies and data.[42]

In December 2014, DOT's Intelligent Transportation Systems program released its 20152019 Strategic Plan, detailing a host of ongoing and planned research projects across six categories that all rely heavily on connected technologies: connected vehicles, which includes V2V communications; automation; emerging capabilities; enterprise data; interoperability; and supporting adoption and deployment.[43] In September 2015, DOT also announced $42 million in funding for New York City, Wyoming, and Tampa to conduct connected vehicle pilot programs to test both V2V and vehicle-to-infrastructure (V2I) technologies that could substantially increase public safety and reduce congestion.[44] Most notably, DOT launched its Smart City Challenge in December 2015 and awarded $40 million from the White House's Smart Cities Initiative to Columbus, Ohio, to integrate connected technologies throughout its transportation network to reduce congestion, improve transportation safety, support underserved communities, promote economic growth, and benefit the environment.[45] To further incentivize participation in the challenge, DOT worked with private firms to provide an additional $20 million in funding and a variety of IoT management tools to the winning city.[46] For example, DOT has partnered with Sidewalk Labs for a project called Flow to create a monitoring and management system for public transportation. This system will allow cities and DOT to better understand how people navigate cities to tackle transportation challenges and increase engagement with citizens.[47] And in October 2016, DOT announced an additional $56.6 million in grant funding for advanced transportation technology projects focusing on connected vehicles and infrastructure in eight cities.[48]

Also, to support smart cities, NIST runs the Global City Teams Challenge, which primarily serves as a community of practice for smart-city companies and municipal governments, which received $2.5 million from the White House Smart Cities Initiative to support participating researchers and municipalities in 2015, and an additional $1 million in 2016.[49]

The Environmental Protection Agency (EPA) has launched a series of smaller-scale challenges to support the development of useful applications of IoT technologies. In June 2012, EPA hosted a challenge with the Department of Health and Human Services (HHS) that awarded $100,000 to teams that developed a method for linking physiological data and air-quality data collected by networked sensors to support research into how pollutants impact human health.[50] In 2013, EPA offered up to $10,000 for the winner of a challenge to develop real-time sewer overflow sensors that could help improve municipal sanitation efforts.[51] And in August 2016, EPA launched the Smart Cities Air Challenge, which will award up to $50,000 each to two communities that submit the best proposals to deploy hundreds of networked air-quality sensors and develop best practices for collecting, managing, and sharing air-quality data.[52]

DHS runs several Apex programs—clusters of R&D projects, most of which involve the Internet of Things—focused on improving border screening and monitoring, national security, public safety, and disaster response.[53] For example, the Next Generation First Responder program, launched in January 2015, spans 40 projects working to develop connected technologies that protect emergency responders, reduce response time, and improve decision-making.[54] Additionally, the Screening at Speed program, run in conjunction with Department of Energy (DOE) national laboratories and the Transportation Security Administration, is developing advanced imaging and detection-sensor technologies to improve airport security, reduce its invasiveness, and make air travel more convenient.[55]

The Centers for Disease Control and Prevention (CDC) launched a pilot research project in October 2015 to investigate the feasibility of existing and emerging technologies, including the Internet of Things, for monitoring underground mining environments to safeguard miners' health.[56] The Intelligence Advanced Research Projects Activity (IARPA) Office of Smart Collection conducts research projects involving the use of sensors and connected technologies to improve intelligence gathering.[57] For example, the Molecular Analyzer for Efficient Gas-phase Low-power INterrogation (MAEGLIN) project is developing low-power chemical-analysis technology for remote inspection and identification of explosives, chemical weapons, and nuclear material.[58]

The National Science Foundation (NSF) provides funding for several research areas related to the Internet of Things. For example, the NSF Small Business Innovation Research/Small Business Technology Transfer program provides seed funding for projects in 10 technology areas, one of which specifically focuses on the Internet of Things, and several others that support it tangentially, such as Smart Health and Biomedical Technologies, as well as Electronic Hardware, Robotics, and Wireless Technologies.[59] NSF's Directorate for Computer & Information Science & Engineering (CISE) also provides funding for a variety of research projects related to the Internet of Things, such as its Information & Intelligent Systems program and its Computing and Communication Foundations program.[60]

