SEMICONDUCTOR INDUSTRY ASSOCIATION

Comments of the
Semiconductor Industry Association (SIA)
On the
NTIA's Request for Comments on
"The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things"

81 Fed. Reg. 19956 (April 6, 2016)

Submitted to iotrfc2016@ntia.doc.gov
June 1, 2016

The Semiconductor Industry Association (SIA) is pleased to submit these comments in response to the NTIA's request for comments on information on "The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things." 81 Fed. Reg. 19956 (April 6, 2016). SIA is the trade association representing leading U.S. companies engaged in the design and manufacture of semiconductors. More information about SIA is available at www.semiconductors.org.

SIA congratulates the NTIA for seeking input on public policies to advance the Internet of Things (IoT). Semiconductors are the fundamental enabling technology of modern electronics, including the IoT. All IoT devices will require semiconductors such as microcontrollers, sensors, and memory to connect to each other and perform their intended function, and the infrastructure to connect all of these added devices will also rely on continued innovations in semiconductor technology. In short, the promise of the IoT to transform our economy will be based, in large part, on the ability of the semiconductor industry to provide high performing and efficient semiconductors that can connect billions of smart devices across government, industry and the consumer marketplace and result in dramatic benefits for the industrial, retail, health care, transportation, and other sectors of the society.

SIA provides the following comments on several of the questions posed by NTIA:

> *3. With respect to current or planned laws, regulations, and/or policies that apply to IoT: a. Are there examples that, in your view, foster IoT development and deployment, while also providing an appropriate level of protection to workers, consumers, patients, and/or other users of IoT technologies? b. Are there examples that, in your view, unnecessarily inhibit IoT development and deployment?*

The U.S. government should work with industry to establish a long-term national strategy that will enable America to lead the world in IoT. To maximize the potential of the U.S. IoT ecosystem, our public policy framework must encourage the development of a robust IoT ecosystem that promotes key capabilities, including connectivity and interoperability, scalability and security, and complex intelligent analytics.

To accelerate and maintain the long term viability of the IoT, our policy framework should encourage solutions based on horizontal building blocks and an open architecture framework, one that is scalable, interoperable, and reusable across deployments, vendors, and sectors. Our nation's public policy framework also should contemplate tools to accelerate IoT adoption and enable cost-effective introduction of new technologies, including open standards efforts, targeted federal funding, and impactful public-private partnerships. With these fundamental building blocks of a successful IoT ecosystem, policymakers will enable the proliferation of IoT technologies across markets and help our nation realize the significant economic and societal benefits that the IoT can deliver.

One example of planned legislation that would foster development of the IoT is the Developing Innovation and Growing the Internet of Things (DIGIT) Act, S.2607 and H.R. 5117. These bipartisan, companion versions of the DIGIT Act, would require the Secretary of Commerce to convene a working group Federal Government to consult with nongovernmental entities and provide recommendations and a report to Congress on how to plan for and encourage the proliferation of the IoT in the United States for the growing number of connected and interconnected devices.

> *6. What technological issues may hinder the development of IoT, if any? a. Examples of possible technical issues could include: i. Interoperability ii. Insufficient/contradictory/proprietary standards/platforms iii. Spectrum availability and potential congestion/interference iv. Availability of network infrastructure v. Other b. What can the government do, if anything, to help mitigate these technical issues? Where may government/private sector partnership be beneficial?*

Technological issues that will hinder IoT include lack of interoperability and industry-driven global standards (vs. proprietary solutions and/or country-specific standards), lack of *scalable* test beds (these should not be one-offs that cannot be increased in size or repeated) and lack of spectrum sharing (especially below 6 GHz) to enable increased spectrum availability.

Government and industry collaboration can be one of our nation's best assets to accelerate the adoption of a world-class IoT ecosystem that successfully supports virtually every sector, including industrial, transportation, health care, and retail sectors. Viable public-private partnerships will make IoT deployments an appealing investment for government and industry, as well as ensure scalability and sustainability of infrastructure and technological innovation over the long term. Government and industry should work together to promote a business environment that motivates private investment and innovation – including the protection of commercial and proprietary data from misuse by competitors and third parties.

Public-private partnerships should leverage existing industry standards and investments and utilize both public and private resources in order to facilitate the research, leadership, and governance to advance our nation's IoT vision. Federal funding may be appropriate in certain targeted situations to incentivize more rapid development and deployment of our nation's IoT ecosystem or to provide more timely and effective capabilities to meet government mission needs.

In 2015, SIA partnered with the Semiconductor Research Corporation (SRC) and the National Science Foundation (NSF) on a workshop to identify the research needs for future computing, including specifically IoT, and the results of this effort are summarized in a report, *Rebooting the IT Revolution: A Call for Action* (September 2015).[1] We already are seeing advancement in several of the research recommendations set forth in the report that pertain to the IoT.

- Energy-efficient sensing and computing

In order to realize the full benefits of the IoT, the U.S. would benefit from additional research to improve the energy efficiency of semiconductors at all levels, from the smallest sensor to ultra-high performance processors. Sensor nodes will often need to operate without access to the electric grid for power, by using battery power or harvesting energy from the environment. Advanced processors are already being developed with novel materials, devices, and computational and physical architectures that reduce the energy used to collect, move, analyze, and store data.

- Intelligent storage

Given the projected explosion in data from the IoT, semiconductor companies are developing sophisticated secure, interoperable and scalable IoT platforms, new memory technologies and improved management systems to store and archive this data in order to maximize its use and action-ability.

