May 27, 2016

National Telecommunications and Information Administration
U.S. Department of Commerce
Attn: IOT RFC 2016
Iotrfc2016@ntia.doc.gov

Comments from Infineon Technologies Americas Corp. on The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things

As a leading producer of Internet of Things (IoT) technology, Infineon Technologies Americas Corp. welcomes the opportunity to provide information to the Department of Commerce defining the opportunity and challenges in establishing a robust market for IoT devices and systems. Infineon's expertise in developing innovative semiconductor products that enable IoT devices, and our broad reach across many market sectors from industrial manufacturing to automobiles to consumer devices, offers unique insight into the challenges and opportunities offered by IoT technologies.

Definition and Impact of IoT

The "Internet of Things" (IoT) is a network of cyber-physical objects that contain embedded electronics to sense, compute, actuate and communicate.

IoT has the potential to radically impact the way businesses and consumers interact with each other and their surrounding infrastructure. It connects the physical world with the virtual world as never before.

IoT technology promises to add new value to our society and to the economy. IoT devices and systems will facilitate autonomous driving, smart manufacturing, smart cities, wearables and smart health care. By 2025, researchers and industry experts envision the IoT to connect seven billion people and 80 billion IoT devices, generating annual economic value of more than six trillion dollars.

1.c. What are the most significant new opportunities and/or benefits created by IoT, be they technological, policy, or economic?

IoT is one of the most important technology trends of our time – with the potential to radically impact the way businesses and consumers interact with each other and their surrounding infrastructure. It connects the physical world with the virtual world as never before.

Market sectors based on IoT technology promise to add new value to our society and to the economy.

The impact of the IoT reaches beyond economic growth and new jobs. IoT can also help address pressing social and global challenges, including demographic shifts, resource scarcity, and climate change. Senior citizens can enjoy living longer in their homes with greater mobility provided by smart homes and autonomous vehicles. Greater resource efficiency through smart manufacturing and data driven markets will reduce energy usage, reduce materials usage, decrease emissions and reduce manufacturing costs.

Specifically, Infineon sees the following market sectors having a substantial impact on safety, reliability, efficiency, convenience and quality in manufacturing, infrastructure and transportation.

Smart Industry

Smart manufacturing with real-time connectivity of value chains provides significant benefits such as

- Shorter product development cycles and reduced time-to-market;
- Faster adaptation to demand changes;
- Optimization of production processes with regard to energy and resource efficiency;
- Higher productivity through optimal capacity utilization; and
- Improved quality and reliability of products.

Infineon itself is an early adopter of the emerging industrial internet, or IoT for industry. Through its own operations, and its participation in organizations like the Industrial Internet Consortium and Industrie 4.0, Infineon has identified not only the key benefits of smart manufacturing, but also the critical security risks and solutions for smart manufacturing.

Smart Cities and Energy

Semiconductors are key enablers for smarter, more energy efficient and more secure infrastructure in the transition to smart cities. The IoT-enabled infrastructure of smart cities will rely on both embedded systems intelligence from chips and modern information and communications technologies (ICT).

Although modern ICT has the potential to considerably reduce overall emissions by enabling new environmentally friendly solutions such as smart vehicles, smart buildings and smart factories, as the IoT becomes ubiquitous, ICT providers will be challenged to support rising data volumes, higher transmission speeds and increased data storage/processing capabilities. Leading-edge power semiconductors will enable industry-leading PUE (power usage efficiency) and DCIE (data center infrastructure efficiency) to mitigate these challenges.

Some examples of semiconductor enabled IoT devices and systems for smart cities include:

- smart lighting systems enabled by state-of-the-art LED technologies;
- smart infrastructure and transportation systems enabled by environmental sensors and microcontrollers;
- smart and secure building technologies; and
- power-efficient generation, storage, management and distribution of energy.

Smart Automotive

Connected Cars are one of the most recognized applications of the emerging IoT market. Connectivity to and between automobiles offers extraordinary potential benefits including:

- increased driving safety;
- improved vehicle operating efficiency;
- higher utilization of roadways infrastructure;
- reduced costs of vehicle recalls/upgrades;
- new convenience possibilities.

IoT-Automotive offers tremendous benefits to society and a multitude of new business opportunities. The challenge is that with increased connectivity and capabilities of advanced driver assistance technologies comes increased security risk. For automotive, the risks include misuse of data, theft of data, and the possibility of injury or death from remote access to vehicle systems and transportation infrastructure.

2. What definition should we use in examining the IoT landscape and why?

The "Internet of Things" (IoT) is a network of cyber-physical objects that contain embedded electronics to sense, compute, actuate and communicate.