USDA's National Institute of Food and Agriculture (NIFA) is offering educational and application assistance, as well as grants, to help spur the use and adoption of the Internet of Things and precision agriculture technologies in the farming sector.[61] In partnership with universities and other agencies, NIFA supports the development of sensors and associated software to better observe and analyze data from animal production, forest production, and crop production, not only so farmers can do their job better, but to help make consumer products safer and more user-friendly.[62]

Finally, in May 2016, the White House released the Federal Big Data Research and Development Strategic Plan, outlining the administration's R&D strategies across seven focus areas, several of which directly relate to the Internet of Things.[63] These strategies include "build and enhance research cyberinfrastructure that enables big data innovation in support of agency missions," "create next-generation capabilities by leveraging emerging big data," and "improve the national landscape for Big Data education and training to fulfill increasing demand for both deep analytical talent and analytical capacity for the broader workforce foundations, techniques, and technologies."[64] The latter strategy will be particularly beneficial for the Internet of Things as the value of connected technologies lies with the data they generate. The United States already suffers from a data-science skills gap, with far fewer workers with the skills to capture the value of data than necessary, and this gap will only widen as IoT deployments increase.[65] Though the private sector invests heavily in worker training, the development of human capital is fundamentally a public-sector responsibility.

COORDINATING STAKEHOLDERS

Many federal agencies are supporting private-sector efforts to develop the Internet of Things by coordinating the actions of government, academic, and other stakeholders.

DOE's Federal Smart Grid Task Force, established in 2007, consists of experts from 11 different federal agencies to coordinate strategies to promote awareness and integration of smart-grid technologies and practices.[66] Also to aid smart-grid efforts, NIST operates the Smart Grid National Coordination project and, in conjunction with the International Trade Administration and DOE, has established the International Smart Grid Action Network, a 17-country collaboration to encourage the adoption of common international standards for smart-grid technologies.[67]

In 2008, CDC partnered with General Motors to develop the Advanced Automatic Collision Notification (AACN), a series of common protocols to support communication between automotive telemetry technologies and emergency medical services.[68] Cars that use AACN can automatically share crucial data with emergency responders in the event of a crash, including the vehicle's location, the severity and direction of impact, and whether or not airbags deployed, which can substantially improve emergency response efforts.[69]

In November 2015, NSF launched its Big Data Regional Innovation Hubs—clusters of academic, industry, government, and civil-society stakeholders working to advance data-driven innovation in areas including precision agriculture, smart communities, and natural hazard management, which all involve the heavy use of connected technologies.[70] The hubs coordinate the activities of 250 organizations across 50 states to facilitate partnerships, collaborate, and address regional challenges.[71]

To support smart manufacturing, NIST runs Manufacturing USA, formerly the National Network for Manufacturing Innovation, a network of nine institutes (with an expected six additional institutes to be announced by 2017) that support pre-competitive cooperative research on advanced-manufacturing technologies.[72] Manufacturing USA convenes public-private partnerships, works with universities, and promotes information-sharing and collaboration across the federal government to spur the development and adoption of innovative manufacturing technologies, such as sensor-laden manufacturing plants.[73] Several of the institutes, such as the Smart Manufacturing Innovation Institute and Advanced Functional Fabrics of America, have an explicit focus on supporting IoT-related technologies.[74] Additionally, NIST's Engineering Laboratory provides a suite of software and tools for testing, evaluation, and standards development for smart-manufacturing applications.[75]

For smart-transportation stakeholders, DOT operates the Research Data Exchange (RDE) transportation data-sharing portal, which allows researchers to access archived and real-time data from smart-transportation testing.[76] The goal of the RDE is to accelerate development and deployment of connected technologies in vehicles, infrastructure, and other platforms by providing relevant testing data sets such as GPS tracking, traffic data, data from vehicle devices, and CCTV cameras.[77] Several of the federal government's research and development efforts also serve a stakeholder coordination function. For example, NIST's Global Cities Team Challenge, the White House Smart Cities Initiative, and DOT's Smart City Challenge all focus on establishing communities of practice, coordinating public and private sector efforts, and sharing best practices.

