PREPARED STATEMENT FOR THE RECORD OF

INTEL CORPORATION

For the

UNITED STATES HOUSE ENERGY AND COMMERCE

SUBCOMMITTEE ON DIGITAL COMMERCE

AND CONSUMER PROTECTION

Hearing On

INTERNET OF THINGS LEGISLATION

MAY 22, 2018

Intel Corporation (Intel) respectfully submits this statement for the record in conjunction with the Energy and Commerce Committee Subcommittee on Digital Commerce and Consumer Protection hearing entitled, "Internet of Things Legislation."

Our statement focuses on the opportunity to unleash the enormous potential of the Internet of Things ("IoT") to positively impact the quality of life for Americans by enabling transformational economic and societal benefits across the consumer and industrial marketplace. The IoT already is enabling more efficient manufacturing, improved healthcare delivery, and new retail experiences, as well as increasingly smarter and more livable cities for American communities. By investing in this vast transformational potential of the IoT, pursuant to a clear national IoT strategy, U.S. policymakers can help ensure that the country's IoT technology evolves at the forefront of innovation, driving America's global competitiveness and growing our economy.

Witness: Dipti Vachani is Vice President of the Internet of Things Group and General Manager of the Platform Management and Customer Engineering organization at Intel Corporation. Her organization is responsible for delivering platform products that scale across IoT vertical segments, customer enablement, and optimizing products across the Internet of Things Group portfolio. Intel's IoT portfolio spans hardware, software, security and services across a wide range of market segments, including automotive and transportation, manufacturing, healthcare, smart video, retail, smart buildings, and smart cities. For more than 30 years, Intel has made significant investments, driven exciting innovations, and led activities across industries in order to foster standards and best practices, and supported what has evolved to become the IoT. At Intel, we like to say the IoT is an overnight transformation over thirty years in the making.

INTEL AND THE INTERNET OF THINGS

The Evolution of IoT at Intel

The evolution of IoT goes back more than 30 years at Intel, a leader in the space from the start. In 1972, Intel introduced the Intel 4004, the world's first commercially available microprocessor – an invention foundational to the "computer revolution." The late 1970s brought the Intel 8048, the world's first commercially available microcontroller, which integrated memory, peripherals and the microcontroller on a single chip. These microcontrollers fueled new business opportunities in a variety of markets. In 1981, IBM launched the IBM 5150, igniting the rapid-paced growth of the "personal" computer (PC) market segment. This first IBM PC ran on an Intel 8088 microprocessor and used Microsoft's MS-DOS operating system.

Initially, microprocessors were used for personal computing, leaving microcontrollers for 'use specific' or 'embedded' applications like factory controls. A critical shift occurred in the mid-1990s as customers began using Intel microprocessors in embedded market segments, bringing the power of computing to what had traditionally been based on microcontrollers. Intel began a concerted effort to support the unique attributes of "embedded" market segments, including

manufacturing life-cycle support for 7-10 years, extended operating temperatures, and utilizing real-time operating systems.

The early 2000s saw an unprecedented uptake in Internet usage as PC and mobile markets exploded. This "connectivity" trend wasn't limited to connecting people; embedded systems introduced in the 1990s were now simultaneously taking advantage of this powerful capability. Over the course of just a few years, industries worldwide were profiting from the scaling benefits of computing and networking, while and consumers enjoyed the benefits of connected PCs. In the late 2000s, "Machine to Machine" (M2M) emerged. M2M refers to technologies that allow both wireless and wired systems to communicate with other devices of the same type. Before M2M, people had to be physically located at the machine to analyze the data to make decisions for managing each machine. With the introduction of M2M, machines could now be managed remotely. All of these innovations, ranging from the datacenter to cloud computing to wireless communications to M2M, formed the basis of what is now widely known as the IoT. And Intel has been a leader in this technology evolution from the start.

Moore's Law, named after Intel co-founder Gordon E. Moore, is the business model that drives the semiconductor industry. It states the number of transistors in an integrated circuit doubles approximately every two years. In essence, the marketplace experiences a doubling of computing capability at approximately the same price every other year. This explosion of networked devices also began to represent another "law" of scaling, known as Metcalfe's Law. Metcalfe's Law states that the value of a telecommunications network is proportional to the square of the number of connected users of the system. This law enables the Network Effect, whereby the value of a product or service is dependent on the number of users. Together, Moore's Law and Metcalfe's Law demonstrate how the power of intelligent, connected devices can unleash innovation, leading to the creation of platforms for new applications and services.

Defining the IoT

The IoT is here, and already is transforming the way we live and work. The IoT offers massive potential for society and business to build a more connected, productive, and engaging world. At its core, the IoT is: "Things" (devices) securely connected through a network to the cloud (datacenter), from which data can be shared and analyzed to create value (solving problems or enabling new capabilities). The IoT enables us to connect "things" like phones, appliances, machinery, and cars to the Internet; share and analyze the data generated by these things; and extract meaningful and actionable insights.

These opportunities are extensive and exciting, with the ability to transform entire industries and our lives for the better. The IoT encompasses two major segments: Consumer IoT and Industrial IoT. The "Consumer IoT," which garners much of the attention in this space, connects devices like smart thermostats, household appliances, wearables, and smart phones. The "Industrial IoT," which is going to be the dominant market for IoT use cases with the most

significant GDP impact, connects devices in industrial environments like factory equipment, retail systems, security cameras, medical devices, and digital signs.[1]

Intel expects the IoT evolution will include three major phases:

- **Phase 1 - Connect the Unconnected:** Because IoT capabilities were built from legacy embedded businesses, all of those embedded devices needed to be able to communicate, share data, and stream information to the back end (data access layer).

- **Phase 2 (today) - Intelligent Interconnected Things:** Today we are in the era where everything is connected and "smart." This is fueled by the advances in machine learning, speech recognition, and artificial intelligence.

- **Phase 3 - Software Defined Autonomous:** In the not so distant future, complex systems will function freely and be able to make important decisions in real-time, and devices will learn from their environment and utilize that learning to improve performance.

Securing the IoT

Security is foundational to the IoT. Intel's IoT hardware and software are designed from the beginning with security, with the goal of delivering trusted data with a tight integration of hardware- and software-based security that starts where data is most resilient to attack. To do this, we build security into the transistors in our chips. We also build security into the software used in the "things," as well as the way in which data is moved from these things or devices to the cloud. In total, we believe reliance upon a hardware- and software-layered approach to security helps achieve the best results and helps minimize and compartmentalize threats when problems do arise. We fully realize safety and security are essential for the promise of the IoT to be realized. Therefore, while the nature of threats continue to evolve in frequency and potency, so do our innovations.

And the market for IoT security is maturing and growing rapidly. We are seeing a significant increase in the amount of investment in security not only by Intel, but across the IoT landscape. From 2017 to 2022, the IoT security market is expected to grow from $6.62 billion to $29.02 billion, at a Compound Annual Growth Rate of over 34 percent.[2] Notably, we are seeing more companies investing in hardware-based security mechanisms, rather than just software-based technologies that are vulnerable to hackers.

---

[1] National IoT Strategy Dialogue Report (Oct. 2017), https://www.itic.org/dotAsset/bdce6de4-8a00-49c5-a7a9-4dfb95609a76.pdf (attached as Appendix 1).

[2] Internet of Things Security Market Worth $29.02 Billion by 2022, Markets and Markets, https://www.marketsandmarkets.com/PressReleases/iot-security.asp.

Developing IoT Standards

In order to accelerate market adoption of secure IoT solutions that are interoperable and scalable across a global IoT ecosystem, Intel and others have come together to drive a voluntary, global, industry-led, open set of standards that enable cost-effective IoT technology solutions. In addition to partnering with entities like NIST (on voluntary frameworks for cyber-physical systems, cybersecurity, and networking) and IEEE (to build standards specifications to meet IoT use cases developed by IoT consortia), we have come together to create global IoT standards consortia to collaboratively create global IoT standards and overcome the technology barriers to accelerate IoT adoption.

Examples of leading global IoT standards consortia include:

- Open Fog Consortium – 57 members – Driving Interoperability that seamlessly bridges the "cloud to things" continuum.

- The Open Group – 111 members – Developing standards-based, open, secure, interoperable process control architecture.

- OPC Foundation – 515 members – Interoperability standard for the secure and reliable exchange of data in the industrial automation space and other industries.

- AVNU Alliance – 67 members – Creating interoperable ecosystem servicing the precise timing and low latency requirements of diverse applications (automotive, consumer, audio/video, industrial) using open standards through certification.

- Open Connectivity Foundation & IoTivity – 340+ members – Ensuring secure interoperability by delivering a standard communications platform and open source implementation for devices to communicate regardless of form factor, operating system, service provider, transport technology or ecosystem.

- 3rd Generation Partnership Project (3GPP) – 370+ members – Uniting multiple telecommunications standard development organizations and providing a stable environment to produce the Reports and Specifications that define cellular telecommunications network technologies such as 5G.

WHY CONGRESS SHOULD CARE: THE VAST SOCIETAL AND ECONOMIC IMPACT OF THE IOT

Why should policymakers care about investing in the IoT in America? By 2020, Gartner predicts that IoT technology will be in 95 percent of electronics for new product designs.[3] Therefore,

---

[3] Gartner's Top 10 Predictions for IT in 2018 and Beyond, Forbes (Oct. 2017), https://www.forbes.com/sites/louiscolumbus/2017/10/03/gartners-top-10-predictions-for-it-in-2018-and-beyond/#7a04a27f45bb.

the potential impact of IoT technology to address important societal and economic challenges in areas ranging from transportation, healthcare, smart cities, manufacturing, smart buildings, and industrial sectors is remarkable. It is critical that these IoT benefits are realized in this nation in a way that enables the U.S. to not only keep pace with, but stay at the forefront of, global innovation.

These transformational societal and economic benefits that will flow from the broad deployment of IoT technology is what energizes our team at Intel, and the SMART IOT Act is a welcome indication that this enthusiasm is matched by leaders in Congress. Indeed, the SMART IoT Act will create the foundational work for a national IoT strategy that prioritizes IoT growth in the U.S. and investment in technologies that can accelerate these benefits for America's communities and businesses.

Massive Economic and Societal Impact

The new markets and services generated by the IoT will add trillions of dollars to the global economy. Accenture estimates that the IoT could add $14.2 trillion to the worldwide economy by 2020.[4] Of this, $6 trillion will be spent on IoT solutions between 2015 and 2020, according to PwC.[5] And Gartner forecasts that the use of connected "things" will reach 20.4 billion globally by 2020.[6]

Countries are racing to lead in this highly competitive IoT race because they know that their communities and industries can be positively transformed by the IoT, as these technologies help solve societal challenges, while making businesses more effective and responsive, and adding new sources of revenue. The U.S. must position itself to lead in this transformational technology evolution. A national IoT study and recommendations to advance the IoT in the U.S. as set forth in the SMART IOT Act – lay the groundwork for a national IoT strategy – that will set the nation on the path to achieve this leadership goal.