Infineon proposes this technical definition because it describes the connections between the physical and virtual worlds, and defines the actions are required to create the value proposition of the Internet of Things, From the IoT network will a new means of multilateral and intelligent communication be established that can create efficiencies, solve social issues, and create new economic opportunity.

3.a. With respect to current or planned laws, regulations, and/or policies that apply to IoT, are there examples that foster IoT development and deployment while also providing an appropriate level of protection to workers, consumers, patients, and other users of IoT technologies?

The National Highway Traffic Safety Administration has a rulemaking underway that would require all vehicles after a certain date to contain vehicle to vehicle (V2V) communication technology, and likewise to protect that communication system with a secure credentialing management system. This rule would push the market for connected cars forward by mandating capability, but not use, of IoT technology. The proposed rule also requires security for the communications system. Automakers can then choose to enable V2V applications on a voluntary basis.

5. Please provide information on any initiatives or research of significance that have examined or made important strides in understanding the IoT policy landscape?

The European Semiconductor Industry Association is one sector that recently provided IoT policy recommendations to the European Union's call for policy recommendations on the Internet of Things. http://www.eusemiconductors.eu/images/static_website/PublicPolicy/Comp_Innovation/ESIA_IoT_PositionPaper2016.pdf

IoT policy is one element of a larger digital market initiative undertaken by the EU, and that initiative includes some preliminary thinking on IoT principles: Press release: Commission sets out path to digitise European industry: http://europa.eu/rapid/press-release_IP-16-1407_en.htm

6.a. What technological issues may hinder the development of IoT, if any?

From a technical perspective, IoT business models across industries rely on gathering data from many IoT devices, analyzing that data, and acting on that data. Sustainable IoT success hinges on making the anticipated billions of IoT devices smart, secure, power-efficient and interoperable.

- **Smart –** Individual IoT devices equipped with semiconductors, such as sensors, processors, actuators and security controllers, must be enabled to deliver the desired data and to take actions as needed.
- **Secure –** Strong security is vital to build trust in the IoT among both businesses and citizens/consumers. Sensitive data must be protected, authentication and authorization must be verified, and device/equipment integrity must be monitored in order to prevent data theft, fraud, and physical and economic damage to IoT enabled systems.
- **Power-efficient –** Power drives IoT devices, allowing them to sense, process, communicate, and act. Power-efficiency is critical to miniaturization of the systems, thus making possible the use of IoT applications everywhere. Connectivity is a substantial power drain to devices. The power needed for wide-scale device connectivity must be produced, managed and delivered in the most energy-efficient way possible, and the performance of all these networked devices must be optimized. A new generation of power semiconductors combined with new packaging technology and digital controller ICs is going to enable the IoT vision.
- **Interoperable -** Interoperability and common standards along the IoT value chain are essential – within an application segment, across different application segments, and across regions. Without interoperability, data will remain fragmented and the promise of IoT cannot be fulfilled.

6.b. What can the government do to mitigate these technical issues? Where may government/private sector partnership be beneficial?

At this early stage in the evolution of the IoT, policymakers should exercise caution in the development of regulations that might restrict innovation in new products and services that promise efficiency and convenience benefits to individuals, government, and industry. At the same time, industry and government together must be vigilant in identifying potential risks to privacy, safety, and health for the emerging IoT devices and systems, as these risks may inhibit the adoption of IoT and thereby restrict innovation. Preventing harm to individuals, organizations and government institutions demands a high level of attention to designing security into IoT devices and systems.

Established security frameworks in critical infrastructure and regulated industries should be reviewed and updated to address IoT security challenges. Industries that have successfully developed cyber security frameworks are natural leaders in the development and implementation of security best practices in the IoT transformation. For example, the aviation and financial services industries have long faced persistent attacks with high consequences. In response, they have developed strong cyber security measures.

Security is fundamental to public trust in IoT products and services, and the benefits of the IoT will not be realized without that trust. Existing and novel security devices and systems are being deployed in some leading IoT applications like connected cars, and slot machines. Key elements of establishing public trust are standardization and certifications for secure IoT applications. Organizations such as UL (previously known as Underwriters Laboratories) can be a model for establishing standards, certification practices, and metrics for cybersecurity.

Today, multiple private groups are coalescing around the challenge of establishing standards for the IoT, including both new consortia and long established organizations such as the Institute of Electrical and Electronics Engineers and UL. Standards organizations are providing guidelines and best practices for device and system security to drive better implementations of IoT in various markets. Nearly all industry consortia recognize the critical role security plays in providing privacy, reliability and safety. And while there have been no public announcements from liability insurers, the insurance industry is present and participating in the discussions within those standards groups.