CONCLUSION

The U.S. federal government has initiated a wide array of projects to support the growth of the Internet of Things. But many of these projects are relatively small scale and one-off. Absent a large-scale coordinated government effort to accelerate the development and deployment of the Internet of Things, these projects are likely insufficient to grow the technology as rapidly as would be desirable, resulting in the United States losing out on considerable economic and social benefits.[78] Fortunately, Congress has signaled its support for a national strategy for the Internet of Things that would remedy this.

In early 2016, bipartisan members of the House and Senate introduced the Developing Innovation and Growing the Internet of Things (DIGIT) Act, which would address many of the questions raised by NTIA's RFC on the Internet of Things.[79] The DIGIT Act would direct the Secretary of Commerce to establish a working group of government, industry, consumer, and civil-society stakeholders to report on policies and practices that hinder IoT development, propose policies to improve federal agency coordination on IoT issues, and identify opportunities for federal agencies to make better use of the Internet of Things.[80] Additionally, the DIGIT Act would direct the FCC to report on the current and future spectrum needs of the Internet of Things and provide recommendations to overcome any relevant regulatory barriers.[81] The DIGIT Act was introduced following 2015 House and Senate resolutions that acknowledged the potential benefits of the Internet of Things and called for the development of a national strategy to support the technology.[82]

The stage is set for the Trump administration to take up the mantle and establish the federal government not only as a lead adopter of the Internet of Things, but also as a champion for the technology and a valuable partner for the private sector.

NTIA's RFC on the Internet of Things also raised the issue of whether the federal government should develop a national strategy for the Internet of Things, and many of the submitted comments agreed this would be beneficial for the growth of the technology.[83] As the Obama administration draws to a close, it is unlikely the federal government will make significant additional progress toward a national strategy. However, the stage is set for the Trump administration to take up the mantle and establish the federal government not only as a lead adopter of the Internet of Things, but also as a champion for the technology and a valuable partner for the private sector.

REFERENCES

1. Daniel Castro and Jordan Misra, “The Internet of Things,” (Center for Data Innovation, November 2013), http://www2.datainnovation.org/2013-internet-of-things.pdf.
2. Joshua New and Daniel Castro, “Why Countries Need National Strategies for the Internet of Things,” (Center for Data Innovation, December 16, 2015), http://www2.datainnovation.org/2015-national-iot-strategies.pdf.
3. Daniel Castro, Joshua New, and Alan McQuinn, “How is the Federal Government Using the Internet of Things?” Center for Data Innovation, July 25, 2016, http://www2.datainnovation.org/2016-federal-iot.pdf.
4. *Framework for Cyber-Physical Systems* (U.S. National Institute of Standards and Technology, May 2016), https://s3.amazonaws.com/nist-sgcps/cpspwg/files/pwgglobal/CPS_PWG_Framework_for_Cyber_Physical_Systems_Release_1_0Final.pdf.
5. Ibid*.*
6. Ibid.
7. “Cyber-Physical Systems,” National Institute of Standards and Technology, accessed October 26, 2016, https://www.nist.gov/el/cyber-physical-systems.
8. “Metrology,” U.S. National Institute of Standards and Technology, accessed October 26, 2016, https://www.nist.gov/topics/metrology.
9. Ibid; “Advanced Metering in Smart Distribution Grids,” U.S. National Institute of Standards and Technology, accessed October 26, 2016, https://www.nist.gov/programs-projects/advanced-metering-smart-distribution-grids.
10. U.S. National Institute of Standards and Technology, “Research Roadmap Traces the Path to 'Smart' Fire Fighting,” news release, June 18, 2015, http://www.nist.gov/el/fire_research/201506_smart_fire_roadmap.cfm.
11. “Big Data Information,” U.S. National Institute of Standards and Technology, accessed October 26, 2016, http://www.nist.gov/itl/bigdata/bigdatainfo.cfm.
12. *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0*, (U.S. National Institute of Standards and Technology, May 2014), http://www.nist.gov/smartgrid/upload/Draft-NIST-SG-Framework-3.pdf; “IoT-Enabled Smart City Framework,” (U.S. National Institute of Standards and Technology, February 18, 2016), https://s3.amazonaws.com/nist-sgcps/smartcityframework/files/IoT-EnabledSmartCityFrameworkWP.pdf.