Here are a just a handful of IoT use cases which Intel has deployed with our partners, demonstrating the positive impact that the IoT already is having on our lives and communities:

Use Case #1: Smart Healthcare (Texas Children's Hospital)

IoT applications in the healthcare sector are transforming and saving lives every day. For example, using IoT solutions, nearly 5 million patients' healthcare conditions were remotely monitored across the globe in 2015, representing a 51 percent increase from the previous year.

---

[4] 2017 Roundup of Internet of Things Forecasts, Forbes (Dec. 2017), https://www.forbes.com/sites/louiscolumbus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/#67cd37561480.

[5] *Id*.

[6] State of the Internet of Things, Verizon (2017), https://www.verizon.com/about/sites/default/files/Verizon-2017-State-of-the-Market-IoT-Report.pdf.

That number is expected to continue its upward trajectory, as remote healthcare services provide essential benefits to patients, while helping bring down associated health care costs.

Yet, currently, much of the data from patient monitoring devices is "siloed" and proprietary, and therefore underutilized. And with downstream systems not designed to manage or transform physiologic data, healthcare teams cannot effectively use data to optimize care delivery for individual patients or predict events. To tackle this challenge, new FDA-cleared IoT solution Sickbay – by Intel Solutions Alliance Member Medical Informatics Corporation, Intel and Dell – enables real-time, data driven medicine and patient-centered healthcare. The Sickbay IoT platform continuously captures patient data from any medical device or system and transforms that data into web-based clinical applications that make the data actionable. This actionable intelligence enables health care teams to make better and faster decisions and predict patient health deterioration before it occurs to save lives. Sickbay already is implemented at six healthcare institutions, including Texas Children's Hospital, which pioneered the technology that allows for viewing of real-time data from cardiac monitors and vents. Texas Children's Hospital used Sickbay to collect data on 302 beds over 4.5 years, which included 2.1 million patients.

Use Case #2: Smart Cities (Global)

The World Health Organization estimates that 92 percent of the world's population does not have access to clean air, and Bosch states reports that 3.2 million deaths occur annually due to air pollution.[7] This figure underscores a massive global societal and economic challenge. In fact, the World Bank Estimates that, in 2013, air pollution was responsible for $225 billion in lost productivity. Through air quality monitoring systems, such as those being deployed through Intel's IoT partnership with Bosch, we are addressing this challenge. The Intel & Bosch-developed IoT-powered pollution monitor systems provide intelligent data and enable real-time analysis of ambient air pollution. This Intel-powered IoT solution is being utilized by governments and traffic authorities across the globe to improve air quality in the most congested urban areas like Pune, India (a sprawling city of over 3.115 million in 94.15 mi²); by factory owners to track emissions and provide safety checks for workers; by worksite managers at construction sites to provide early warning signals and improve efficiency and work conditions; and in communities around the world to provide residents with air quality warnings and recommended times for fitness activities to lower health incidents from air pollution.

Use Case #3: Smart Transportation (San Diego, CA)

Traffic congestion presents a number of problems for communities. IoT traffic management can alleviate the time spent in traffic jams and reduce drive times, thus improving the quality of life for drivers and passengers, as well as reducing the economic losses which arise from this wasted time in traffic. IoT traffic management solutions also can reduce air pollution by smoothing traffic flow, reducing idling times, and improving traffic monitoring activities.

---

[7] Bosch (visited May 18, 2018), http://www.boschclimo.com/.

For example, Intel, together with Current by GE and AT&T, are providing IoT technology built into street lights. These unique intelligent nodes are embedded with multiple sensors that can be used to collect data related to air quality, weather, vibration, noise and lighting. The City of San Diego has the largest urban sensor project in the world. This technology has allowed for the city to reduce energy consumption and improve the quality of life for its residents. IoT initiatives like this can help to further address the problems of sound levels and better respond to weather conditions like rain, flooding, snow, ice, and other situations. IoT can even be used to deal with other challenges such as mapping health patterns and addressing crime trends.

Moreover, autonomous vehicles will have an enormous impact in increasing mobility for our aging and disabled populations. The number of U.S. residents age 70 and older is projected to increase to 53.7 million in 2030, compared to 30.9 million just 4 years ago. Approximately 16 million people over the age of 65 live in communities where public transportation is poor or non-existent. With the advent of autonomous vehicles, disabled and physically-challenged individuals will have the opportunity to move and travel more easily than ever before.

Use Case #4: Smart Buildings (New York City)

The integration of Intel IoT technology with sensors and building automation systems, such as heating and air conditioning, allows for the identification of opportunities in real-time to reduce energy costs. In conjunction with Intel, Rudin Management, a large, commercial real estate company in New York City, deployed Intel's Smart Building IoT solution to better manage its utility consumption. This IoT deployment saved Rudin $1.8 million in just one building over three years, and reduced electric consumption by nine percent. And this is only one building. Consider the potential IoT impact for the over 5 million commercial buildings and industrial facilities in America, with a current combined annual energy cost of more than $202 billion.

U.S. GLOBAL LEADERSHIP

It has been Intel's strong recommendation to see the U.S. government overtly adopt a more proactive national strategy when it comes to harnessing the economic and societal benefits of the IoT. In order to truly take a global leadership role, the U.S. must first declare the IoT a national priority for innovation, investment and competitiveness. We strongly applaud the Committee for its bipartisan effort to set America on the path to make this vision a reality. The Committee's work in drafting the SMART IOT Act creates the opportunity for the U.S. to identify the state of the IoT in America, and begin to do the foundational work to develop a meaningful and comprehensive national IoT strategy based on the Department of Commerce's recommendations.

Therefore, Intel supports the concept of requiring a national study to survey the IoT industry, as well as agency activity and resources. We also strongly support the requirement that the IoT report is submitted to Congress with recommendations on how best to promote adoption of the IoT to grow the U.S. economy. For policymakers who are responsible for ensuring that the

IoT ecosystem reaches its full economic and societal potential in America, interaction between key agencies and the Congress is both important and appropriate.

Intel Recommendations for the SMART IOT Act

<u>IoT Terminology and Definition</u>. We respectfully encourage the Committee to:

- Use the term "IoT device" in place of "internet-connected device." The latter is a very broad term, including devices that are not IoT.

- Include a robust definition of the IoT that is aligned with the definition in the recently unveiled National IoT Strategy Dialogue Report (attached as Appendix 1),[8] which was widely supported by the Information Technology Industry Council, the U.S. Chamber of Commerce, and the Semiconductor Industry Association. This definition is non-proprietary and is neutral with respect to technologies, applications and deployments. It also broadly defines the IoT to include consumer and industrial IOT sectors, to reflect the reality of the IoT marketplace. Contrary to popular belief, the IoT is not primarily about consumer applications. Rather, industrial, smart city, and connected health applications will account for 70 percent of the IoT market.[9] We recommend that the legislation contemplate both consumer and industrial IoT applications by adopting the non-proprietary and neutral definition in the National IoT Strategy Dialogue Report.

<u>Additional Guidance to the Department of Commerce</u>. We see opportunity in this legislation to identify aspects where Department of Commerce recommendations would be highly impactful in laying the groundwork for a meaningful national IoT strategy. To this end, we encourage the Committee to seek specific recommendations from the Department including:

- How to prioritize the development of a national IoT strategy that will grow the American economy and drive global competitiveness;

- Incentives for federal departments and agencies to adopt interoperable, scalable and secure (multi-layer hardware and software) IoT technologies for data-driven solutions to advance their federal missions, including smart infrastructure solutions;

- How to ensure the federal government does not adopt new regulations that are duplicative to existing or already underway industry-led-standards, best practices and regulations that cover IoT technologies;

---

[8] National IoT Strategy Dialogue Report (Oct. 2017), https://www.itic.org/dotAsset/bdce6de4-8a00-49c5-a7a9-4dfb95609a76.pdf (attached as Appendix 1).
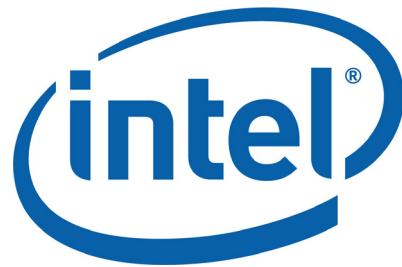
[9] 2017 Roundup of Internet of Things Forecasts, Forbes (Dec. 2017), https://www.forbes.com/sites/louiscolumbus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/#67cd37561480

- How federal departments and agencies can best support and promote leading global, industry-led IoT standards efforts, and engage as a key participant where appropriate;

- How to coordinate across federal departments and agencies to prevent inconsistent, duplicative, or unnecessary new IoT regulations, as well as to avoid creating barriers to integration of devices, data, and services across industry sectors;

- Criteria for the federal government to invest in IoT public-private partnerships, research and testbeds, such as those being driven by leading global industry consortia; and

- How the federal government can best advocate internationally for foreign counterparts to participate in and support global, industry-led IoT standardization activities, protect the free flow of data across borders necessary for a thriving global IoT marketplace, and prevent harmful policies against U.S. companies in the application of laws and regulations impacting IoT technologies.

Thank you for the opportunity to share Intel's thoughts on the IoT marketplace and the SMART IOT Act. We look forward to working with the Committee to see this bipartisan legislation enacted into law as a productive first step toward a National IoT Strategy. With these efforts, Congress will set America on the path to realize the vast economic and societal benefits of the IoT, and ensure U.S. leadership in this globally competitive marketplace that will define the 21st century.

APPENDIX 1 – National IoT Strategy Dialogue Report (Oct. 2017)

National IOT Strategy Dialogue

intel®

SAMSUNG

ITI

S I A SEMICONDUCTOR INDUSTRY ASSOCIATION

C_TEC
U.S. Chamber of Commerce
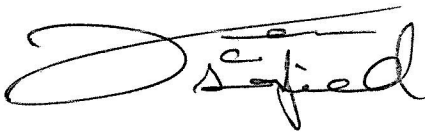Technology Engagement Center

INTRODUCTION

The U.S. technology sector is the envy of the world. Following the advent of the Internet, the United States has led every major technological revolution in no small part due to the innovative policy approach of the federal government. We are at the next major technological turning point as we witness the widespread proliferation of the Internet of Things (IoT). To lead the world and fully realize the potential of all the economic, societal, and innovative benefits the IoT will deliver, the United States must have a national strategy to promote investment, development, and widespread utilization of the IoT. To help guide this goal, we are pleased to unveil this report, which has been developed through collaboration and discussion among leading industry, academic, governmental, and other stakeholders in the IoT. With the adoption of these strategic policy recommendations, we believe the United States will be the unquestioned leader in the IoT.