16.a. What are the cybersecurity concerns raised specifically by IoT/ How are they different from other cybersecurity concerns?

Widespread adoption of IoT technologies means that cybersecurity now has a much greater impact in the physical world. Because cybersecurity is asymmetric, a weak attacker can cause disproportionate damage. With IoT, this disproportionate level of damage can extend into the physical world.

The type and magnitude of risk associated with IoT cybersecurity varies substantially depending on the application – smart home, manufacturing, chemical, utilities, automotive, etc. Injection of fake commands into an IoT system can be an annoyance to a homeowner, cause monetary loss to a manufacturing company, damage critical infrastructure and dependent systems, or even cause injury or death.

Because of this widely varying impact, there cannot be a one-size-fits-all approach to cybersecurity. Instead, a risk-based approach must be used. For high-risk applications, strong security must be used. For lower-risk applications, lesser measures may be employed. Fortunately, cybersecurity defenses that have been developed for information systems can be readily adapted for IoT, at least initially. Software-only approaches are suitable for low risk applications while the use of robust hardware-based security can resist even determined attackers that have access to sophisticated resources.

As we have shown, neither risk nor security is binary. Therefore, objective metrics must be established for cybersecurity risks and countermeasures. One good example of such metrics is the four levels of authentication assurance established in NIST SP 800-63. These levels are widely cited and used throughout information security. NIST should focus on establishing similar levels for IoT risk and security.

Specifically for smart manufacturing:

> Protecting investments, including Intellectual Property, and ensuring the effective operation of a smart manufacturing site requires dedicated security solutions. These security solutions vary for different levels of the industrial automation architecture, and for different forms of communications infrastructure between those levels. In today's world of industrial IoT, the supervisor level and the control level may be hosted in the cloud. This creates a need for secure Internet communications between all levels of the industrial automation architecture, from supervisor level, to control level, and finally to field level. Further complicating the security requirements, these communications can take place over public or private networks which may be wired or wireless. Each of these architectural alternatives will drive the need for specific and unique security requirements. Semiconductors are the foundation for enabling specific system performance and security criteria specifications. Secure chips create the root of trust for connected components, systems, and solutions in smart manufacturing.
>
> A secure (and in many cases certified) trust anchor is the first step along the IoT value chain to build systems that protect the availability of data, the integrity of processed data, and the confidentiality of data. Secure chips enable secure communication across companies, across countries and across industries through the encryption of sensitive data. Secure chips foster secure identification of connected components, objects, systems and persons. This could mean, for example, mutual authentication of authorized connected devices, authorized cyber physical systems and authorized operators.
>
> New industry standards are essential. For the generation of data, the combination of sensors with secure anchors functioning as roots of trust will be needed in the near future. With this approach, a new class of industry standards in the sensor area is needed. For the hyper-connected world of smart manufacturing, other new standards like ISO/IEC 62443, which combines security and safety in industrial internet, are necessary.

Specifically, for automotive,

> IoT-Automotive offers tremendous benefits to society and a multitude of new business opportunities. The challenge is that with increased connectivity and capabilities of advanced driver assistance technologies comes increased security risk. For automotive, the risks include misuse of data, theft of data, and the possibility of injury or death from remote access to vehicle systems and transportation infrastructure.
>
> Industry best practices, policy guidelines and technical standards are needed:
>
> - To ensure interoperability of devices and systems in connected vehicles;
> - To ensure that adequate security measures are installed which offer protection throughout the vehicle lifetime;
> - To establish a means to rate the security protections included in new vehicles.

16.c. What role or actions should the Department of Commerce, and more generally the federal government, take regarding policies, rules, and/or standards with regards to cybersecurity, if any?

Addressing cybersecurity in IoT devices and systems will be critical to the continued innovation this technology trend promises. Without security by design, the IoT will not be fully realized. The government can exercise its convening authority to bring private sector experts together with policymakers to define security principles for IoT, facilitate IoT security framework development by sector and application, and encourage the implementation of best practices and/or minimum standards.

20.a. What factors should the Department consider in its international engagement in standards and specification organizations?

Interoperability and mutual recognition of standards will be critical to creating a successful global market for the IoT.

26. What role should the Department of Commerce play within the federal government in helping to address the challenges and opportunities of IoT? How can the DoC best collaborate with stakeholders on IoT matters?

The Department of Commerce must continue to be an energetic advocate for innovation and the opportunity potential of the IoT. It must bring together stakeholders in government and the private sector to define risks to realizing the potential, and subsequently facilitate the deployment of standards to mitigate against those risks.