- Redundant and Multi-level security solutions

The semiconductor industry recognizes that security is a foundation for the IoT and continues to improve its multi-level security solutions -- including dedicated security products and security features embedded into both our hardware and software products. Indeed, hardware and software are being designed from the beginning to be secure. Increased and dynamic security solutions are being built into hardware at the transistor level as well as software, from the smallest microcontroller at the edge of the network to the most advanced server in the cloud and all gateways and devices in between. The semiconductor industry prioritizes security, accuracy, privacy and integrity of data in all market sectors, especially in the industrial domain where the safeguarding of critical infrastructure can be vital to economic and social stability. These hardware- and software- level security capabilities will create redundancies to prevent intrusions and enable a robust, secure, trusted IoT end-to-end solution.

[1] This report is available at: http://www.semiconductors.org/clientuploads/directory/DocumentSIA/Research%20and%20Technology/RITR%20WEB%20version%20FINAL%201.pdf.

The semiconductor industry, in conjunction with the National Science Foundation (NSF), is researching these topics via the Secure, Trustworthy, Assured and Resilient Semiconductors and Systems (STARSS) program. The U.S. would benefit from increased funding for this important effort, which is currently only funded at $3 million per year.[2]

- Next-generation manufacturing paradigm

In order to produce the billions of very small, high-performance, low-power, low-cost sensors needed to drive the IoT, new manufacturing processes need to be developed. Additional fundamental research in materials, fabrication, assembly, and packaging would be beneficial. This would further enable new IT hardware – from the smallest sensor node to ultrahigh performance processors. Developing new processes such as rapid three-dimensional additive manufacturing would be significant, and over the longer term, the convergence of semiconductor technology and biology offers increasing possibilities for disruptive new designs and processes.

- IoT test platform

As stated in the SIA/SRC "Rebooting" report, a test platform "to adequately model the bourgeoning complexity of the IoT would be an important step forward. Without such a test platform, solution verification and benchmarking is not possible. Such a platform should be accessible to researchers from academia, industry, and government."

Significant and coordinated research in these areas would help fully achieve the benefits of the IoT and generate long term economic and security benefits for the U.S. SIA calls on the Administration and Congress to work with the semiconductor industry to develop and fund such a comprehensive research program.

15. What are the main policy issues that affect or are affected by IoT? How should the government address or respond to these issues?

The approach of the federal government toward the IoT should be guided by the following principles:

- *Invest in basic research* – The federal government has a critical role in investing in research that will accelerate the adoption of the IoT in the U.S. and improve America's global competitiveness. Suggested areas for research investments, in conjunction with the semiconductor sector, are summarized above.

[2] NSF funds other hardware security research under their Secure and Trustworthy Cyberspace program. Also, other agencies are funding R&D aimed at ensuring US government access to secure electronic components. For example, the Defense Advanced Research Projects Agency (DARPA) manages the SHIELD program on anti-counterfeit taggants and the Intelligence Advanced Research Projects Activity (IARPA) manages the Trusted IC program on split manufacturing.

- *Promote the adoption of IoT* – The government should act to promote the adoption of IoT solutions and avoid hampering innovation in this emerging set of technologies. Policymakers should proceed cautiously in attempting to legislate or regulate the IoT. There is a risk that ill-conceived actions or unintended consequences could hamper adoption of the IoT in the U.S. On the other hand, removing regulatory barriers would hasten its adoption. For example, a device or accessory to a smartphone should not be subject to regulation as a "medical device" simply because it might play some role in health monitoring. Similarly, policies encouraging private sector testing of autonomous vehicles on public roads would help facilitate the emergence of the IoT and enable U.S. leadership in that field.

- *Enable connectivity and interoperability* – The government should act to enable connectivity and interoperability among devices. Without seamless interoperability, the promise of the IoT will not be realized.

- *Leverage industry standards* – The government should promote global voluntary industry-driven standards and best practices. The private sector has the expertise to develop consensus-based standards that will promote competition and continued innovation.

- *Facilitate the deployment of ubiquitous broadband* – In order to enable and maintain U.S. leadership in the IoT, the government should facilitate the development and availability of ubiquitous, affordable, high-speed broadband connections for advanced cellular technologies like 5G and advanced wireless technologies like next-generation WiFi.

  16. How should the government address or respond to cybersecurity concerns about IoT? a. What are the cybersecurity concerns raised specifically by IoT? How are they different from other cybersecurity concerns? b. How do these concerns change based on the categorization of IoT applications (e.g., based on categories for Question 4, or consumer vs. industrial)?

In addressing cybersecurity topics related to IoT, the U.S. would benefit from additional government funding to research security across the entire network, including security research for semiconductors. As stated above, one of the research topics identified by SIA is additional redundant and multi-level security research. Semiconductor companies will play a major role in providing end-to-end IoT security, such as by providing on-chip security at the transistor level, enabling IoT device security; enabling communications and process control security; partitioning processor functions on chip, or supplying comprehensive hardware and software services, including authentication, data encryption, and access management.[3]

[3] Global Semiconductor Alliance and McKinsey & Company (2015), "The Internet of Things: Opportunities and Challenges for Semiconductor Companies", http://www.gsaglobal.org/wp-content/uploads/2015/05/1.-GSA-McK_Report-IoT_Text_Executive-Summary.pdf.

IoT introduces a distinct information processing hierarchy whereby computing is distributed among clients (smart phones/tablets), central nodes (cloud), gateways (fog) and edge nodes (mist) containing sensor/actuator interfaces. Each has unique attributes with respect to size, cost, energy consumption, processing power, memory capacity, communication interfaces, and security. This distributed environment can host applications mapped across its spectrum in a multitude of ways. SIA members are focused on a holistic approach to IoT security that encompasses the entire chain of computing devices that support end-to-end applications enabled by the emergence of IoT.

+ \+ \+

SIA appreciates the opportunity to submit these comments.