I want to thank all those who participated in the National IoT Strategy Dialogue (NISD) discussions and development of this report. In particular, I want to thank NISD Co-Chair Marjorie Dickman and Intel Corporation for the leadership and strategic vision in the development of this report. As Intel's global expert on IoT policy, her sage guidance and time commitment were invaluable. Further, I want to thank Samsung and NISD Co-Chair John Godfrey for providing the platform to launch this important initiative, together with Intel and the Information Technology Industry Council (ITI), at their 2016 IoT event in Washington. Lastly, numerous companies and associations participated in NISD and contributed to the ideas in this report. In particular, we want to thank the Semiconductor Industry Association (SIA) and the U.S. Chamber of Commerce Technology Engagement Center for their partnership in unveiling this report.

Fully harnessing the transformative nature of the IoT is a tremendous opportunity for the United States. We encourage the U.S. government to act on this report's strategic policy recommendations – starting with adopting a National IoT Strategy.

Sincerely,

Dean C. Garfield
President and CEO
Information Technology Industry Council

In June 2016, Intel, Samsung, and the Informational Technology Industry Council (ITI) launched the [National IoT Strategy Dialogue](#) (NISD), an initiative to convene industry partners and organizations to collaboratively develop strategic recommendations for U.S. policymakers on the Internet of Things (IoT). The launch of this IoT initiative answered the call of a chorus of technology leaders seeking a forum to proactively coordinate and drive industry's trusted advisor role in helping the United States to fully realize the vast benefits of IoT for economic and societal good.

NISD has grown significantly since its launch a year ago. In addition to broad industry engagement, we have reached out extensively to a wide range of government stakeholders engaged in IoT policy for their input. Government participants in this collaborative effort include the Department of Commerce (DOC), Department of Health and Human Services (HHS), Department of Homeland Security (DHS), National Institute of Standards and Technology (NIST), White House Office of Science and Technology Policy (OSTP), National Telecommunications Information Administration (NTIA), and Food and Drug Administration (FDA). Industry and other external participants include ITI, the Semiconductor Industry Association (SIA), CTIA the Wireless Association, Advanced Medical Technology Association (AdvaMed), World Bank, and Information Technology and Innovation Foundation (ITIF). It became clear from these discussions among government and industry experts that a National IoT Strategy is a much-needed first step to drive U.S. IoT leadership, and some of the most important elements of a national strategy will require affirmative action from Congress and the administration.

This breadth of industry participation is indicative of the fact that the expansive technology sector is critical to the IoT's success. IoT solutions consist of hardware, software, security, and services across a wide range of market segments, including automotive and transportation, energy, healthcare, smart manufacturing, retail, smart buildings, and smart homes. Not since the advent of the Internet has there been such a technological shift that presents an opportunity for U.S. consumers, businesses, government, and the economy at large.

Among its many benefits, the IoT will enable increased safety in our communities, offer consumers significant improvements in their daily lives, make government and business more efficient and productive, and create new job opportunities by stimulating economic growth in all sectors of the economy, similar to prior technology evolutions that have been critical to America's leadership and long-term growth. The IoT will fundamentally transform our lives for the better, bringing us a society and environment where everything is smarter and more connected, from smart cities and smart cars, to intelligent wind farms, precision agriculture, and next generation health care.

What is at stake at this moment is whether the United States will be able to win the global race to test, develop, and deploy these beneficial technologies. With these vast economic and societal benefits in mind, NISD was launched with the goal of collaboratively working with policymakers to develop a much needed strategic roadmap to position the United States as the global IoT leader now and for decades to come. To this end, we are focusing on the advancement of pro-innovation public policies, market incentives, and regulatory frameworks, as well as government use and adoption of IoT to showcase America's global leadership.

Our strategic recommendations seek to lay the foundation to drive scalable U.S. IoT infrastructure investment; facilitate interoperability; foster security; promote voluntary, industry-led, global consensus-based IoT standards and best practices; and leverage public-private partnerships (PPPs).

Why is a strategic plan necessary for America? Because U.S. IoT success and leadership will not occur without appropriate planning nor will it happen in a policy vacuum. The positive social and economic potential of the IoT is massive and capturing the lead in this area appeals to every developed nation. It is estimated that IoT will produce a total economic impact of $3.9 to $11 trillion per year globally by 2025, equivalent to 11 percent of the world economy.[1] This vast economic impact already has led many other countries to promote the adoption of IoT across multiple sectors; the United States must not just follow suit, but rather proactively chart a strategic course to sustainably surpass these countries if we want a competitive advantage in the future of manufacturing, transportation, agriculture, energy, finance, healthcare, and other key sectors of high gross domestic product (GDP) impact that are being rapidly transformed by the IoT.

This report provides strategic recommendations for the U.S. government to work with industry to drive American IoT leadership. We are eager to support Congress and the Trump Administration in taking these steps to create a policy and regulatory environment that will attract unparalleled private sector investment and innovation in the IoT, thereby modernizing the nation's infrastructure, improving American manufacturing, and growing GDP. We thank all of the individuals, organizations, and government entities that collaborated with us throughout this process and look forward to collaboratively advancing these strategic recommendations and achieving U.S. IoT leadership.

Sincerely,

Marjorie Dickman, Co-Chair, National IoT Strategy Dialogue
Global Director & Associate General Counsel, Internet of Things & Automated Driving Policy
Intel Corporation

John Godfrey, Co-Chair, National IoT Strategy Dialogue
Senior Vice President, Public Policy, Office of U.S. Public Affairs (USPA)
Samsung Electronics America

Vince Jesaitis
Vice President, Government Affairs
Information Technology Industry Council

EXECUTIVE SUMMARY

This report makes the following strategic recommendations for Congress and the Trump Administration to establish America as the leader in the Internet of Things (IoT):

1. **Prerequisite – IoT Definition:** Congress and the administration should adopt this broad-based IoT definition as an initial level-set for any future policymaking regarding the IoT:

- The IoT consists of "things" (devices) connected through a network to the cloud (datacenter) from which data can be shared and analyzed to create value (solve problems or enable new capabilities). The IoT enables us to connect "things" like phones, appliances, machinery, and cars to the Internet, share and analyze the data generated by these "things," and extract meaningful insights; those insights create new opportunities, help solve problems, and implement solutions in the physical world.

2. **Prioritization of a National IoT Strategy:** Congress should promptly enact, and the president sign into law, the bipartisan *Developing Innovation and Growing the Internet of Things (DIGIT) Act* (S. 88/H.R. 686) to make a National IoT Strategy a priority and position America to lead the global IoT future.

3. **Ensuring Consistent IoT Standards and Rules at the Federal Level and Internationally:**

- Federal agencies should not adopt new regulations where existing standards, best practices, and regulations exist, or are underway that would include IoT technology, or where the costs of new regulations have not been offset by the reform of previous regulations.

- Based upon existing authority, or the grant of new authority where necessary, the White House and Congress should direct federal agencies to support and promote leading global, industry-led IoT standards efforts, and the U.S. government should engage as a key participant where appropriate.

- The Department of Commerce (DOC) should coordinate across federal agencies to prevent inconsistent, duplicative, or unnecessary IoT regulations, as well as to avoid creating barriers to integration of devices, data, and services across industry sectors.

- The federal government should advocate internationally for our foreign counterparts to participate in and support global, industry-led IoT standardization activities, protect the free flow of data across borders, and prevent discrimination against U.S. companies in the application of laws and regulations.

4. Commitment to Security of the IoT:

- Congress and the administration should incentivize multi-layered protection of IoT solutions using hardware- and software-integrated security. Any legislation providing funding for IoT solutions or smart technology should include this in the eligibility criteria for federal funding.

- Congress and the administration should encourage flexible federal policies that promote ongoing innovation and best practices for hardware- and software-integrated security.

- It must be a federal priority to continue to build upon and invest in cybersecurity multi-stakeholder efforts, leveraging the best of our public and private sector experts and resources to constantly improve the security of the IoT and other technologies. The federal government should continue to initiate and support multi-stakeholder activities and working groups, collaborate with industry to understand evolving threats, and develop best practices for IoT security and data privacy. DOC and its agencies, such as the National Institute of Standards and Technology (NIST) and the National Telecommunications Information Administration (NTIA), as well as the Department of Homeland Security (DHS), are the appropriate entities to continue to lead such efforts.

- Congress should direct the Federal Trade Commission (FTC), Small Business Administration (SBA), and Federal Communications Commission (FCC) – with input from industry – to develop complementary cybersecurity hygiene education and awareness outreach initiatives for consumers and small businesses. These initiatives should focus on security tools and best practices for Internet-connected things to help better secure devices and wireless networks from intrusions.

- Congress should direct federal departments and agencies in the procurement process to prioritize secure, interoperable, and scalable IoT solutions for federal assets based on voluntary, industry-led, consensus-based, global standards. Secure solutions, with multi-layered hardware- and software-level capabilities, must be a government procurement requirement for both IoT and non-IoT solutions to protect the nation.

5. Prioritization of Smart Infrastructure Solutions: Congress and the administration should make it a federal priority in infrastructure legislation to both fund and incentivize smart, data-driven IoT solutions that advance federal agency missions.

- To modernize the nation's transportation system, infrastructure legislation should fund and incentivize smart IoT solutions on a technology-neutral basis in a way that boosts market-driven investment, including investing in technologies that will accelerate the safe deployment of automated vehicles.

- Infrastructure legislation should promote the deployment of key foundational technologies like 5G mobile broadband networks that will serve as the core architecture for the IoT. Congress should also direct the NTIA and FCC to allocate commercial licensed and unlicensed spectrum in a technology-neutral and service-neutral way across a wide range of frequencies to address the breadth of IoT use cases today and into the future.

- Infrastructure legislation should fund and incentivize smart government building technologies using data-driven IoT solutions to improve building automation in new construction, renovation, and retrofit of both civilian and military buildings.

6. Invest in IoT Public-Private Partnerships (PPPs), Research, and Testbeds: To ensure U.S. global IoT leadership, the federal government should invest in IoT PPPs, research, and testbeds, such as those being driven by leading global industry consortia like the Industrial Internet Consortium (IIC), Open Connectivity Foundation (OCF), and OpenFog Consortium (OpenFog).

