PREPARED STATEMENT FOR THE RECORD OF

INTEL CORPORATION

For the

UNITED STATES SENATE COMMITTEE ON

COMMERCE, SCIENCE & TRANSPORTATION

On

THE CONNECTED WORLD: EXAMINING THE INTERNET OF THINGS

FEBRUARY 11, 2015

Intel Corporation ("Intel") respectfully submits this statement for the record in conjunction with the Senate Commerce, Science & Transportation Committee's hearing on "The Connected World: Examining the Internet of Things." Our statement focuses on the opportunity to unleash the vast potential of the Internet of Things (IoT) through public-private partnerships and to create a leadership opportunity for the U.S. in this multi-industry transformation.

Witness: Doug Davis is the vice president and general manager of Intel's worldwide IoT Group (IOTG). Doug has been an Intel employee for 31 years, and began his career as a product engineer in the company's Military and Special Products Division. Over the last decade, Doug has run Intel's worldwide Embedded and Communications Group, managed wafer factory operations, and now leads the IoT Group. This organization is responsible for the company's IoT strategy and solutions – consisting of hardware, software, security and services across a wide range of market segments, including transportation, manufacturing, healthcare, retail, smart home, smart buildings and smart cities. For the past 30 years, Intel has made significant investments, driven exciting innovations, led standards activities, and supported what has evolved to become the Internet of Things. At Intel, we like to say IoT is an overnight transformation thirty years in the making.

INTEL AND THE INTERNET OF THINGS

Intel's Role

The evolution of IoT goes back more than 30 years with Intel as a leader from the start. In 1972, Intel introduced the Intel 4004, the world's first commercially available microprocessor – an invention foundational to the "computer revolution." In the late 1970s, came 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 utilization of real-time operating systems.

The early 2000s saw an unprecedented uptake in internet usage, as the PC and mobile markets exploded. This "connectivity" trend wasn't limited to connecting people; embedded systems were 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 and consumers were enjoying the benefits of connected PCs.

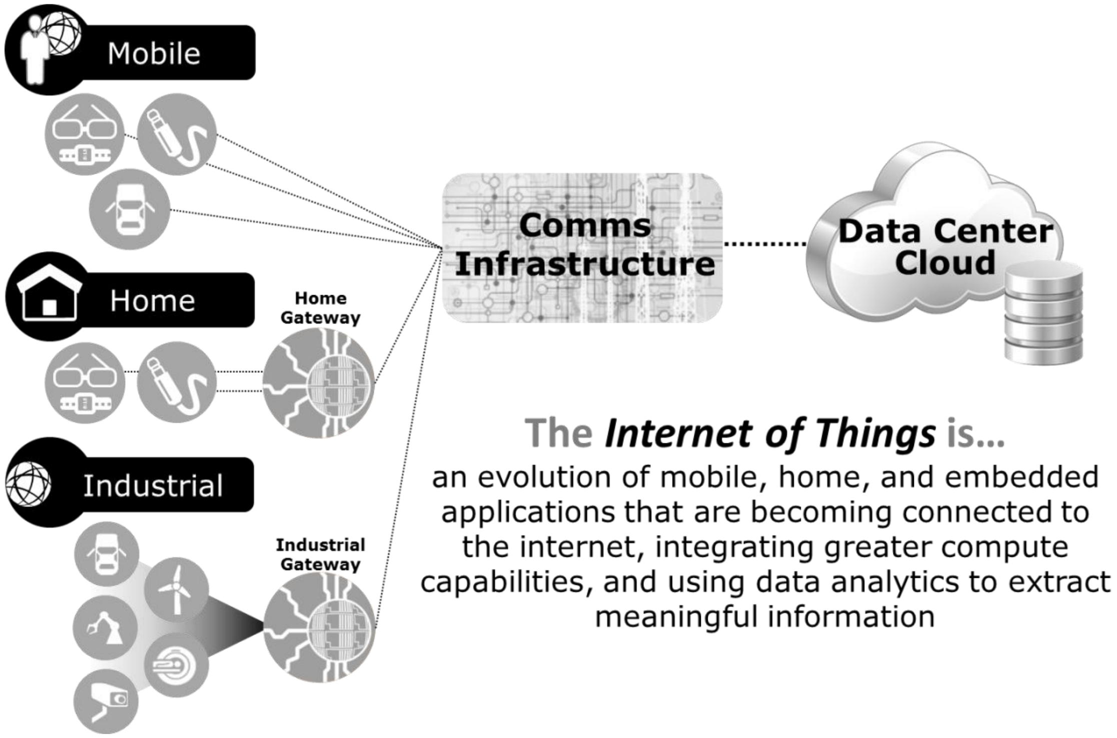
In the late 2000s, “Machine to Machine” (M2M) emerged. M2M refers to technologies that allow both wireless and wired systems to communicate with other devices of the same type. Before M2M, people had to be physically located at the machine to analyze the data to make decisions for managing each machine. With the introduction of M2M, machines could now be managed remotely. All of these innovations within the datacenter, cloud computing, wireless communications and M2M formed the basis of what is now widely known as the IoT.