13. “Key Program Activities,” U.S. Department of Transportation Intelligent Transportation Systems Joint Program Office, accessed October 26, 2016, https://www.standards.its.dot.gov/About/ProgramActivities.

14. “Framework for Improving Critical Infrastructure Cybersecurity,” National Institute of Standards and Technology, February 12, 2014, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

15. Ron Ross, Michael McEvilley, and Janet Oren, *Systems Security Engineering* (U.S. National Institute of Standards and Technology, May 2016), http://csrc.nist.gov/publications/drafts/800-160/sp800_160_second-draft.pdf; “Building Security into Cyber-Physical Systems: NIST Researchers Suggest Approach for Trustworthy Modern Infrastructure,” National Institute of Standards and Technology, May 4, 2016, http://www.nist.gov/itl/csd/building-security-into-cyber-physical-systems-nist-researchers-suggest-approach-for-trustworthy-modern-infrastructure.cfm.

16. “Careful Connections: Building Security in the Internet of Things,” U.S. Federal Trade Commission, January 2015, https://www.ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf.

17. “Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching,” U.S. National Telecommunications and Information Administration, October 24, 2016, https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security.

18. “Strategic Principles for Securing the Internet of Things (IoT),” U.S. Department of Homeland Security, November 15, 2016, https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf.

19. *Guidelines for Smart Grid Cybersecurity Volume 1 - Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements* (U.S. National Institute of Standards and Technology, September 2014), http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf; FCC TAC Cybersecurity Working Group, “Technical Considerations White Paper” (U.S. Federal Communications Commission, December 4, 2015), https://transition.fcc.gov/oet/tac/tacdocs/reports/2015/FCC-TAC-Cyber-IoT-White-Paper-Rel1.1-2015.pdf.

20. “Postmarket Management of Cybersecurity in Medical Devices” (U.S. Food and Drug Administration, January 22, 2016), http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf.

21. "Cybersecurity Best Practices for Modern Vehicles," (National Highway Traffic Safety Administration, October 2016), http://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf.

22. Mohana Ravindranath, “DARPA Looking for Tech to Protect the ‘Internet of Things,’” Nextgov, September 28, 2015, http://www.nextgov.com/emerging-tech/2015/09/darpa-looking-tech-protect-internet-things/122231/

23. Ibid.

24. Ibid.

25. “Draft Guidance for Industry and Food and Drug Administration Staff,” (Silver Spring, MD: U.S. Food and Drug Administration’s Center for Devices and Radiological Health, January 22, 2016), http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf.

26. “General Wellness: Policy for Low Risk Devices,” (Rockville, MD: U.S. Food and Drug Administration’s Center for Devices and Radiological Health, July 29, 2016), http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm429674.pdf.

27. Ibid.

28. “Medical Device Data Systems, Medical Image Storage Devices, and Medical Image Communications Devices,” (Rockville, MD: U.S. Food and Drug Administration’s Center for Devices and Radiological Health, February 9, 2015), http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm401996.pdf.

29. U.S. Department of Transportation, “U.S. Department of Transportation Issues Advance Notice of Proposed Rulemaking to Begin Implementation of Vehicle-to-Vehicle Communications Technology,” news release, August 18, 2014, https://www.transportation.gov/briefing-room/us-department-transportation-issues-advance-notice-proposed-rulemaking-begin.