STRATEGIC RECOMMENDATIONS

The following is a set of strategic recommendations for Congress and the Trump Administration to set America on a path of U.S. Internet of Things (IoT) leadership for decades to come. We provide a blueprint of specific and timely steps to enable the development and deployment of the IoT in the United States, thus, enabling the nation's global competitiveness across numerous key market sectors. Some of our recommendations require direct investment of resources, while others entail a commitment by the United States to lead the continuous IoT technology evolution that is transforming the global economy. In the aggregate, these strategic recommendations will deliver national alignment and efficiency across an innovation ecosystem to ensure that America realizes the vast economic and societal benefits of the IoT.

1. Prerequisite: IoT Definition

The world is in the midst of a dramatic transformation from isolated systems to Internet-enabled devices that can network and communicate with each other and the cloud. Commonly referred to as the IoT, this new reality is being driven by the convergence of increasingly connected devices, compute and data economics, and the proliferation and acceleration of cloud and big data analytics. This shift in technology is generating unprecedented opportunities for the U.S. public and private sectors to develop new services, enhance productivity and efficiency, improve real-time decision-making, solve critical societal problems, and develop new and innovative user experiences.[2]

In recent years, we have seen many proprietary definitions of the IoT that tend to focus on specific business interests. However, it is important to have an agreed upon definition of the IoT that comprehends the fullest breadth of IoT applications. At its simplest, the IoT consists of "things" (devices) connected through a network to the cloud (datacenter) from which data can be shared and analyzed to create value (solve problems or enable new capabilities). The IoT enables us to connect "things" like phones, appliances, machinery, and cars to the Internet, share and analyze the data generated by these "things," and extract meaningful insights; those insights create new opportunities, help solve problems, and implement solutions in the physical world.

The IoT encompasses two major segments: Consumer IoT and Industrial IoT. The Consumer IoT connects devices like smart TVs, household appliances, gaming consoles, wearables, and smart phones. The Industrial IoT connects devices in industrial environments like factory equipment, retail systems, medical devices, and digital signs.

<u>Recommendation:</u> **Congress and the administration should adopt this broad-based IoT definition as an initial level-set for any future policymaking regarding the IoT.**

2. Prioritization of a National IoT Strategy

It is imperative that the U.S. federal government declares the IoT a strategic national priority in 2017. This effort must begin with a simple, yet profound, declaration of a national IoT vision.

The federal government must declare IoT investment, innovation, and competitiveness a U.S. priority and institute an expedient process and timeline for the development of a National IoT Strategy in conjunction with the private sector. This strategy must be built with a strong commitment to scalability, interoperability, and security, as well as with sufficient flexibility to address the inevitable reality that IoT technologies and their applications will continually evolve.

Success in developing and implementing a meaningful national IoT strategy will require leadership at the highest levels of the U.S. government in partnership with the private sector. This strong leadership is needed to take the strategic steps necessary to facilitate policies that accelerate development and deployment of the IoT in the United States, and ensure that U.S. government, businesses, and consumers can leverage the wide range of benefits the IoT offers. Without a clear strategic vision for enabling and adopting IoT solutions across many key market sectors, the United States is certain to fall behind as other countries reap the vast economic and societal benefits of these technologies, along with the benefits that accrue from creating and owning the expertise behind the IoT. However, by implementing a clear strategic plan with a series of impactful steps, the United States can and will lead the world – and drive GDP – for decades to come.

The bipartisan *Developing Innovation and Growing the Internet of Things (DIGIT) Act*, (S. 88/H.R. 686) sets forth a collaborative process for developing a National IoT Strategy. Specifically, it would require the federal government, under the leadership of the Secretary of Commerce, to convene a working group of federal entities that would consult with private sector stakeholders to provide recommendations to Congress on how to plan for and encourage the proliferation of the IoT in the United States. This joint government-industry process would produce a unified vision and critical first step toward development and implementation of America's National IoT Strategy.

<u>Recommendation:</u> **Congress should promptly enact, and the president sign into law, the bipartisan DIGIT Act to make a National IoT Strategy a priority and to position America to lead the global IoT future.**

3. Ensuring Consistent IoT Standards and Rules at the Federal Level and Internationally

As emphasized in the Department of Commerce's (DOC) IoT green paper,[4] voluntary, consensus-based, global standards developed through open participation efforts will drive interoperability, scale, and IoT investment. Depending upon existing authorities, the White House and Congress should work to direct federal agencies to support and promote such global, industry-led IoT standards efforts – many of which have been underway for years.

The U.S. government should support industry in continuing to lead IoT standards development and engage as a key participant where appropriate. Government should avoid adopting new regulations where existing standards, industry voluntary practices, and regulations exist, or are underway, that would otherwise encompass IoT technology. Moreover, consistent with the intent of Executive Orders 13771 and 13777,[5] federal agencies should not adopt new regulations where the costs have not been offset by the reform of previous regulations.

<u>Recommendation:</u> **Federal agencies should not adopt new regulations where existing standards, best practices, and regulations exist, or are underway that would include IoT technology, or where the costs of new regulations have not been offset by the reform of previous regulations.**

Some leading examples of global standards efforts with broad private sector membership include the Industrial Internet Consortium (IIC), Open Connectivity Foundation (OCF), OpenFog Consortium (OpenFog), and GSMA's initiative on IoT device self-certification:[6]

- **IIC:** Launched in March 2014, the IIC is a global, member-supported organization that promotes the accelerated growth of the Industrial IoT by coordinating ecosystem initiatives to securely connect, control, and integrate assets and systems of assets with people, processes, and data using common architectures, interoperability, and open standards to deliver transformational business and societal outcomes across industries and public infrastructure.[7]

- **OCF:** Launched in February 2016 to bring together the competing Open Internet Consortium and AllSeen Alliance, the OCF is defining connectivity requirements to improve interoperability between the billions of devices making up the IoT. OCF will deliver a specification, an open source implementation, and a certification program ensuring interoperability regardless of manufacturer, form factor, operating system, service provider, or physical transport technology.[8]

- **OpenFog:** Launched in November 2015, Open Fog is driving industry and academic leadership in fog computing architecture, testbed development, and a variety of interoperability and composability deliverables that seamlessly leverage cloud and edge architectures to enable end-to-end IoT scenarios.[9]

- **GSMA:** The embedded SIM certification initiative,[10] launched in November 2010, will provide a mechanism for the remote provisioning and management of machine to machine connections in a more efficient and secure manner through the use of tested embedded subscriber identity modules.

Industry-led, global standards efforts with respect to security (see pg. 14), interoperability, scalability, and other key tenets will accelerate IoT adoption, drive competition, and enable cost-effective introduction of new technologies in a scalable way. Government adoption of IoT solutions should follow and adopt industry-led standards, thereby, ensuring that government-deployed solutions will benefit from the scope and scale of the broader IoT and not be relegated to a proprietary or isolated silo.

Recommendation: **Based upon existing authority, or the grant of new authority where necessary, the White House and Congress should direct federal agencies to support and promote leading global, industry-led IoT standards efforts, and the U.S. government should engage as a key participant where appropriate.**

In addition to ensuring that each U.S. federal agency supports the international, industry-led standards development process for the IoT within its own sector, government must ensure coordination across these agencies to prevent inconsistent, duplicative, or unnecessary IoT regulations. Indeed, one of the greatest benefits of the IoT is its power to aggregate data intelligence from devices and systems from diverse sources, crossing traditional industry boundaries. For example, to improve traffic congestion, real-time data and rich insights about transportation patterns can be gleaned from automobiles, street lights, and traffic sensors along roadways. Similarly, to improve public health, data can come from wearables, connected medical devices, environmental sensors, doctors' offices, and even restaurants. The interconnection of the data and devices across these boundaries is essential for IoT innovation and growth.

These changes in traditional industry boundaries can blur historical regulatory distinctions, and there is a significant risk that fragmented regulatory approaches across the government could prevent these and other IoT benefits from being realized. If federal regulatory agencies implement different, incompatible technical standards, or impose different, inflexible security or privacy obligations, the consequences will include the fragmentation of the IoT, barriers to scale, and lost opportunities for the United States. For this reason, coordination across government agencies is essential to prevent a patchwork of inconsistent policies which could disrupt the IoT's transformative potential.

As discussed above, agencies should avoid imposing new regulations where existing standards, voluntary industry standards and best practices, or government regulations already address the devices, services, or sectors that make up the IoT. Federal agencies should continue to partner with the private sector on multi-stakeholder efforts and global industry standards organizations (as discussed below) rather than defaulting to the imposition of new government regulations. Furthermore, where regulations are deemed necessary based on facts and market failure (not hypotheticals), agencies should adopt consistent, flexible approaches. DOC should lead this effort with respect to the horizontal, industry-crossing aspects of the IoT instead of each agency developing its own unique and possibly inconsistent guidelines or regulations.
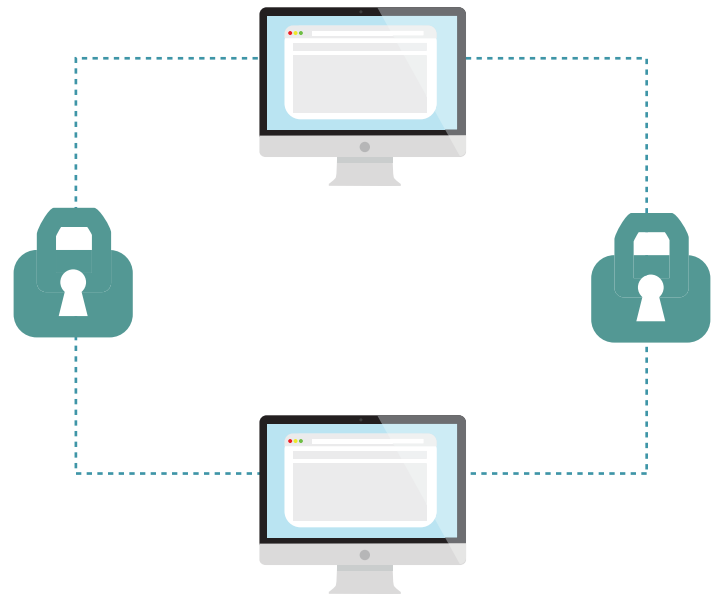
Recommendation: DOC should coordinate across federal agencies to prevent inconsistent, duplicative, or unnecessary IoT regulations, as well as to avoid creating barriers to integration of devices, data, and services across industry sectors.

But ensuring consistency in federal agency policies is not sufficient; the U.S. government must also strongly encourage our foreign counterparts to participate in and support global, industry-led IoT standardization activities. Many of these Standards-Setting Organizations (SSOs) have formed technical study groups to ascertain whether, and to what extent, additional standards development may be necessary to advance the IoT. These SSOs attract experts and participation from across the globe, as well as across various industry sectors that will be impacted by and benefit from the IoT.