Moore's Law, the business model that drives the semiconductor industry, states that the number of transistors in an integrated circuit doubles approximately every two years. In essence, the marketplace experiences a doubling of the computing capability at approximately the same price every other year. The observation is named after Intel co-founder Gordon E. Moore. This explosion of networked devices also began to represent another “law” of scaling called 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 (n^2). This enables the Network Effect, whereby the value of a product or service is dependent on the number of others using it. Together, Moore’s Law and Metcalfe’s Law demonstrate how the power of intelligent, connected devices like connected digital signs, cars and homes can unleash innovation, leading to the creation of platforms for new applications and services.

IOT DEFINITION

IoT is defined as endpoint devices such as cars, machinery or household appliances that connect to the internet and generate data that can be analyzed to extract valuable information. There are three sub-definitions emerging out of the IoT space, however, all three definitions overlap. The “Mobile IoT” comprises devices like cars, wearables, sensors and mobile phones which all connect directly through broadband wireless networks. The “Industrial IoT” connects devices in industrial environments like factory equipment, security cameras, medical devices, and digital signs. These devices are able to connect to the internet and into the datacenter (cloud) through an industrial “gateway.”[1] Finally, the “Home IoT” connects devices like game consoles, smart TVs, home security systems, household appliances and thermostats through at gateway to the internet.

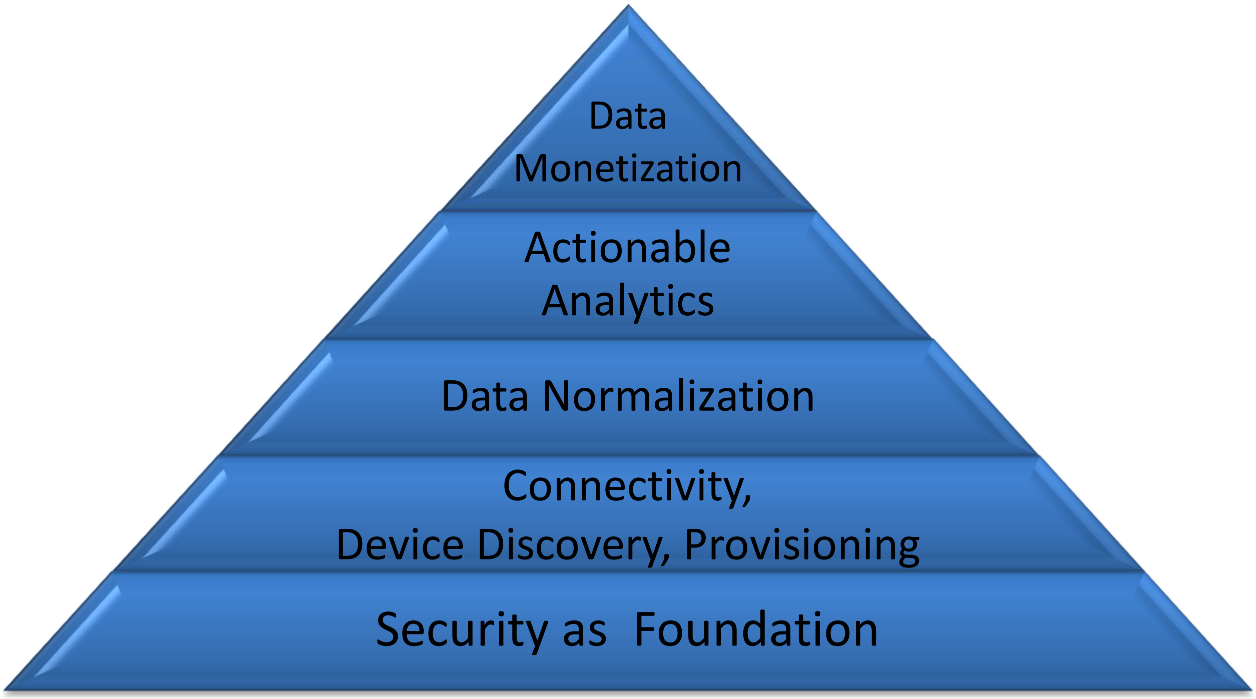
[1] A gateway is a node on a network that serves as an entrance to another network.


Mobile
Home
Home Gateway
Industrial
Industrial Gateway
Comms Infrastructure
Data Center Cloud
The *Internet of Things* is...
an evolution of mobile, home, and embedded applications that are becoming connected to the internet, integrating greater compute capabilities, and using data analytics to extract meaningful information

THE FIVE CRITICAL TENETS OF IOT

In September 2014, Intel and key global partners collaboratively identified five critical IoT tenets which describe how endpoint devices should connect to the cloud. Here are the five key tenets, as illustrated in the graphic below:

First, *Security as the Foundation*: With billions of internet-connected devices by 2020, it is important that IoT is secure from the sensor to the cloud, including all hardware and software. Second, *Connectivity, Device Discovery, and Provisioning*: Billions of devices cannot be managed manually. Rather, devices need to be able to communicate their "status" to the rest of the system independently. Third, *Data Normalization*: With so many different data types, there must be some level of interoperability between devices such that they are speaking the same language. Fourth, *Actionable Analytics*: The data must be turned into meaningful information through analytics. Fifth, *Monetize Hardware, Software, and Data Management*: The IoT infrastructure must be built to allow developers to manage and monetize innovative applications and services.