30. Junk Yoshida, “V2X Mandate: It’s Now or Never,” *EE Times*, October 13, 2016, http://www.eetimes.com/document.asp?doc_id=1330623.

31. Anthony Foxx, “A Dialogue with Industry, a Conversation between Cars,” U.S. Department of Transportation, May 13, 2015, https://www.transportation.gov/fastlane/dialogue-industry-conversation-between-cars.

32. National Highway Traffic Safety Administration, *Federal Automated Vehicles Policy* (U.S. Department of Transportation, September 2016), https://www.transportation.gov/sites/dot.gov/files/docs/AV%20policy%20guidance%20PDF.pdf

33. Daniel Castro and Joshua New, “Comments to NHTSA on Proposed Federal Automated Vehicles Policy,” Center for Data innovation, November 21, 2016, http://www2.datainnovation.org/2016-federal-automated-vehicle-policy.pdf.

34. “Internet of Things: Privacy and Security in a Connected World,” (U.S. Federal Trade Commission, January 2015),

https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

35. Ibid.

36. "Big Data: A Tool for Inclusion or Exclusion?" (U.S. Federal Trade Commission, January 2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.

37. "Request for Comments on the Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things," U.S. National Telecommunications and Information Administration," April 5, 2016, https://www.ntia.doc.gov/federal-register-notice/2016/rfc-potential-roles-government-fostering-advancement-internet-of-things.

38. Ibid.

39. Ibid.

40. "FCC Raises Record USD 44.9 Billion in AWS-3 Airwaves Auction," *American Herald*, February 1, 2015, http://www.americaherald.com/fcc-raises-record-usd-44-9-billion-in-aws-3-airwaves-auction/22530/; John Leibovitz, "Breaking Down Barriers to Innovation in the 3.5 GHz Band," U.S. Federal Communications Commissions, April 21, 2015, https://www.fcc.gov/news-events/blog/2015/04/21/breaking-down-barriers-innovation-35-ghz-band; Dan Meyer, "FCC 600 MHz Inventive Auction stage Three Set to Begin Nov. 1," *RCR Wireless*, October 25, 2016, http://www.fiercewireless.com/special-reports/600-mhz-incentive-auction-primer-who-will-bid-when-it-will-happen-how-it-wi; "Notice of Inquiry," (Washington, DC: U.S. Federal Communications Commission, October 17, 2014) https://apps.fcc.gov/edocs_public/attachmatch/FCC-14-154A1.pdf.

41. "FACT SHEET: Administration Announces New 'Smart Cities' Initiative to Help Communities Tackle Local Challenges and Improve City Services," The White House, September 14, 2015, https://www.whitehouse.gov/the-press-office/2015/09/14/fact-sheet-administration-announces-new-smart-cities-initiative-help.

42. "FACT SHEET: Announcing Over $80 million in New Federal Investment and a Doubling of Participating Communities in the White House Smart Cities Initiative," The White House, September 26, 2016, https://www.whitehouse.gov/the-press-office/2016/09/26/fact-sheet-announcing-over-80-million-new-federal-investment-and.

43. Jim Barbaresso et al., "ITS Strategic Plan 2015-2019," (Washington, DC: U.S. Department of Transportation Intelligent Transportation Systems Joint Program Office, December 2014), http://www.its.dot.gov/strategicplan/index.html.

44. U.S. Department of Transportation, "U.S. Department of Transportation Announces up to $42 Million in Next Generation Connected Vehicle

Technologies," news release, September 14, 2015, https://www.transportation.gov/briefing-room/us-department-transportation-announces-42-million-next-generation-connected-vehicle.

45. "FACT SHEET: Obama Administration Announces Columbus, OH Winner of the $40 Million Smart City Challenge to Pioneer the Future of Transportation," The White House, June 23, 2016, https://www.whitehouse.gov/the-press-office/2016/06/23/fact-sheet-obama-administration-announces-columbus-oh-winner-40-million.