It is critical to the success of the IoT that the U.S. government advocate internationally for other governments to support these SSOs' multi-stakeholder processes and participate when appropriate. When other countries insist on pursuing non-SSO processes the U.S. government should strongly encourage them to allow full industry participation and to look to existing or pending global standards before undertaking any activity that may be duplicative of, or conflict with, global, industry-led IoT standards. We also strongly encourage the U.S. government to include in its international advocacy a common definition of the IoT (see pg. 8) and a statement of policy that will accelerate development and adoption of IoT technologies (consistent with the recommendations in this report).

For example, as the Department of Homeland Security (DHS) concluded in its Strategic Principles for Securing the Internet of Things report, "IoT is part of a global ecosystem, and other countries and international organizations are beginning to evaluate many of the[] same security considerations. It is important that IoT-related activities not splinter into inconsistent sets of standards or rules. As DHS becomes increasingly focused on IoT efforts, we must engage with our international partners and the private sector to support the development of international standards and ensure they align with our commitment to fostering innovation and promoting security."[11]

Furthermore, in today's globally connected world, international commerce cannot function without data freely flowing across borders. The free movement of data allows U.S. companies of all sizes and in all industries to bring new innovations to global markets – driving investment, growth, and job creation in America. Cross-border data flows particularly enable small- and medium-sized enterprises (SMEs) to compete in the global economy, which is essential to maximizing the benefits of the IoT. Unfortunately, some governments around the world are considering, or are already imposing, digital trade barriers. American companies have the most to lose if these barriers are not addressed.

Therefore, in order to support the growth of the IoT and the continued competitiveness of the American economy, the federal government should aggressively protect cross-border data flows through trade agreements and other enforceable mechanisms with trading partners. Specifically, these agreements must include binding provisions protecting cross-border data flows and preventing data localization requirements, which mandate U.S. companies to store, process, or handle their data within the local country's borders. They also must include provisions on transparency, predictability, and nondiscrimination in the application of laws and regulations, on trade in goods and services, and on protection of intellectual property. The U.S. government should leverage these commitments to respond to unfavorable trade policies that could undermine existing rights and obligations of U.S. companies, and which would discourage U.S. investment and threaten scalability of the IoT.

Recommendation: The federal government should advocate internationally for our foreign counterparts to participate in and support global, industry-led IoT standardization activities, protect the free flow of data across borders, and prevent discrimination against U.S. companies in the application of laws and regulations.

4. Commitment to Security of the IoT

A strong commitment to the vast benefits of the IoT must be accompanied by an equally strong commitment to ensuring the security of the IoT ecosystem. As advocates of the expansive benefits of the IoT, we are equally convinced that an appropriate federal policy framework prioritizing joint industry-government, multi-stakeholder initiatives for IoT security is a foundational component of our nation's IoT success. Federal policies must promote security for IoT solutions from end-to-end (device-to-network-to-cloud), and include both legacy systems and new deployments.

With billions of connected devices generating more than 44 zettabytes of data by 2020,[12] security of this data and the networks and systems they transit will be critical to enable scale of IoT deployments. That is why we emphasize the importance of having security designed into the IoT systems from the outset. Secure systems, including all connected things that generate the data, and send the data through the communications network to the cloud and back, are critical to enabling trusted data exchange and scale, thereby unlocking the full potential of the IoT.

Numerous government-industry collaborative efforts have considered how to address the question of IoT security, and they have come to similar key conclusions. There is general agreement on five important fronts:

- Multi-layered protection using hardware- and software-integrated security at the outset that, at a minimum, protects storage, device identification and authentication, software authentication, and enables a trusted execution environment is critical;

- Federal policies must be sufficiently flexible for industry to innovate and address the ever-changing threat landscape;

- Government-convened, multi-stakeholder processes – bringing together security experts across government, industry, and academia – have a proven track record of success and should be continually honed and replicated;

- As new technologies develop and threat landscapes evolve, ongoing and evolving small business and consumer education on how to appropriately secure connected devices is critical; and

- Improved federal procurement requirements for multi-layered hardware- and software-integrated cybersecurity solutions must be a priority.

Integration of Security at the Outset: Industry agrees on the importance of integrating security into the hardware and the software components of IoT solutions from the beginning of the design process – from the smallest microcontroller (MCU) at the edge of the network to the most advanced server central processing unit (CPU) in the data center, and all gateways and devices in between. Specifically, multi-layered protection using hardware- and software-integrated security that, at a minimum, protects storage, device identification and authentication, software authentication, and enables a trusted execution environment is critical.

These hardware- and software-level security capabilities will create redundancies, which prevent intrusions and enable robust, secure, trusted end-to-end IoT solutions. Industry appreciates that we must deliver and evoke consumer trust through these hardened security solutions in order to motivate adoption and participation in the IoT marketplace.

Recommendation: Congress and the administration should incentivize multi-layered protection of IoT solutions using hardware- and software-integrated security. Any legislation providing funding for IoT solutions or smart technology should include this in the eligibility criteria for federal funding.

Flexibility of Federal Policies: There is a vast array of technologies that are, and will be, deployed in the global marketplace and the IoT will be one subset in that expanse of marketplace technologies. Accordingly, it is critical that security is viewed in a comprehensive manner rather than forcing one subset of the ever-changing technology landscape in a regulatory silo targeted at IoT alone. Indeed, while security is critical for IoT technologies – as it is for all current and future technologies – IoT-specific security legislation or regulation is not the answer.

Security is a continuous process of risk management that is an ongoing and evolving challenge for all technologies, including the IoT. Thus, it is imperative for government to tread carefully in its policy response to any cyberattack. There is no single "silver bullet" in risk management and mitigation. Reflexive or prescriptive legislative or regulatory solutions are not the right mechanism to address complex hardware and software engineering challenges. Nor are technology mandates prescribing a specific security solution, which will become quickly outdated as technology advances. For this reason there is broad agreement that in order to be effective, federal policies must focus on best-known methods and be sufficiently flexible to address new vulnerabilities in the constantly evolving threat landscape, whether with respect to the IoT or other technologies.

These policies must focus on the desired outcome (multi-layered hardware and software security) rather than attempting to specify the technologies or techniques that must be used. Therefore, in order to best enable secure solutions, government must avoid technology mandates that require a specific technology solution as they will quickly become obsolete and can have the potential (and unintended consequence) of increasing susceptibility to new cyberattacks.

Recommendation: Congress and the administration should encourage flexible federal policies that promote ongoing innovation and best practices for hardware- and software-integrated security.

Multi-stakeholder Processes: The interests of the government, consumers, and industry are aligned in the shared desire to minimize vulnerabilities and create safe devices, networks, products, and services that are as secure as possible. Consequently, the most productive and impactful activities designed to enhance cybersecurity take place through voluntary consultation and close collaboration with the private sector. We strongly encourage that this approach continue.

For example, the National Institute of Standards and Technology (NIST) Cybersecurity Framework was published in February 2014 following a collaborative, multi-stakeholder process involving industry, academia, and government agencies. According to NIST, "[t]he original goal was to develop a voluntary framework to help organizations manage cybersecurity risk in the nation's critical infrastructure, such as bridges and the electric power grid, but the framework has been widely adopted by many types of organizations across the country and around the world."[13] NIST, in collaboration with industry, academia, and other government agencies continues to update the framework on an ongoing basis. In January 2017, NIST issued a draft update to the Cybersecurity Framework, providing new details on managing cyber supply chain risks, clarifying key terms, and introducing measurement methods for cybersecurity.[14]

In addition, in mid-2014, NIST established the Cyber-Physical Systems Public Working Group (CPS PWG).[16] Cyber-physical systems (CPS) are smart systems that include engineered interacting (interconnected) networks of physical and computational components.[17] The CPS PWG brought together a wide range of public, private, and academic experts from the United States and around the globe in an open public forum to help define and shape key characteristics of CPS, with the objective of better managing development and implementation within and across multiple smart application domains including smart manufacturing, transportation, energy, and healthcare.[18] The CPS PWG established five expert subgroups to deep dive on important CPS issues including cybersecurity, privacy, data interoperability, vocabulary and reference architecture, timing and synchronization, and use cases. After two years of intense collaboration, the CPS PWG completed the CPS Framework Release 1.0 in May 2016 which documented the work of the five subgroups. [19] As the Framework states, "CPS and IoT are sometimes used interchangeably; therefore, the approach described in this CPS Framework should be considered to be equally applicable to IoT."[20] This is an ongoing activity. After public review and finalization of the Framework, the applicability of this approach will be assessed in selected CPS domains leading to a planned future road mapping activity to both improve the CPS Framework and develop understanding and action plans to support its use in multiple CPS domains.[21]

Similarly, the multi-stakeholder efforts undertaken by the DOC and convened by the National Telecommunications Information Administration (NTIA) should be utilized to a greater and ongoing extent in addressing complex security issues. The current NTIA Cybersecurity Vulnerabilities multi-stakeholder process, as well as the current NTIA IoT Security Upgradability and Patching multi-stakeholder process, provide examples of public-private collaboration to address pressing security needs while maintaining the necessary flexibility that rigid regulatory approaches would prevent. NTIA's Cybersecurity Vulnerabilities multi-stakeholder process, which launched in September 2015, is a "collaboration between security researchers and software and system developers and owners to address security vulnerability disclosure."[22] In December 2016 stakeholder participants released a set of initial findings, recommendations, and resources, and NTIA continues to work with stakeholders on further developments and outreach.[23]

Similarly, the NTIA-convened IoT Security and Upgradability and Patching multi-stakeholder process launched in October 2016 to help with the recognized need for a secure lifecycle approach to IoT devices, focused on developing a broad, shared definition around security upgradability for Consumer IoT, as well as strategies for communicating the security features of IoT devices to consumers.

These voluntary, broad-based efforts exemplify a proven track record of success in improving security innovation and protection through multi-stakeholder efforts and public-private collaboration. Other examples include DHS' Strategic Principles for Securing the IoT, released in November 2016 after consultation with industry stakeholders. The DHS paper sets forth non-binding principles for mitigating IoT security risks for those who "develop, manufacture, implement, or use network connected devices"[24] and notes that, while there is "no one-size-fits-all solution for mitigating IoT security risks across the diversity of IoT devices[,]" "widespread adoption of these strategic principles and the associated suggested practices would dramatically improve the security posture of IoT."[25] Moreover, the technology industry also leads and contributes to other significant cybersecurity public-private partnerships with the federal government, including information sharing, analysis, and emergency response with government and industry peers such as the Department of Defense's (DoD) Defense Industrial Base Cybersecurity Information Sharing Program (cybersecurity information sharing and incident reporting); the Information Technology Information Sharing and Analysis Center (sharing of cybersecurity threats and insights); and DHS' Sector Coordinating Councils (coordination of critical infrastructure security and resilience).