With these tenets in mind, in December of 2014, Intel launched the Intel® IoT Platform,[2] which unifies security and connectivity to enable scalable IoT deployments. The Platform provides a secure device-to-cloud (end-to-end) open reference model for connecting devices to deliver trusted data to the cloud and value through analytics. The Platform enables tenets 1-3 – security, connectivity, and interoperability – by creating a foundation on which to build IoT solutions. This enables tenets 4 and 5 – data analytics and monetization of new products and services, many of which we never could have imagined a decade ago and may not even conceive of today.

IOT: A TRANSFORMATIONAL OPPORTUNITY BUILT ON A FOUNDATION OF SECURITY

With respect to the critical element of security, Intel values this first and foremost. We believe that security is the foundation of IOT and it is fundamental to Intel's roadmap planning. We have dedicated security products and security features embedded into both our hardware and software products. Our hardware and software are being designed from the beginning to be secure. This is important for trusted data exchange in the IoT, as data generated by devices and

[2] *Intel Unifies and Simplifies Connectivity, Security for IoT*, Intel Corp. (Dec. 2014), http://newsroom.intel.com/community/intel_newsroom/blog/2014/12/09/intel-unifies-and-simplifies-connectivity-security-for-IoT.

existing infrastructure must be able to be shared among the cloud, the network, and intelligent devices for analysis. This enables users to aggregate, filter and share data from the edge of the network all the way to the cloud with robust protection. Moreover, data must be accurate to be beneficial. Intel prioritizes the security, accuracy, privacy and integrity of data in all market sectors, and especially in the industrial domain where the safeguarding of critical infrastructure can be vital to economic and social stability. Intel understands that we must deliver and evoke consumer and industry trust through these hardened security solutions in order to motivate adoption and participation in the IoT marketplace.

Intel believes it is critical to integrate security into the hardware *and* the software, from the smallest microcontroller (MCU) at the edge of the network to the most advanced server CPU in the data center (cloud) and all gateways and devices in between. These hardware- and software-level security capabilities will create redundancies which prevent intrusions and enable a robust, secure, trusted IoT end-to-end solution.

Hardware. Intel's hardware will provide transistor-level security *on the actual compute device itself*. By integrating security into the device itself from the outset (rather than layering it on top at a latter point in the design cycle with other, less secure external features), Intel's IoT solutions will enable our customers to know the exact unique identity of every device on their network. This technology also has the capability for encrypting that unique identity to provide anonymity properties in addition to hardware enforced integrity. Because each compute device can have an immutable identification to enable secure provisioning, a non-approved device will not be allowed to access the network. The MCU or CPU itself will provide the "baked in" (irremovable, non-changeable) identity of the device, making the level of security significantly more robust.

On top of this immutable device identification, Intel's IoT solutions will employ advanced hardware level security capabilities such as "whitelisting," which prevents harmful applications like viruses, control agents, and malware from ever being activated on the device. What this means is that, if the CPU ever "sees" an application that is not on its known good list ("whitelist") try to run on the device, it will automatically lock out that device and not allow it turn on. At other layers in IoT solutions, Intel also uses another advanced hardware security capability called "blacklisting," which blocks a defined list of known malware from entering the device and the network.

Software. In addition to the advanced hardware security capabilities in Intel's IoT solutions, Intel Security (formerly McAfee) integrates advanced security capabilities that provide robust software-level protection. This means that the software is continually monitoring the activity of its networked devices and looking for any abnormalities or possible threats. If the monitoring software identifies a threat, it proactively notifies users and/or automatically quarantines any devices on the network that could be at risk.

By employing this combination of transistor-level security, along with advanced hardware and software level security, from devices on the edge of the network all the way to the data centers in the cloud, Intel will protect IoT assets and information in ways few others can. Intel knows that security is critical to protect the integrity of IoT solutions, so we will design it in from the outset.

IOT PRIORITIES – ENABLERS OF SCALE

Security

As discussed above, security is foundational to the IoT ecosystem and a top Intel priority. With billions of connected devices producing enormous amounts of data –EMC/IDC forecasts that devices will generate more than 44 zeta bytes of data by 2020[3] – security of this data will be critical to enable scale of IoT deployments. That is why we emphasize again the importance of having security designed into the IoT systems from the outset. Secure data delivery systems are critical to enabling trusted data exchange and scale, thereby unlocking the full potential of IoT.

Interoperability

The IoT marketplace is currently aligning around industry sectors/verticals that are starting to deploy IoT solutions to meet their specific business requirements: manufacturing, retail, transportation, healthcare, and others. As early adopters deploy technologies to enable IoT solutions, it is important that the various IoT technologies are "interoperable" with each other as well as being able to adapt and grow to accommodate new and changing business requirements. Proprietary technologies that are inherently antithetical to the concept of the internet of *All* Things will slow down IoT adoption, limit scalability and delay economic benefits.

The Intel IoT Platform's building block components are secure, interoperable, and scalable, enabling "horizontal" end-to-end IoT deployments across industry sectors from transportation to energy to healthcare and beyond. By creating a secure, horizontal, interoperable platform, Intel will enable IoT to scale quickly by creating a repeatable (reusable) foundation that ultimately enables choice and interoperability in the marketplace. For example, Intel offers businesses that use the Intel IoT Platform the choice and flexibility to use some or all of the technology components from Intel, or interchange them with ecosystem partner components. In summary, if the U.S. wants to lead in IoT, we must prioritize interoperability from the start.