46. Ibid.

47. Ibid.

48. "FACT SHEET: Advanced Transportation and Congestion Management Technologies Deployment Program," U.S. Department of Transportation, accessed October 27, 2016, https://www.transportation.gov/Briefing-Room/ATCMTD-Fact-Sheet-2016.

49. "FACT SHEET: Administration Announces New 'Smart Cities' Initiative to Help Communities Tackle Local Challenges and Improve City Services," The White House, September 14, 2015, https://www.whitehouse.gov/the-press-office/2015/09/14/fact-sheet-administration-announces-new-smart-cities-initiative-help.; "FACT SHEET: Announcing Over $80 million in New Federal Investment and a Doubling of Participating Communities in the White House Smart Cities Initiative," The White House, September 26, 2016, https://www.whitehouse.gov/the-press-office/2016/09/26/fact-sheet-announcing-over-80-million-new-federal-investment-and.

50. "My Air, My Health: An HHS/EPA Challenge," Innocentive, June 5, 2012, https://www.innocentive.com/ar/challenge/9932947.

51. "Real-Time Sensor to Monitor Sewer overflows," Innocentive, July 19, 2013, https://www.innocentive.com/ar/challenge/9933103.

52. U.E. Environmental Protection Agency, "Smart City Air Challenge," accessed October 27, 2016, https://www.challenge.gov/challenge/smart-city-air-challenge/.

53. "Apex Programs," U.S. Department of Homeland Security, accessed October 27, 2016, https://www.dhs.gov/science-and-technology/apex-programs.

54. "Next Generation First Responder Apex Program," U.S. Department of Homeland Security, accessed October 27, 2016, https://www.dhs.gov/science-and-technology/ngfr

55. "Screening at Speed," U.S. Department of Homeland Security, accessed October 27, 2016, https://www.dhs.gov/science-and-technology/apex-screening-speed.

56. "Mining Project: Industrial Internet of Things (IIoT) Applications in Underground Coal Mines," Centers for Disease Control and Prevention, December 10, 2015,

http://www.cdc.gov/niosh/mining/researchprogram/projects/project_IndustrialInternet.html.

57. Mohana Ravindranath, "IARPA Wants to Rethink Intelligence Collection," *Nextgov*, May 13, 2015, http://www.nextgov.com/emerging-tech/2015/05/iarpa-wants-rethink-intelligence-collection/112681/?oref=ng-channeltopstory

58. "Molecular Analyzer for Efficient Gas-phase Low-power INterrogation (MAEGLIN)," Office of the Director of National Intelligence, accessed October 27, 2016, https://www.iarpa.gov/index.php/research-programs/maeglin.

59. "Technology Topic Areas," U.S. National Science Foundation, accessed October 27, 2016, http://www.nsf.gov/eng/iip/sbir/topics.jsp.

60. "Information and Intelligent Systems," National Science Foundation, accessed October 27, 2016, https://www.nsf.gov/div/index.jsp?div=IIS; "Computing and Communication Foundations," National Science Foundation, accessed October 27, 2016, https://www.nsf.gov/div/index.jsp?div=CCF.

61. "Precision, Geospatial & Sensor Technologies Programs," U.S. Department of Agriculture, accessed April 21, 2016, https://nifa.usda.gov/program/precision-geospatial-sensor-technologies-programs.

62. "Sensor Applications," U.S. Department of Agriculture, accessed April 21, 2016, https://nifa.usda.gov/sensor-applications/.

63. Keith Marzullo, "Administration Issues Strategic plan for Big Data Research and Development," The White House, May 23, 2014, https://www.whitehouse.gov/blog/2016/05/23/administration-issues-strategic-plan-big-data-research-and-development.

64. "The Federal Big Data Research and Development Strategic Plan," (Executive Office of the President, May 2016), https://www.whitehouse.gov/sites/default/files/microsites/ostp/NSTC/bigdatardstrategicplan-nitrd_final-051916.pdf.