We applaud and encourage the federal government to continue its leadership as a convener and thought leader in this regard. As DHS – the nation's expert agency responsible for safeguarding the American people and our homeland's critical infrastructure – states in its Strategic Principles: "As with all cybersecurity efforts, IoT risk mitigation is a constantly evolving, shared responsibility between government and the private sector ... The role of government, outside of certain specific regulatory contexts and law enforcement activities, is to provide tools and resources so companies, consumers, and other stakeholders can make informed decisions about IoT security."[26] Industry is in broad agreement that we must continue to leverage America's private sector, academic, and other third party experts to collaboratively address cybersecurity of the IoT and other technologies, and further invest in these important and forward-thinking multi-stakeholder and public-private efforts currently underway. Policymakers should seek to reinforce this collaborative environment to encourage innovative, private-public cooperation on these issues, rather than top-down regulations that may duplicate ongoing work or become quickly outdated by the evolving threat landscape.

Recommendation: It must be a federal priority to continue to build upon and invest in cybersecurity multi-stakeholder efforts, leveraging the best of our public and private sector experts and resources to constantly improve the security of the IoT and other technologies. The federal government should continue to initiate and support multi-stakeholder activities and working groups, collaborate with industry to understand evolving threats, and develop best practices for IoT security and data privacy. DOC and its agencies such as NIST and NTIA, as well as DHS, are the appropriate entities to continue to lead such efforts.

Consumer and Small Business Education: Consumer education and awareness of threats and how consumers can protect themselves must be a critical part of the nation's cybersecurity plan. The October 2016 Distributed Denial of Service (DDoS) attack on Dyn (a cloud-based Internet performance management company) – which targeted many now-connected legacy devices – highlights the importance of consumer cybersecurity education. In this regard, we encourage innovative efforts like the Federal Trade Commission (FTC) Home Inspector Challenge announced in January, where the agency is challenging the public to create an innovative tool that will help protect consumers from security vulnerabilities in software of home devices connected to the IoT with a focus on addressing risks created by legacy devices and of out-of-date software.[27] Similarly, we support efforts like the FTC's Start with Security guidance to help small business secure the IoT devices they deploy on their networks. [28]

There are other steps that should be taken as well. For example, the Small Business Administration (SBA) has established programs to educate small- and medium-sized business (SMBs) owners about cybersecurity, provide resources to assess information security resilience, and create customized cybersecurity plans.[29] Congress can reinforce these and other existing programs by providing more resources for agencies to educate SMBs on risk management and promote the use of processes and procedures to protect information systems against cybersecurity threats. As a result, SMBs would not only implement better cybersecurity practices, but also contribute to more secure supply chains for large businesses and the federal government.

Moreover, as new technologies develop and threat landscapes evolve, ongoing and evolving consumer education on how to appropriately secure Internet-connected personal devices like smart phones, baby monitors, and cameras, as well as home wireless networks, becomes even more important. To this end, there is broad agreement that the appropriate expert federal agencies like the FTC and Federal Communications Commission (FCC) should educate consumers on cybersecurity tools on an ongoing basis and encourage the use of cybersecurity best practices that incentivize good cyber hygiene.

Recommendation: Congress should direct the FTC, SBA, and FCC – with input from industry – to develop complementary cybersecurity hygiene education and awareness outreach initiatives for consumers and small businesses. These initiatives should focus on security tools and best practices for Internet-connected things to help better secure devices and wireless networks from intrusions.

Federal Procurement: A 2015 Veracode study compared civilian federal agencies to the private sector and found that federal agencies rank last in fixing security problems and even fail to comply with existing security requirements 76 percent of the time.[30] In today's threat environment, this should be unacceptable. The federal government must address this problem, largely involving legacy systems, both promptly and comprehensively in order to protect federal assets. We encourage Congress and the administration to immediately require federal departments and agencies to comply with existing security requirements, at the very minimum, and deploy multi-layered hardware- and software-integrated cybersecurity solutions to protect legacy and new assets.

In addition, the federal government should upgrade its IT systems. Secure, interoperable (non-proprietary), and scalable IoT solutions can vastly improve the federal government's efficiency and productivity, helping to meet department and agency missions in a more timely manner and saving significant taxpayer dollars. Moreover, upgrading to hardened end-to-end (device to cloud) IoT solutions will protect storage, device identification and authentication, software authentication, and enable a trusted execution environment that will be far more secure than legacy systems that can be rife with vulnerabilities. We must prioritize federal procurement requirements for such multi-layered protection using hardware- and software-integrated security. Doing so would help secure not only federal assets, but also drive awareness and deployment for contractors and other stakeholders that interface with the federal government.

Recommendation: Congress should direct federal departments and agencies in the procurement process to prioritize secure, interoperable, and scalable IoT solutions for federal assets, based on voluntary, industry-led, consensus-based, global standards. Secure solutions, with multi-layered hardware- and software-level capabilities, must be a government procurement requirement for both IoT and non-IoT solutions in order to protect the nation.

5. Prioritization of Smart Infrastructure Solutions

As U.S. policymakers consider how best to address America's infrastructure, we appreciate the challenge facing Congress and the administration in efficiently allocating limited federal taxpayer dollars and attracting private sector investment. We recognize the importance of federal and state physical infrastructure spending such as building new highways and repairing roads and bridges. These expenditures are necessary, and importantly, create immediate job growth in construction and related sectors that is positive for American families. Moreover, physical infrastructure spending, when enhanced by the capabilities of IoT solutions, will not only increase jobs in the short-term but also drive economic growth in the medium- and long-term. Thus, we stand at a fortuitous moment in America's history when physical and digital capabilities can be harnessed simultaneously to generate maximum returns on public investments.

For this reason, we urge Congress and the administration to also prioritize smart, data-driven infrastructure solutions to drive U.S. leadership and economic growth over the medium- and long-term. Building IoT solutions into our infrastructure will create thousands of new construction jobs in the short-term — while also saving significant taxpayer dollars, helping solve longstanding societal challenges, and boosting America's economy over the long-term. In fact, "studies find that investments in IT-enabled infrastructure can have 60 percent greater productivity impacts than investments in roads alone" because "making physical infrastructure smart will enable … network effects, enabling smart vehicles, smart logistics, and other related improvements."[31] These network effects are critical to driving medium- and long-term growth because they "unlock new economic opportunities, create jobs, and improve people's quality of life"[32] long after short-term job growth and construction ends.

Therefore, as America's policymakers draft legislation to improve and modernize the nation's infrastructure, we encourage Congress and the administration to make significant investments in deploying 21st century, data-driven solutions in both new and existing infrastructure – whether building from the ground up or repairing older assets. We support a mix of federally-funded projects and tax incentives, as well as PPPs, to accelerate these smart infrastructure investments in the United States. These smart IoT solutions can significantly increase infrastructure safety, efficiency, and reliability by improving real-time decision-making and management of infrastructure assets, enabling predictive maintenance, lowering long-term infrastructure costs, and increasing infrastructure life-span. To this end, legislation must have a clear and articulate goal of transforming traditional infrastructure into smart, 21st century infrastructure to enable increased connectivity, security, compute capabilities, and data-centric decision-making. Legislation also must promote the advancement of associated policies needed to accomplish this objective, or else this much needed infrastructure transition will lag.[33]

Moreover, consistent with prior recommendations in this report, infrastructure legislation should require these smart IoT solutions to meet the following criteria: end-to-end solutions that enable data-driven decisions utilizing hardware, analytics software, non-proprietary networks, sensors, gateways, and servers; multi-layered protection using hardware- and software-integrated security from the outset that, at a minimum, protects storage, device identification and authentication, software authentication, and enables a trusted execution environment; solutions based on industry-led, global, consensus-based standards and not government mandates; and interoperable, scalable, secure platforms and technologies.

Specifically, we recommend deploying data-driven IoT infrastructure solutions to address federal agency missions, as well as to future proof the nation's transportation system, electric grid modernization and reliability, water management facilities, government buildings, public safety broadband networks, and critical infrastructure.

Federal Agencies: The infrastructure package is an excellent opportunity to leverage the benefits that government can achieve as a user of data-driven, IoT solutions – with the goal of making the U.S. government the IoT showcase for the world. Just as the IoT will transform the private sector through innovation and efficiency, so too can the IoT help government agencies achieve their own missions more effectively and at lower cost. Additionally, government reliance upon IoT as an early adopter, including new public-private collaborative uses of IoT solutions, also will help stimulate and accelerate private sector IoT investment in the America.

Recommendation: Congress and the administration should make it a federal priority in infrastructure legislation to both fund and incentivize smart, data-driven IoT solutions that advance federal agency missions.

Transportation and Automated Vehicles: We encourage investment in smart infrastructure to improve and modernize the nation's transportation system and accelerate the safe deployment of automated vehicles. Indeed, transportation is one of the most promising sectors for the IoT. The International Data Corporation (IDC) has projected that global revenue from the transportation sector will reach $325 billion by 2018. By converting vast amounts of data into meaningful and actionable intelligence, IoT infrastructure solutions will help solve transportation safety, efficiency, and mobility challenges.

For example, "[s]mart traffic lights that sense ebbs and flows and adjust accordingly can reduce travel time in cities by 25 percent."[34] IoT infrastructure solutions also will "help maximize the use of existing transportation infrastructure and even improve its maintenance and repair,"[35] as well as modernizing any new infrastructure – making the nation's roads and highways "smarter, more efficient, safer, and more durable."[36] Moreover, "[a]pplying a digital layer allows for real-time insight into infrastructure performance, which can generate substantial economic and public safety benefits through preventative maintenance and early warning systems." [37]

We must also invest in the modern infrastructure necessary to accelerate the safe deployment of automated vehicles. This means investing in consistent digital signage, smart sensors, and clear road markings if America is to attract significant investment and lead the world in this competitive sector. "Shoddy infrastructure has become a roadblock to the development of self-driving cars, vexing engineers and adding time and cost. Poor markings and uneven signage on the 3 million miles of paved roads in the United States are forcing automakers to develop more sophisticated sensors and maps to compensate."[38] To address this barrier to automated vehicle deployment, Congress should direct the Department of Transportation (DOT) to allocate a substantial portion of its innovation funding[39] to IoT transportation solutions and automated vehicle infrastructure projects, including the integration of next generation mobile broadband networks to improve transportation safety. Congress also should ensure that these upgrades and implementations are immediately eligible for funding under the existing highway transportation authorization.[40] They also should tie a share of federal surface transportation funding to states' actual improvements in transportation system performance using IoT solutions which would promote an incentive to invest in cost-efficient digital infrastructure.[41]

Moreover, as stated in the Conference Report accompanying the *Fixing America's Surface Transportation (FAST) Act*, Congress should "ensure[] that [DOT] programs are implemented and Intelligent Transportation Systems (ITS) are deployed in a technology neutral manner. The FAST Act promotes technology neutral policies that accelerate vehicle and transportation safety research, development, and deployment by promoting innovation and competitive market-based outcomes, while using federal funds efficiently and leveraging private sector investment across the automotive, transportation, and technology sectors."[42] Clearly, Congress recognized that when government seeks to directly or indirectly choose technologies, however well-intended, these decisions lag behind and often thwart marketplace innovation.