[3] *The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things*, EMC/IDC (April 2014), http://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm .

Open Standards

How do we drive a secure solution that is interoperable and scales across a global IoT ecosystem? The solution is a voluntary, global, industry-led, open set of standards which enable scale to drive cost-effective solutions. Over the last 10 months, Intel co-founded two industry consortia focused on interoperability and open standards: The Industrial Interconnect Consortium (IIC)[4] and the Open Internet Consortium (OIC).[5]

IIC founding members include major U.S. companies such as AT&T, Cisco, GE, IBM and Intel. The IIC has reached over 135 members since its inception in March 2014. IIC goals are to: (i) build confidence around new and innovative approaches to security; (ii) drive innovation through the creation of new industry use cases and test beds for real-world applications; (iii) define and develop the reference architecture and frameworks necessary for interoperability; (iv) influence the global development standards process for internet and industrial systems; and (v) facilitate open forums to share and exchange real-world ideas, practices, lessons and insights.

The OIC was founded by leading technology companies with the goal of defining the connectivity requirements for devices, and for ensuring interoperability between the millions of devices that will make up the emerging IoT. OIC founding members include Cisco, GE, Intel, MediaTek and Samsung, and membership has reached over 54 members. OIC goals are to: (i) define the specification, certification and branding to deliver reliable interoperability; (ii) ensure this standard will be an open specification that anyone can implement and is easy for developers to use; (iii) include IP protection and branding for certified devices and service-level interoperability; (iv) provide an open source implementation of the standard; and (v) ensure this open source implementation will be designed to enable application developers and device manufacturers to deliver interoperable products across Android, iOS, Windows, Linux, Tizen, and more.

Both IIC and OIC recognize that a certain level of standardization and interoperability is necessary to achieve a successful IoT ecosystem. In the emerging IoT economy, voluntary global standards can accelerate adoption, drive competition, and enable cost-effective introduction of new technologies. Furthermore, open standards which facilitate interoperability across the IoT ecosystem will stimulate industry innovation and provide a clearer technology evolution path. Industry is in the best position to develop the technological standards and solutions to address global IoT ecosystem opportunities and challenges, and Intel is taking a leading role.

[4] http://www.industrialinternetconsortium.org/

[5] http://openinterconnect.org/

MARKET TRENDS DRIVING THE EMERGENCE OF IOT

If we've had broad use of the internet for over two decades why is the IOT industry emerging now? Intel believes there are three emerging trends are driving the inflection:

Ease of connectivity – Whether it is an unlicensed (WiFi, Bluetooth) or licensed (3G, LTE, 5G) spectrum, connectivity is becoming more pervasive and inexpensive. The opportunity to add value via increased connectivity is extremely large, as 85 percent of devices are not connected today.

Compute economics – Moore's Law is impacting technologies that range from the cloud to the network to storage to sensors. This means that the economics for "compute" have become much more appealing. Specifically, there has been a huge drop in cost for "compute" technologies over the last 10 years; the cost of sensors has decreased 2X, the cost of bandwidth has decreased 40X, and the cost of processing has decreased 60X.

Big Data and Analytics – The emergence of data science (extracting knowledge from data) combined with the reduction in the cost of high performance computing has created an opportunity to turn data into actionable information, thereby enabling new services and new business model innovation.

These three market trends are 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. All of these opportunities are revolutionizing sectors like smart buildings, transportation, healthcare, and manufacturing. Here are just a few examples of quantitative results already enabled by IoT:

Smart Buildings: 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 and Cisco, Rudin Management, a large, commercial real estate company in New York City, deployed Intel's Smart Building IoT solution, which saved Rudin $1 million in just one building in the first year of deployment. Consider the U.S. potential opportunity: There are over 5 million commercial buildings and industrial facilities in the U.S.,[6] with a combined annual energy cost of more than $202 billion.[7]

[6] *Commercial Buildings Energy Consumption Survey (CBECS)*, US Energy Information Administration (5.6 million commercial buildings in U.S. in 2012), http://www.eia.gov/consumption/commercial/reports/2012/preliminary/index.cfm?src=%E2%80%B9%20Consumption%20%20%20Commercial%20Buildings%20Energy%20Consumption%20Survey%20(CBECS)-b1.

[7] http://thesemco.com/about-us/why-energy-efficiency/

It is estimated that the U.S. could save $20 billion if all commercial buildings and industrial buildings increased their energy efficiency by just 10%.[8]

Smart Transportation: The integration of Intel IoT technology with New York-based Vnomics fleet management solutions enabled real-time monitoring and feedback to Georgia-based SAIA Trucking drivers and headquarters. The goal was to reduce maintenance costs and improve driver safety by monitoring braking in real-time. In the first year, SAIA increased fuel efficiency by 6 percent across a fleet of 3,000 trucks, achieving a savings of $15 million. Consider the U.S. potential opportunity: The U.S. trucking industry accounts for about 13 percent of all fuel purchases in the U.S. and trucks consume about 54 billion gallons/year for business purpose.[9] Extrapolating SAIA's success, a 6 percent improvement in fuel efficiency across all trucks in the U.S. would save more than 3 billion gallons of fuel each year, as well as help reduce CO_2 emissions.

