Additional Questions for the Record

Internet of Things Legislation
Before the Subcommittee on Digital Commerce and Consumer Protection
The House Committee on Energy and Commerce

Michelle Richardson, Deputy Director
Freedom, Security, and Technology Project, Center for Democracy and Technology
Submitted July 11, 2018

The Honorable Robert E. Latta

1. In your testimony you state that government should take a soft touch approach to regulating in the technology space, especially when the technology is still developing. Can you explain why a soft touch approach is important?

> Answer: The characteristics that have made the Internet such a success—its open, decentralized, and user-controlled nature and its support for innovation and free expression—may be put at risk by heavy-handed government mandates on the private sector. This is not to suggest that government has no role in shaping the development of the Internet of Things (IoT), but only that it take a nuanced and thoughtful approach in consideration of the diverse entities, services and devices that make up the IoT.

Ideally, IoT developers will adopt privacy and security practices that fairly balance their interests with those of users, and as we testified, we believe this bill would be greatly strengthened by an amendment to ensure that the Secretary investigates the *adoption* of these practices. The nuanced and thoughtful government approach we endorse must start with an understanding of the security and privacy realities of the IoT ecosystem.

2. You state in your testimony that compiling a list of industry-standard setting efforts and government activities that will be created by the SMART IoT Act will help inform future congressional action. Why do you believe gathering such information is critical for future IoT policy?

> Answer: The review conducted under the SMART IoT Act will likely return an extensive list of IoT standards that range from highly technical interoperability requirements to generically desirable privacy and security outcomes. We recommend that Congress focus on culling this list to create minimum privacy and security standards for government procurement of IoT devices. This is the logical next step to implement guidance developed by the Departments of Commerce and Homeland Security, the Office of Management and Budget, and the General Services Administration. It is also timely given the administration's efforts at IT modernization and the expected purchases agencies should be making in the near future. While there are competing, but justified views on government intervention in the private sector, it should be non-controversial

that the government needs to secure its own systems and devices. To accomplish this goal, the government must be able to set the minimum privacy and security standards for the IoT devices it purchases.

We also recommend that the SMART IoT Act review be the jumping off point for more oversight of consumer grade IoT devices. Much of IoT is arguably in the purview of agencies who regulate critical infrastructure, transportation and medical devices, but consumer devices are falling through the cracks of our current sectoral approach.

The Honorable Michael C. Burgess

1. Sector-based Information Sharing and Analysis Centers (ISAC) have been successful in coordinating information sharing between private sector critical infrastructures and the government. These ISACs help industry protect from cyber and physical threats, as well as coordinate responses with government, when appropriate.

a. Will the study on the internet-connected devices industry evaluate the feasibility of establishing an Internet of Things ISAC?

Answer: The SMART IoT Act draft dated May 15, will not evaluate the feasibility of establishing an Internet of Things ISAC.

b. Would it be appropriate to recognize the Internet of Things environment as critical infrastructure? If so, what barriers currently exist?

Answer: Critical infrastructure is defined as:

systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.[1]

We do not recommend that the IoT sector be designated as a stand-alone sector. By and large, compromises of IoT devices do not pose the catastrophic effects as contemplated by the standard CI designation. Additionally, IoT devices increasingly pervade most existing CI sectors and to the extent they do, they may be considered within the oversight and regulatory authorities of the sector specific agency already. We expect that the list of government oversight activities in Sections 2(a)(2)-(6) in the SMART IoT Act will include such CI routes to IoT oversight and regulation.

[1] 42 U.S.C. § 5195c.

If the designation is under consideration solely or primarily to permit the creation of an ISAC, we note that nothing legally prohibits IoT manufacturers or operators from sharing a lot of information with one another or with the government through more informal means. ISACs are only useful if the participants respond to the unique information they provide. Considering that a significant number of consumer IoT manufacturers use hard coded passwords, fail to offer patches for publicly known security flaws, and/or abandon devices after a short period of time, it is unlikely that many IoT manufacturers would be meaningful participants in an ISAC.

2. In the past few years, vulnerabilities in information technology systems and programs have led to large-scale cyber-attacks. Often devices and applications are produced and administered for government and public use by the same company.

a. Will the results of the study help determine the level of vulnerability in the current Internet of Things environment?

Answer: As drafted, the SMART IoT Act will only produce a list of standards, working groups, jurisdictions and similar data points. We recommend that the bill be amended to explicitly require an evaluation of whether these standards are being adopted by the private sector. This is no small task, but the committee could choose a few specific sectors to focus on, such as consumer devices. That would help determine the level of vulnerability of IoT devices in those sectors.

3. We understand that IoT applications and solutions promise to improve lives and offer societal benefits. Can you highlight current examples of how IoT is doing just that and any future applications you see as offering meaningful benefits?

Answer: CDT is excited to witness and participate in the technological evolution that is changing the world around us. But we believe the many benefits of the IoT will only be stymied by continued security and privacy failures and look forward to working with Congress to building an IoT system that people can trust.