**Department of Commerce**
**National Telecommunications and Information Administration**
**Further Request for Comments**
**Green Paper: Fostering the Advancement of the Internet of Things**
**Docket No. 170105023-7023-01**

On behalf of the Information Technology Industry Council, we commend the Department of Commerce, the National Telecommunications and Information Administration, the Internet Policy Task Force, and the Digital Economy Leadership Team for the release of the recent Green Paper: Fostering the Advancement of the Internet of Things.[1] This comprehensive effort captures the wide range of benefits the Internet of Things (IoT) will have on the U.S. economy, the range of policy issues that will impact IoT development, investment, and deployment, as well as an overview of what is currently occurring across the federal government. ITI believes this Green Paper, as well as the Department of Commerce's historic leadership on many of the policy issues that will allow the IoT to reach its full potential, demonstrate the pivotal role the Department can hold as the IoT grows and matures; ITI supports the role identified in the Green Paper.[2]

## Definition

While the Green Paper notes there was no consensus on a formal definition for the IoT,[3] ITI would encourage the Department to consider defining one to ensure all stakeholders engaging the Department and other government entities are speaking the same language. At its simplest, the IoT is: "Things" (devices) securely connected through a network to the cloud (datacenter), from which data can be extracted, shared and analyzed to create value (solve problems). The IoT enables the connection of "things" like phones, appliances, machinery and cars to the Internet, integrating greater computing capabilities to share and analyze the data

[1] Green Paper: Fostering the Internet of Things; National Telecommunications and Information Administration January 12, 2017 ("Green Paper").
[2] Green Paper, pp. 2-3, 10-14.
[3] Green Paper, pp. 5-8.

generated by these things, and extract meaningful insights that enable new opportunities and solve problems. These opportunities have 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" connects devices like household appliances, wearables and smart phones. The "Industrial IoT" connects devices in industrial environments like factory equipment, building systems and digital signage.

**Promotion of Global, voluntary, open industry-led standards**

ITI whole-heartedly supports the Green Paper's strong promotion of global, voluntary, industry-led standards.[4] ITI member companies participate in many standards development organizations; just several of those with broad membership, driving global IoT standards and interoperability are:

- Industrial Internet Consortium – The IIC is a global, member supported organization that promotes the accelerated growth of the Industrial Internet of Things 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.[5]
- Open Connectivity Foundation –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.[6]

[4] Green Paper, pp. 44-48.
[5] For more information, see http://www.iiconsortium.org
[6] For more information, see https://openconnectivity.org

- Open Fog Consortium - 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.[7]

Many of the existing foundational elements that drove the development, evolution, and investment in the Internet ecosystem will be necessary to fully realize the potential of the IoT. Promotion, support and adoption of global, consensus-based standards is critical for providing the interoperability necessary for the IoT to thrive.

**Cybersecurity**

Since the initial request for comment, there has been significant activity across the federal government and in Congress on cybersecurity in the IoT. Several of those are captured in the Green Paper, and ITI would specifically commend the multi-stakeholder approach both endorsed in the Green Paper[8], and carried out in practice by NTIA through such efforts as the Multistakeholder Process for IoT Security Upgradability and Patching.[9] The tech industry constantly works to stay ahead of threats, not only through its own solutions but also in partnership with the Federal Government. The IT industry leads and contributes to a range of significant public-private partnership activities, including:

- National Institute of Standards & Technology (NIST) Cyber-Physical Systems Working Group on security and privacy;
- National Institute of Standards & Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity;
- National Telecommunications & Information Administration (NTIA) Multi-stakeholder process on IoT patching;

[7] For more information, see https://www.openfogconsortium.org/about-us/
[8] Green Paper, pp. 41, 43, 57.
[9] See https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security

- Department of Homeland Security (DHS) IoT security principles;
- DoD-Defense Industrial Base (DIB) Cybersecurity (CS) Information Sharing Program;
- Information Technology Information Sharing and Analysis Center (IT-ISAC); and
- Sector Coordinating Councils (SCCs).

As the Green Paper properly notes, policymakers and regulators 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. Through oversight, policymakers should also endeavor to better coordinate the many IoT security related policy efforts currently in progress across the Administration. Furthermore, Congress and certain federal agencies can encourage the use of high-level, cybersecurity best practices that incentivize good cyber behavior. For example, the Small Business Administration has established programs to educate small and medium-sized business owners (SMBs) about cybersecurity, provide resources to assess information security resilience, and create customized cybersecurity plans. 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. Thus, SMBs will not only implement better cybersecurity practices, but also contribute to more secure supply chains for large businesses and the Federal Government. Similarly, the Federal Trade Commission continuously provides and updates information to, and for consumers to improve their online security practices, and information on securing connected devices in the IoT.

**Privacy**

Given the projected exponential growth in the number of IoT devices that will produce, analyze, or transmit data, it is not surprising that questions were raised in initial responses around data privacy. ITI would like to agree with the comments of several others in first pointing out that a significant amount of IoT data will often have no connection to a person or individual; for

instance, industrial or commercial IoT applications will largely be used for diagnostic, logistic, or other performance-related purposes.[10] Further, it is worth noting data that is de-identified or anonymized and aggregated do not raise the same privacy concerns as other collections and uses of data.

ITI agrees with and would like to reiterate the sentiments identified in the Green Paper which stressed that many of the privacy issues arising in the IoT context are nonetheless not new, as IoT applications where data on individuals is collected, the collection, use, sharing, and protection of such data are already subject to existing laws.[11] For instance, IoT consumer products fall within the jurisdiction of the Federal Trade Commission (FTC) and are thus subject to its unfair or deceptive acts or practices authority under Section 5 of the Federal Trade Commission Act. Grounded in Fair Information Practices Principles (FIPPs), the FTC's approach to privacy helped enable the Internet to thrive and, as a consequence, ITI companies have been able to offer an expanding range of services and applications (including IoT devices), often times free or at a nominal expense to consumers. While all FIPPs protections may not be applicable in all instances and flexibility may be necessary for certain IoT applications,[12] the FTC has the expertise and authority to oversee privacy matters for consumer IoT devices.

**Additional Activity**

ITI strongly supports the development of a National IoT Strategy, and is hopeful Congress will advance, and the President will sign, S. 88, the "Developing Innovation and Growing the Internet of Things Act" or "DIGIT Act". This bill will direct the Department to lead interagency coordination for federal government IoT activity, by creating a working group of government, industry, and other external stakeholders. The working group will be responsible for providing Congress with recommendations for government action to advance the IoT in the U.S., as well as commencing a public comment process on spectrum needs for IoT. ITI views this as

[10] Green Paper pp. 7, 30
[11] Green Paper, p. 31.
[12] See ITI comments to FTC, in *In the Matter of the Internet of Things*; FTC Project No. P135405; January 9, 2014.

complementary to the Green Paper, and a critical step in the development of a National IoT Strategy.

**Conclusion**

Again, ITI appreciates the Department of Commerce and NTIA's leadership on IoT. We stand ready to continue working with the Department to ensure the U.S. federal government has policies in place that will promote investment, development, and adoption of IoT, thereby harnessing the multitude of benefits discussed in the Green Paper and initial comments.

Respectfully submitted,

J. Vince Jesaitis
Vice President, Government Affairs
ITI - Information Technology Industry Council
1101 K Street NW, Suite 610
Washington, DC 20005
202-737-8888
www.itic.org

March 13, 2017