Smart Healthcare: Intel has partnered with the Michael J. Fox Foundation to research the use of big data analytics to help improve the treatment of Parkinson's disease. Our IoT personal healthcare solution enables 300 observations per second per patient, thereby monitoring patients' symptoms and drug effectiveness in real-time. This real-time data collection and analysis allows for the identification of the first signs of disease progression and enables physicians to instantly address changes. Patients can receive better, personalized care, and physicians can make improved decisions for treatment in the event that the patient does not notice slight changes that could cause a decline in health before their next regularly-scheduled appointment. Consider the U.S. potential opportunity: Imagine what real-time monitoring of Parkinson's patients' vitals, as well as the ability to make drug and treatment adjustments in real-time, in addition to better tracking and predictability of disease progression could do to improve the quality of life of Parkinson's patients not only in the U.S., but the world.

Smart Cities: Intel has partnered with the city of San José, California in a public-private partnership to further the city's 'Green Vision' goals. This Smart Cities Project, announced as part of the Smart America Challenge in 2014,[10] is expected to help drive San José's economic growth, foster 25,000 clean-tech jobs, create environmental sustainability and enhance the quality of life for residents. Together, Intel and San José City Management are deploying a network of sensors to create a "sustainability lens" that uses Intel IoT technology to measure characteristics such as particulates in the air, noise pollution and traffic flow. This real-time city data will produce meaningful insights that enable the City to make better management decisions, and lead to improvements in air quality, transportation efficiency, environmental sustainability,

[8] *Id.*

[9] http://www.truckinfo.net/trucking/stats.htm

[10] *Intel Helps San Jose Become America's First Smart City*: http://www.psfk.com/2014/06/san-jose-intel-smart-city.html

health, and energy efficiency. Consider the U.S. potential opportunity: The ten largest U.S. cities alone have an aggregated population of 25,292,500 people.[11] What if we initially focused on 10 cities, 10 counties, and 10 rural towns from across the nation and implemented IoT "smart city" solutions into those communities?

IOT: EXTRAORDINARY POSITIVE IMPACT ON U.S. GDP

The IoT presents staggering economic opportunities for the U.S. and the world. Market research firm IDC estimates that there will be 50 billion connected devices in the marketplace by 2020,[12] and Morgan Stanley forecasts 75 billion in that same time period.[13] These estimates would equate to 6 to 10 connected devices for every person on earth. Whether the exact number of devices is 50 billion or 75 billion or something more, one thing is for certain: The number of connected devices will explode in the next five years. In just the automotive industry alone, it is projected that 250 million (or one in five) cars worldwide will be connected to the internet by 2020 – via technologies like WiFi, LTE, Bluetooth, satellite, and 5G communications networks.[14] For perspective, 250 million is roughly the same number of total cars on U.S. roads in 2013.[15]

The reason that policymakers should be excited about this explosion of devices and this technological revolution is the staggering positive impact that the IoT is projected to have on the U.S. and global economy. McKinsey projects that IoT will have an incredible $2.7 trillion to $6.2 trillion global economic impact by 2025.[16] And what should most excite U.S. policymakers is that the U.S. and other developed economies are expected to capture a remarkable 70 percent of this economic impact, if we develop a leadership position.[17] In fact, GE estimates that IoT

[11] United States Census Bureau: U.S. and World Population Clock http://www.census.gov/popclock/

[12] *Business Strategy: The Coming of Age of the "Internet of Things" in Government*, IDC (April 2013), http://www.idc.com/getdoc.jsp?containerId=GIGM01V.

[13] *Morgan Stanley: 75 Billion Devices Will Be Connected To The Internet Of Things By 2020, Business Insider* (Oct.2 2013) http://www.businessinsider.com/75-billion-devices-will-be-connected-to-the-internet-by-2020-2013-10.

[14] *Gartner Says By 2020, a Quarter Billion Connected Vehicles Will Enable New In-Vehicle Services and Automated Driving Capabilities*, Gartner Inc. (Jan. 26, 2015), http://www.gartner.com/newsroom/id/2970017.

[15] *Average Age of Vehicles on the Road Remains Steady at 11.4 years, According to IHS Automotive*, IHS (June 2014) (253M cars on US roads in 2013), http://press.ihs.com/press-release/automotive/average-age-vehicles-road-remains-steady-114-years-according-ihs-automotive.

[16] *Disruptive Technologies: Advances that will transform life, business, and the global economy*, McKinsey Global Institute (May 2013), http://www.mckinsey.com/insights/business_technology/disruptive_technologies.

[17] *Id.*

could boost average incomes in the U.S. by an exceptional 25 to 40 percent over the next twenty years.[18]

Moreover, a recent Accenture survey of CEOs reveals that 87 percent of CEOs expect long-term job growth from IoT.[19] This will positively impact American lives from our nation's farms and factories to markets and Main Street. Indeed, "as the world struggles to emerge from a phase of weak productivity growth, fragile employment and pockets of inadequate demand, the [IoT] offers a chance to redefine many sectors and accelerate economic and employment growth."[20] The U.S. must lead in this technological revolution.

RECOMMENDATIONS FOR POLICYMAKERS

Given the predicted enormous positive impact on the U.S. economy and society, how can policymakers help accelerate IoT and ensure the U.S. leads this next evolution of computing?