Accordingly, Congress should direct DOT to award innovation funding on a technology-neutral basis to help enable and accelerate industry-driven innovation and investment, maximizing the return on U.S. taxpayer dollars.
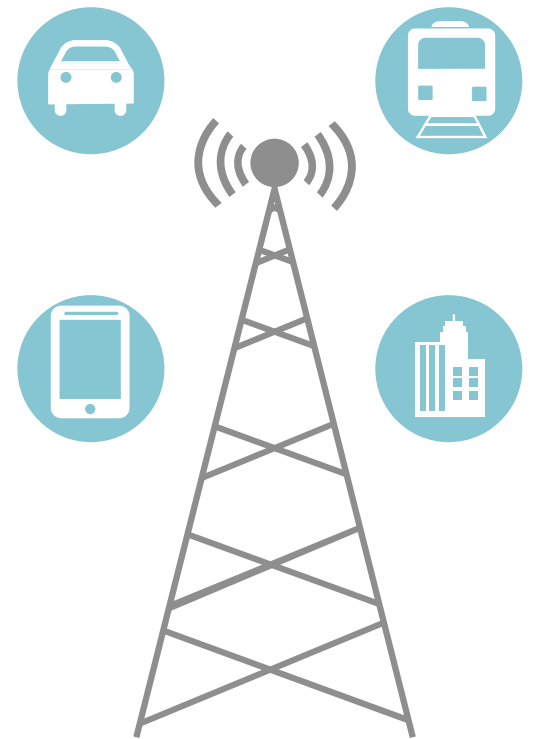
Industry, not government, should be driving innovation in the transportation and automotive sectors; government should not be using taxpayer dollars to create a market for government-favored technologies or to choose technology winners and losers. Public policies that encourage innovation, competition, and market-driven investment are critical to enable self-driving vehicles to reach their full potential in the United States, realize maximum economic and safety benefits for Americans, and become widely available across the nation in a timely and globally competitive manner.

Recommendation: To modernize the nation's transportation system, infrastructure legislation should fund and incentivize smart IoT solutions on a technology-neutral basis in a way that boosts market-driven investment, including investing in technologies that will accelerate the safe deployment of automated vehicles.

5G and Next Generation Mobile Broadband Networks: When considering infrastructure legislation, it also will be important how the federal government addresses key foundational technologies that will serve as the core architecture for the IoT. Most significantly, in the next few years, 5G – the rapidly emerging successor to today's 4G – will bring communications and computing together in a fundamental shift for the United States and the world in a way that is essential to lay the foundation for our IoT future. 5G will be defined by a heterogeneous network of wireless communications technologies – including Wi-Fi, LTE-Advanced, mmWave, and others – combined with a virtualized core and intelligent edge services. It will not only increase capacity, but it will also enable even the smallest devices to perform heavy computational tasks by bringing the cloud to the edge of the network. According to Intel's Communication and Devices Group, moving to 5G will transform our daily lives. For instance, "autonomous vehicles will be able to make decisions in milliseconds to keep drivers and vehicles safe. Drones will aid in disaster recovery efforts, providing real-time data for emergency responders. Smart cities will monitor air and water quality through millions of sensors, giving them insights needed to provide a better quality of life."[43] And this is just the start.

Evidence of the global race to secure 5G leadership is everywhere and should be viewed by U.S. policymakers as both a wakeup call, as well as a challenge to move intelligently and swiftly.[44] For example, 5G deployments are already underway in Russia for the 2018 FIFA World Cup,[45] in South Korea for the 2018 Winter Olympics,[46] and in Japan for the 2020 Summer Olympics.[47]

China started large-scale testing of 5G networks this year, and China Mobile aims to continue with deployment testing in 2018 with commercial operations starting in 2020.[48] Meanwhile, Europe has a 5G Action Plan to boost the deployment of 5G infrastructure and services across the Digital Single Market with the objective of making 5G a reality for all citizens and businesses by 2020.[49] Clearly, the global 5G race is on.

Moreover, 5G offers the benefits of extensive global private industry investment, coupled with strong consumer demand, similar to its previous cellular iterations of 3G and 4G. These benefits propel technologies to the forefront and enable them to evolve at the pace of innovation – which will be key to the long-term evolution and scale of the IoT. Accordingly, for the United States to lead the IoT future, it is vital that the nation's infrastructure strategy recognizes this worldwide marketplace direction and enormous industry investment in 5G – and that America invests wisely in this innovative communications and computing technology platform.

In addition, with respect to spectrum and mobile broadband networks more generally, today's communication infrastructure – comprised of a diverse portfolio of licensed and unlicensed spectrum – will be challenged by the rapid and extensive proliferation of IoT devices and services. Connecting tens of billions of things to each other, to people, and to the cloud will place unprecedented demands on today's wireless networks and generate many zettabytes of data.[50] Our nation's infrastructure must continue to evolve to meet these rapidly increasing capacity and computational demands across the growing breadth of IoT applications, many unimaginable today. And these applications will vary widely in their requirements and the diverse set of wireless communications technologies used. Thus, rather than designate specific IoT bands or technical standards, the federal government should continue to foster private investment and public-private collaboration.

Government can accomplish this objective by allocating commercial licensed and unlicensed spectrum in a technology-neutral and service-neutral way across a wide range of frequencies. This will enable service providers and innovators to make use of the most appropriate communications spectrum and technologies for their IoT applications. For example, emergency medical services may require guaranteed low-latency, high-reliability communication between an instrument carried by a first responder and a doctor at a central location, while a distributed network of moisture sensors for drought-tolerant farming may need very low power consumption (for long battery life) with less dependence on instantaneous delivery. The federal government also should identify additional government-used spectrum for clearing and/or sharing with commercial wireless services and streamline the regulatory environment for deployment of communications network infrastructure.

Recommendation: Infrastructure legislation should promote the deployment of key foundational technologies like 5G mobile broadband networks that will serve as the core architecture for the IoT, and Congress should direct NTIA and the FCC allocate commercial licensed and unlicensed spectrum in a technology-neutral and service-neutral way across a wide range of frequencies to address the breadth of IoT use cases today and into the future.

Smart Buildings: As part of an infrastructure package, we encourage Congress to allocate funding to smart building technologies using data-driven IoT solutions to improve building automation in new construction, renovation, and retrofit of civilian and military buildings. Such IoT solutions should connect, secure, and manage actionable data from existing and new building systems (e.g., heating, ventilation, and air conditioning (HVAC), electricity, lighting, water, natural gas) to achieve the following operational efficiency goals: enable remote monitoring of building assets; enable predictive maintenance of building assets; improve building comfort for increased productivity; improve real-time decision-making regarding building assets; and lower long-term building and asset costs for increased sustainability and life-span. For example, water mains embedded with Internet-connected sensors can detect and transmit information on leaks. Smart traffic lights that adjust with ebbs and flows of traffic can reduce travel time in cities by 25 percent.[51]

The criteria for smart building solutions (similar to those discussed above) should be the following: secure, scalable, interoperable IoT platforms; end-to-end solutions that utilize hardware, analytics software, non-proprietary networks, sensors, gateways, and servers to enable data-driven decisions; multi-layered protection of building assets using hardware- and software-integrated security that, at a minimum, protects storage, device identification and authentication, software authentication, and enables a trusted execution environment. These smart building IoT solutions should be a priority consideration in the design, renovation, or retrofit of all civilian and military construction projects including any new or existing office space, housing, commercial, and other facilities. These projects should serve as scalable models for implementation of data-driven IoT solutions to enable asset optimization in civilian and military buildings across the nation.

Including smart building goals in federal facilities will save the government considerable public resources and federal taxpayer dollars. At a time when the federal government is looking for ways to save money, embrace smart technology, and spur innovation, electing to embrace IoT technologies across its vast government and military facility base would be a wise use of limited resources. Supporting the use of large scale smart building testbeds would also encourage local and state governments to follow the federal government's lead in adopting cutting-edge and resource-saving IoT technologies.

Recommendation: Infrastructure legislation should fund and incentivize smart government building technologies using data-driven IoT solutions to improve building automation in new construction, renovation, and retrofit of both civilian and military buildings.

6. Invest in IoT PPPs, Research, and Testbeds

Government and industry collaboration can be one of our nation's best assets to accelerate the deployment of the IoT in America in a globally competitive manner. Using public and private resources to facilitate IoT testbeds and research – while leveraging existing industry standards and investments – will accelerate the nation's future toward IoT leadership. Viable PPPs will entail logical investments for both government and industry, as well as ensure scalability of IoT innovations and sustainability of deployments over the long term.

Therefore, as part of our National IoT Strategy, U.S. policymakers should encourage the deployment of globally competitive and rapidly scalable PPPs, research initiatives, and testbeds. These joint public-private efforts should span the breadth of IoT sectors from automotive and energy to agriculture and manufacturing – like those being launched by global industry-led efforts such as IIC. Through this collaborative innovation, we can transform America's landscape to smart cities and communities that use IoT solutions to improve traffic management, public safety, air quality, energy reliability, and water management. Such IoT PPPs, research, and testbeds are critical to accelerate the nation's IoT infrastructure and, accordingly, essential to U.S. leadership in this transformative technology evolution.

Specifically, we recommend that U.S. policymakers encourage and participate in IoT PPPs, research, and testbeds including, but not limited to, these areas:

- **Trusted Data and Secure Compute**: Industry has long touted security as a foundation for the IoT. Indeed, powerful computing with integrated hardware and software level security is critical to the IoT's success. For example, securing connected vehicles and the supporting infrastructure is foundational to keeping passengers safe and secure, and requires an end-to-end system (vehicle-to-network-to-cloud) approach. Not only must every connected vehicle be safeguarded against cyber threats, but every device connected to the vehicle and the personal information available via these devices must also be kept private as it moves between the vehicle, connected devices, connected infrastructure, and the cloud.