65. Daniel Castro, "Why Skills Matter more than Ever in Our data-Driven Economy," Center for Data Innovation, May 19, 2016, https://www.datainnovation.org/2015/05/why-skills-matter-more-than-ever-in-our-data-driven-economy/.

66. "Federal Smart Grid Task Force," U.S. Department of Energy, accessed October 27, 2016, http://energy.gov/oe/technology-development/smart-grid/federal-smart-grid-task-force.

67. "Smart Grid National Coordination," U.S. National Institute of Standards and Technology, accessed October 27, 2016, http://www.nist.gov/el/smartgrid/sgridcoord.cfm; "Smart Grid International Coordination," U.S. National Institute of Standards and Technology, accessed October 27, 2016, http://www.nist.gov/smartgrid/international-coordination.cfm.

68. "Recommendations from the Expert Panel: Advanced Automatic Collision Notification and Triage of the Injured Patient," (Atlanta, GA: U.S. Centers for Disease Control and Prevention, 2008), https://stacks.cdc.gov/view/cdc/5304/.

69. Ibid.

70. U.S. National Science Foundation, "Establishing a Brain Trust for Data Science," news release, November 2, 2015, http://www.nsf.gov/news/news_summ.jsp?cntn_id=136784.

71. Ibid.

72. "Manufacturing USA – the National Network for Manufacturing Innovation," U.S. National Institute of Standards and Technology, accessed October 27, 2016, https://www.manufacturing.gov/nnmi/.

73. "National Network for Manufacturing Innovation: A Preliminary Design," (Washington, DC: Executive Office of the President, January 10, 2013), https://www.manufacturing.gov/files/2015/12/NNMI_prelim_design.pdf.

74. "Institutes," Manufacturing USA, accessed December 5, 2016, https://www.manufacturingusa.com/institutes.

75. "Software and Tools," U.S. National Institute of Standards and Technology, accessed October 27, 2016, http://www.nist.gov/el/softwaretool.cfm.

76. "Research Data Exchange (RDE) Announcement," U.S. Department of Transportation Intelligent Transportation System Joint Program Office, accessed October 27, 2016, http://www.its.dot.gov/press/2013/rde.htm.

77. Ibid.

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

79. DIGIT Act, S. 2607, 114th Cong. (2016).

80. Ibid.

81. Ibid.

82. A Resolution Expressing the Sense of the Senate About a Strategy for the Internet of Things to Promote Economic Growth and Consumer Empowerment, S.Res. 110, (2015); Expressing the Sense of the House of Representatives About a National Strategy for the Internet of Things to Promote Economic Growth and Consumer Empowerment, H.Res. 195, (2015).

83. "Comments on the Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things," U.S. National Telecommunications and Information Administration, June 6, 2016, https://www.ntia.doc.gov/federal-register-notice/2016/comments-potential-roles-government-fostering-advancement-internet-of-things.

ABOUT THE AUTHORS

Daniel Castro is director of the Center for Data Innovation and vice president at the Information Technology and Innovation Foundation. His research interests include health IT, data privacy, e-commerce, e-government, electronic voting, information security, and accessibility. Previously, Castro worked as an IT analyst at the Government Accountability Office where he audited IT security and management controls at various government agencies. He has a B.S. in foreign service from Georgetown University and an M.S. in information security technology and management from Carnegie Mellon University.

Joshua New is a policy analyst at the Center for Data Innovation. He has a background in government affairs, policy, and communication. His research focuses on methods of promoting innovative and emerging technologies as a means of improving the economy and quality of life. New graduated from American University with degrees in C.L.E.G. (communication, legal institutions, economics, and government) and public communication.

ACKNOWLEDGEMENTS

The authors wish to thank Robert D. Atkinson and Alan McQuinn for providing input to this report. Any errors or omissions are the authors' alone.

ABOUT THE CENTER FOR DATA INNOVATION

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

contact: info@datainnovation.org

datainnovation.org