1. **Continue an open dialogue with industry, experts and stakeholders as you are doing today.** This IoT hearing is a promising start and the right first step. Intel believes that an open, multi-stakeholder process can best enable a secure and vibrant IoT ecosystem. Also, legislators may want to consider encouraging the Department of Commerce to create a non-partisan National IoT Advisory Board of policymakers, agency representatives, industry leaders, think tanks, academia, and leaders of IoT-focused consortia like IIC and OIC.

2. **Encourage focus on security and interoperability as critical foundational elements of IoT**. While industry is in the best position to develop and determine security and interoperability solutions, government can encourage industry alignment around large-scale IoT deployments based on secure, open and interoperable IoT solutions. This will enable deployments to scale quickly and provide both short-term and long-term economic and social benefits to consumers, government, and businesses.

[18] *New "Industrial Internet" Report From GE Finds That Combination of Networks and Machines Could Add $10 to $15 Trillion to Global GDP*, GE (Nov. 2012), http://www.gereports.com/post/76430585563/new-industrial-internet-report-from-ge-finds-that.

[19] *CEO Briefing 2015, From Productivity to Outcomes: Using the Internet of Things to drive future business strategies*, Accenture, at 7 (2015), http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture-Industrial-Internet-of-Things-CEO-Briefing-Report-2015.PDF.

[20] *Winning the Industrial Internet of Things*, Accenture, at 2 (Jan. 2015), http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture-Industrial-Internet-of-Things-Positioning-Paper-Report-2015.PDF.

3. **Encourage open standards and open architectures** to maintain the long term viability of IoT, based on an approach that is scalable, interoperable and reusable across a variety of use case deployments, vendors and sectors. While industry is in the best position to develop the technological standards and solutions to address global IoT ecosystem opportunities and challenges, government should encourage industry to collaborate in open participation global standardization efforts to develop technological best practices and standards. Specifically, government should encourage the use of commercially available solutions to accelerate innovation and adoption of IoT deployments. The emphasis on commercially available solutions and market-adopted voluntary standards will allow for faster adoption and increase innovation, bringing the IoT and its benefits to reality sooner.

4. C**ollaborate with the industry to develop a U.S. National IoT Strategy** with time-bound goals for sector-specific IoT deployments over the next 3 to 5 years. These deployments will not only address critical societal issues and save tax payer dollars, but also will demonstrate U.S. leadership. A National IoT Strategy will help align IoT stakeholders and incentivize innovation, ultimately creating value for society by increasing efficiencies and productivity, creating jobs, sustaining our environment, and improving quality of life in our cities and towns.

5. **As part of our National IoT Strategy, encourage Public-Private Partnerships (PPPs)** to address societal problems and accelerate more rapid deployment of IoT solutions. Government and industry collaboration can be one of our nation's best assets to accelerate the adoption of a world-class IoT ecosystem. Viable PPPs will make IoT deployments an appealing investment for both government and industry, while ensuring scalability and sustainability of infrastructure and technological innovation over the long term. Notably, countries like China,[21] the UAE,[22] Malaysia,[23] Germany[24], Brazil[25] and others are moving

[21] China's Ministry of Industry and Information Technology is implementing a three-year (2013-15) action plan to establish a National innovation demonstration area of sensor networks in Wuxi, actively promoting pioneer projects of applications such as intelligent manufacturing, agriculture, transportation, medical systems, and environmental protection: http://www.usito.org/news/miit-emphasize-iot-rd-sensors-and-chips-2014.

[22] The Telecommunications Regulatory Authority, in collaboration with the Prime Minister's Office, is working to announce The National Plan for UAE Smart Government Goals*:* http://www.tra.gov.ae/news_The_TRA_to_announce_The_National_Plan_for_UAE_Smart_Government_Goals-636-1.php.

[23] Eyeing a role in global IoT, Malaysia opens CREST centre in Penang (Feb. 2, 2015), http://www.mis-asia.com/tech/applications/eyeing-a-role-in-global-iot-malaysia-opens-crest-centre-in-penang/#sthash.enmSihPu.dpuf.

[24] "As part of its High-Tech Strategy ("Ideas. Innovation. Prosperity.") to consolidate German innovation leadership, Germany is making significant R&D investment in the Internet of Things and new services for the diverse application areas within this new connected world." http://www.gtai.de/GTAI/Navigation/EN/Invest/Industries/Smarter-business/smart-products-industrie-4.0.html

aggressively ahead on IoT deployments – establishing national IoT plans and blueprints establishing time-bound measurable goals, investing substantial funding in IoT research and deployments, and launching PPPs to jumpstart these opportunities and quickly enable IoT scale. As these other countries have recognized, a vibrant and state-of-the-art IoT ecosystem is critical to a nation's global competitiveness and economic stability in the 21st century. By adopting and implementing a National IoT Strategy, the U.S. can seize the leadership position in this next evolution of computing.