- **Artificial Intelligence (AI):** AI and IoT are interdependent; IoT has enabled the collection and use of data across multiple devices, paving the way for the development of AI technologies that rely on and learn from this data. We have already begun to see how AI can benefit people and society in fields as diverse as healthcare, transportation, the environment, criminal justice, and economic inclusion. For example, autonomous vehicles, the product of the IoT and AI, collect and analyze data that will enhance human safety, increase productivity, and yield economic gains for society. Intel has been investing in companies with expertise in functional safety and doing foundational research in Deep Learning for many years, and is working to ensure that our products, from the thing (vehicle) to the network to the cloud, are capable of bringing the intelligence needed for the vehicle to sense and adapt.

- **Open, Standards-Based Platforms:** Global standards, such as those being driven by IIC, OCF, OpenFog, and the Open Fabrics Alliance[52] can accelerate adoption, drive competition, and enable the cost-effective introduction of new technologies. For example, the tech industry is partnering with the auto industry to research and define standards to accelerate autonomous driving deployments and create economies of scale that enable rapid marketplace adoption. This will enable industry leaders to contribute core technology including platform software, machine learning algorithms, and data collected from vehicle sensors to enable a safe and secure driving experience. And, as noted above, the IoT industry is contributing broadly to the global consortia efforts of organizations like IIC, OCF, and OpenFog in researching and developing interoperable standards for IoT platforms.

Industry is leading IoT PPPs, research, and testbed efforts, often in concert with academia and government partners, around globe. The U.S. government should participate in these activities. However, government should refrain from directing the activity in order to allow industry to innovate, develop, and adopt flexible solutions. Specifically, government participants should not use their participation in PPPs, research, or testbed activities to steer industry innovation toward a government-favored technology, or as an indirect "carrot" mechanism to pick technology winners and losers.

Recommendation: **To ensure U.S. global IoT leadership, the federal government should invest in IoT PPPs, research, and testbeds, such as those being driven by leading global industry consortia like IIC, OCF, and OpenFog.**

1 McKinsey and Company, Unlocking the Potential of the Internet of Things, June 2015 https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world.

2 Intel Corporation, Internet of Things Policy Framework, at 1, http://www.intel.com/content/dam/www/public-/us/en/documents/corporate-information/policy-iot-framework.pdf.

3 Developing Innovation and Growing the Internet of Things (DIGIT) Act, S. 88, 115th Cong. (2016), https://www.congress.gov/bill/115th-congress/senate-bill/88.

4 U.S. Dept. of Commerce, Fostering the Advancement of the Internet of Things, at 44-48 (Jan. 2017), https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf.

5 Executive Order 13771, Presidential Executive Order on Reducing Regulation and Controlling Regulatory Costs (Jan. 30, 2017); Executive Order 13777, Enforcing the Regulatory Reform Agenda (Feb. 24, 2017).

6 See Comments of Information Technology Industry Council, Docket No. 160331306-6306-01, at 12 (June 2, 2016); Comments of the U.S. Chamber of Commerce Technology Engagement Center, Docket No. 170105023-7023-01, at 5 (Mar. 13, 2017); Comments of the Consumer Technology Association, Docket No. 170105023-7023-01, at 13-14 (Mar. 13, 2017).

7 For more information, see Industrial Internet Consortium http://www.iiconsortium.org/about-us.htm (last visited May 23, 2017).

8 For more information, see Open Connectivity Foundation, https://openconnectivity.org/about (last visited May 23, 2017).

9 For more information, see OpenFog Consortium, https://www.openfogconsortium.org/about-us/ (last visited May 23, 2017).

10 GSMA, Connected Living: The importance of Embedded SIM certification to scale the Internet of Things, http://www.gsma.com/connectedliving/wp-content/uploads/2017/02/1038-FM-GSMA-Test-Cert-eBook-V6.pdf (February 2017).

11 U.S. Dept. of Homeland Security, Strategic Principles for Securing the Internet of Things, at 14 (Nov. 15, 2016) ("DHS IoT Cybersecurity Principles"), https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf..

12 EMC2/IDC, The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things: Executive Summary (Apr. 2014), http://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm.

13 U.S. Dept. of Commerce NIST, NIST Releases Update to Cybersecurity Framework (updated Jan. 31, 2017), https://www.nist.gov/news-events/news/2017/01/nist-releases-update-cybersecurity-framework..

14 See U.S. Dept. of Commerce NIST, Framework for Improving Critical Infrastructure Cybersecurity: Draft Version 1.1 (Jan. 10, 2017), https://www.nist.gov/sites/default/files/documents////draft-cybersecurity-framework-v1.11.pdf.

15 Id. at 14.

16 U.S. Dept. of Commerce NIST, CPS PWG, https://pages.nist.gov/cpspwg/ (last visited May 19, 2017).

17 U.S. Dept. of Commerce NIST, CPS PWG, Framework for Cyber-Physical Systems Release 1.0, at xiii (May 2016), https://s3.amazonaws.com/nist-sgcps/cpspwg/files/pwgglobal/CPS_PWG_Framework_for_Cyber_Physical_Systems_Release_1_0Final.pdf

18 Id.

19 Id.

20 Id. at 1.

21 Id. at xiii.

22 U.S. Dept. of Commerce NTIA, Multistakeholder Process: Cybersecurity Vulnerabilities, https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities (last visited May 19, 2017).

23 Id.

24 DHS IoT Cybersecurity Principles at 4.

25 Id. at 5.

26 Id. at 4.

27 Press Release, FTC, FTC Announces Internet of Things Challenge to Combat Security Vulnerabilities in Home Devices (Jan. 4, 2017), https://www.ftc.gov/news-events/press-releases/2017/01/ftc-announces-internet-things-challenge-combat-security..

[28] FTC, Start with Security: A Guide for Business, Lessons Learned from FTC Cases (June 2015), https://www.ftc.gov-/tips-advice/business-center/guidance/start-security-guide-business.

[29] See, e.g., SBA Learning Center, Cybersecurity for Small Businesses, https://www.sba.gov/tools/sba-learning-center/training/cybersecurity-small-businesses (last visited May 23, 2017).

[30] Arik Hesseldahl, Why the Federal Government Sucks at Cyber Security, Recode (June 23, 2015), https://www.recode.net/2015/6/23/11563798/why-the-federal-government-sucks-at-cybersecurity..

[31] Peter L. Singer, Investing in "Innovation Infrastructure" to Restore U.S. Growth, ITIF at 9 (Jan. 2017) ("ITIF Innovation Infrastructure"), http://www2.itif.org/2017-innovation-infrastructure.pdf?_ga=2.236106113.1093994383.-1495464199-421905161.1495464159..

[32] Robert D. Atkinson et al., A Policymaker's Guide to Smart Infrastructure, ITIF at 1 (May 2016) ("ITIF Policymaker's Guide"), http://www2.itif.org/2016-policymakers-guide-digital-infrastructure.pdf. See also Innovation Infrastructure at 9 (stating, "[S]mart infrastructure is likely to have bigger productivity payoffs than … pouring more concrete or laying pipe.").

[33] ITIF Policymaker's Guide at 26.

[34] ITIF Innovation Infrastructure at 9.

[35] ITIF Policymaker's Guide at 12.

[36] Id. at 10.

[37] Id. at 21.

[38] Alexandria Sage, Where's the lane? Self-driving cars confused by shabby U.S. roadways, Reuters (Mar. 31, 2016), http://www.reuters.com/article/us-autos-autonomous-infrastructure-insig-idUSKCN0WX131.

[39] The FAST Act authorized $305 billion over fiscal years 2016 through 2020 for highway, highway and motor vehicle safety, public transportation, motor carrier safety, hazardous materials safety, rail, and research, technology and statistics programs. See The Fixing America's Surface Transportation Act, H.R.22, 114th Cong., Title VI – Innovation (2015), https://www.fhwa.dot.gov/fastact/.

[40] See, e.g., ITIF Policymaker's Guide at 25.

[41] See, e.g., id.

[42] H.R. Rep. No. 114-357, at 507 (2015), http://www.gpo.gov/fdsys/pkg/CRPT-114hrpt357/pdf/CRPT-114hrpt357.pdf.

[43] Aicha Evans, Intel Accelerates the Future with World's First Global 5G Modem, Intel (Jan. 4, 2017), https://newsroom.intel.com/editorials/intel-accelerates-the-future-with-first-global-5g-modem/.

[44] Testimony of Doug Davis, Intel, U.S. Senate Cmte. on Commerce, Science and Transportation, Subcmte. on Surface Transportation et al., at 5 (June 28, 2016), available at https://www.commerce.senate.gov/public/_cache/files/46c728ce-377e-4060-9cac-55db2230ddf8/17D163EB418271C1D3BBC8D572D589EE.doug-davis-testimony.pdf.

[45] Luke Johnson, Huawei to introduce 5G networks for 2018 FIFA World Cup, Trusted Reviews (Nov. 19, 2014), http://www.trustedreviews.com/news/huawei-to-introduce-5g-networks-for-2018-fifa-world-cup..

[46] James F. Larson, PyeongChang 2108, the "5G Olympics", Korea's Information Society (Apr. 7, 2016, 8:51 PM), http://www.koreainformationsociety.com/2016/04/pyeongchang-2018-5g-olympics.html.

[47] Eric Auchard, Nokia, NTT DoCoMo prepare for 5G ahead of Tokyo Olympics launch, Reuters (Mar. 2, 2015), http://www.reuters.com/article/us-telecoms-mwc-ntt-docomo-idUSKBN0LY0FD20150302..

[48] Tim Hardwick, China Mobile to Begin Large-Scale 5G Testing This Year, MacRumors (Feb. 22, 2017, 2:11 AM), https://www.macrumors.com/2017/02/22/china-mobile-5g-testing-qualcomm/. .

[49] European Commission, Digital Single Market: 5G for Europe Action Plan, https://ec.europa.eu/digital-single-market/en/5g-europe-action-plan (last visited May 22, 2017).

[50] Press Release, Intel, Intel Accelerates Path to 5G (Feb. 22, 2016), https://newsroom.intel.com/news-releases/intel-accelerates-path-to-5g/.

[51] ITIF Innovation Infrastructure at 9.

[52] See Industrial Internet Consortium, http://www.iiconsortium.org/ (last visited May 23, 2017); Open Connectivity Foundation, https://openconnectivity.org/ (last visited May 23, 2017); OpenFog Consortium, https://www.openfogconsortium.org/ (last visited May 23, 2017); Open Fabrics Alliance, https://www.openfabrics.org/ (last visited May 23, 2017).