PUBLIC-PRIVATE PARTNERSHIPS – MARKET SEGMENT FOCUS

Specifically, over the next 3 to 5 years, the U.S. should focus on industry vertical segments with the potential to have the most impact: transportation, cities (generally communities, urban and rural), and buildings. Here are proposed PPPs for these market segments:

Smart Transportation PPP: The transportation segment is predicted to be valued at more than $351 billion by 2025, with a CAGR of 19.6 percent (2012-25).[26] In FY 2012, the Federal Agency fleet consisted of more than 650,000 vehicles, which collectively drove over 5 billion miles, consumed nearly 400 million gallons of fuel, and had operating costs of approximately $4 billion.[27] The U.S. Postal Service fleet alone is over 190,000 vehicles.[28] Intel recommends encouraging an IoT Smart Transportation PPP around the USPS fleet or another considerably sized government fleet to implement IoT solutions and benchmark increases in fuel economy, logistics and driver efficiency, and improvements in customer service. Focus areas could include, but are not limited to, fleet and freight management, passenger optimization, automatic train protection and control systems and advanced driver assistance and safety.

Impact – Logistics and Transportation was a $1.3 trillion industry in the U.S. in 2012, and represented 8.5 percent of GDP. With almost 9 percent of the U.S. labor force employed in the transportation sector and the U.S. spending roughly $160 billion annually on highway infrastructure (about ¼ funded by the federal government), a more efficient and effective trucking industry has the potential to yield significant savings to the U.S. economy. For

[25] Smart-city to be deployed by Telefonica/VIVO, ISPM in Brazil http://www.smartgridtoday.com/public/Smartcity-to-be-deployed-by-TelefonicaVIVO-ISPM-in-Brazil.cfm

[26] *Strategic Opportunity Analysis of the Global Smart City Market: Smart City Market to be Worth a Cumulative $3.3 Trillion by 2025*, Frost & Sullivan (Sept. 2013) ("Frost & Sullivan"), http://www.frost.com/prod/servlet/report-brochure.pag?id=M920-01-00-00-00.

[27] *Federal Motor Vehicle Fleet Report FY 2012*, http://www.gsa.gov/portal/mediaId/181179/fileName/FY_2012_Federal_Fleet_Report.action.

[28] *Delivery Vehicle Fleet Replacement* (June 10 2014) Office of the Inspector General United States Postal Service [https://www.uspsoig.gov/sites/default/files/document-library-files/2014/dr-ma-14-005.pdf]

example, the commercial trucking industry in the U.S. uses about 50 billion gallons of fuel each year. A 7 percent increase in fuel efficiency results in more than 3.5 billion gallons of fuel saved. Imagine if we set a national goal for 25 percent of the Federal Fleet in 3 years, and 50 percent in 5 years, be retrofitted with IoT transportation solutions, not just for telematics but to increase fuel economy by a minimum of 5 percent, with incentives for higher efficiency.

Approach **–** Consistent with existing national goals to improve the fuel efficiency of American trucks – thereby bolstering energy security, cutting carbon pollution, saving money, and spurring manufacturing innovation[29] – this proposed PPP would leverage private sector and academia IoT expertise in "Intelligent Transportation" solutions. The PPP would accelerate efforts by Congress, DOT, DOC, DOE, EPA, and U.S. commercial fleet managers to increase engine efficiency and fuel economy of large fleets traveling our nation's roads and highways. It would realize direct economic savings including increased fuel efficiency, reduction in carbon dioxide emissions, labor savings, improved driver safety, accident savings, productivity and distribution proficiency, and logistics tracking effectiveness. The PPP also would provide insights into improvements and new business models for the U.S. transportation sector at large, leading to more satisfied employees and customers. Notably, this PPP would be an early step toward the ultimate goal of an autonomous trucking industry; the estimated savings to the U.S. freight transportation industry from autonomous vehicles is $168 billion per year, with savings from labor ($70 billion), fuel efficiency ($35 billion), productivity ($27 billion), and accident savings ($36 billion).[30] Funding for and benefits from the PPP would be shared across public and private sector partners, and could range from in-kind to matching funds to purely financial investments. One possibility could be for public and private partners to share in the transportation fuel savings. For example, if the PPP were to reduce a department', or commercial end user operator's fleet, fuel expenses by 7 percent, the department (operator) could allot 2 percent of that savings to the (other) private partners over a specified period of time until the (other) private partners recoup their upfront investment plus some incremental percent of return. The department operator would retain the remaining percentage of the savings, after which time, the department and U.S. taxpayers (operator) would retain 100 percent of the fuel savings benefit in perpetuity.

[29] *Improving the Fuel Efficiency of American Trucks – Bolstering Energy Security, Cutting Carbon Pollution, Saving Money and Supporting Manufacturing Innovation*, White House (Feb 18, 2014), http://www.whitehouse.gov/the-press-office/2014/02/18/fact-sheet-opportunity-all-improving-fuel-efficiency-american-trucks-bol.

[30] *Autonomous Cars: Self-Driving the New Auto Industry Paradigm*, Morgan Stanley Research (Nov. 6, 2013), *available at* http://www.morganstanley.com/public/11152013.html. The authors indicate that $1.3 trillion is a base case estimate and indicate a bear case scenario of $0.7 trillion savings per year in the U.S. and a bull case scenario of $2.2 trillion per year.

Smart Cities PPP: Today's cities consume two-thirds of the world's energy.[31] By 2025, 37 cities worldwide will each have a population of greater than 10 million.[32] To address the escalating demands of existing and future residents, cities are looking for ways to introduce more technology to become "smarter" about the use of limited resources and more flexible in responding to residents' needs. Examples of "Smart Cities" capabilities could include but are not limited to: City Sensing including monitoring and providing IoT data to improve air quality, noise pollution, ambient light, weather, and traffic flow; smart parking which is using IoT to "smartly" guide citizens to open parking spaces; smart roads that enable "smart" traffic navigation and roadside service; smart emergency response which facilitates "smart" public and residential community alert and response for vulnerable areas; and smart energy/grid that facilitates "smart" renewable energy and distributed power.

Impact – IoT technologies could realize direct economic savings for cities and municipalities (and their local tax base) due to more efficient city planning and management. Results would include improvement in city residents' quality of life, health, and safety. Some examples of this benefit could include more efficient traffic flow, real-time public notifications of pollution "hot spots," and early detection and correction of chemical and gas leaks in aging city infrastructure.

Approach – Consistent with the goals of NIST's Smart America and Global Cities Team Challenges[33] – to use IoT solutions to improve services, promote economic growth, and enhance quality of life – this proposed PPP would leverage private sector IoT expertise in deploying "Smart Community" solutions. These IoT solutions would accelerate local government and municipality efforts to improve urban management and planning in a variety of ways. For example, the PPP could provide a model to improve operational efficiencies and safety across existing and new city infrastructure by utilizing air quality and traffic flow data to enable sustainable traffic management and planning, and create an innovative tool for urban growth management and planning. The funding for and benefits from the PPP would be shared across public and private sector partners, and could range from in-kind to matching funds to purely financial investments. One opportunity may include public and private partners to share in new revenue streams by leveraging the IoT sensor network infrastructure to deliver new services to city residents. For example, if the PPP were to deliver new services to city residents (i) via the city sensor network or (ii) by sharing the real-time data generated by the city sensor network, the city could share the new revenue stream with the private partners. The city (and its taxpayers) would enjoy the benefits of improved traffic flow, air quality, and safety, and avoiding the hefty cost to rebuild city infrastructure.

[31] *World Urbanization Prospects The 2011 Revision*, United Nations Department of Economic and Social Affairs (March 2012), http://esa.un.org/unpd/wpp/ppt/CSIS/WUP_2011_CSIS_4.pdf.

[32] Nate Berg, *The Uneven Future of Urbanization* (April 9, 2012), http://www.citylab.com/housing/2012/04/uneven-future-urbanization/1707/.

[33] http://www.nist.gov/cps/sagc.cfm

Smart Buildings PPP: The smart building segment is predicted to be valued at almost $249 billion by 2025, with a CAGR of 4.1 percent (2012-25).[34] The U.S. government owns or manages more than 900,000 buildings or other structures across the country making it the nation's largest landlord. Smart building examples could include, but are not limited to, Smart Government Buildings enabling "smart energy" (HVAC) management, water flow and usage, predictive maintenance/mechanical operations and building security, and smart military bases facilitating the integration of systems and logistics for "smart" traffic flow, people flow, air quality, retail commerce operations, personnel safety and parking.

Impact **–** The proposed PPP would help the U.S. save on energy expenses while reducing carbon pollution. The U.S. government – and thus U.S. taxpayers – would realize direct (and possibly significant) economic savings due to improved efficiency in consumption, distribution, and management of energy and utilities across federal government buildings and installations. The PPP also would provide insight into savings opportunities and consumption planning for other federal properties, as well as state and local government properties. In addition, the PPP would introduce new business models that could increase efficiencies and offer new revenue streams for building owners in the public and commercial sectors, while improving services for building tenants and residents.

Approach – Consistent with the goals of the Better Buildings Challenge, to realize building energy savings of 20 percent or more over 10 years[35] and other current initiatives, this proposed PPP would leverage private sector IoT expertise in "Smart Building" IoT solutions to accelerate the U.S. government efforts to improve operational efficiencies across federal buildings and/or military installations. Imagine if we set a national goal for 25 percent of Federal Government buildings to be retrofitted with IoT solutions in three years, and 50 percent to be retrofitted with IoT solutions in five years, to increase energy efficiency by a minimum of 20 percent. Upfront funding for the PPP would be shared across public and private sector partners, and could range from in-kind to matching funds to purely financial investments. Benefits from the PPP also would be shared among public and private sector partners over the short- and long-term, ensuring PPP viability and creating a win-win scenario. One possibility in this case could be for public and private partners to share in the federal building/installation's energy and utility savings. For example, if the PPP were to reduce a department's energy and utility expenses by 20 percent, the U.S. government could allocate 10 percent of that savings to the private partners over a specified period of time until the private partners recoup their upfront investment plus some incremental percent of return, and the U.S. government (U.S. taxpayers) would retain the

[34] Frost & Sullivan.

[35] Administration Announces 14 Initial Partners in the Better Buildings Challenge, White House (June 30, 2011), http://www.whitehouse.gov/the-press-office/2011/06/30/obama-administration-announces-14-initial-partners-better-buildings-chal.

remaining 10 percent of the savings. After which time, the U.S. government would retain 100 percent of the energy and utility savings benefit.

CONCLUSION

Intel appreciates the opportunity to share our perspective on the enormous opportunity of the IoT and a proposed strategy for U.S. leadership in the next evolution of computing.