Response of Intel's Dipti Vachani to Additional Questions for the Record

July 11, 2018

The Honorable Robert E. Latta

1. What obstacles do you currently see slowing the progress of IoT adoption and what can Congress do to promote continued innovation in this space?

At Intel, we believe one of the biggest obstacles – and ultimate drivers – for the IoT is scalability across sectors. The adoption of a meaningful National IoT Strategy by the federal government, in partnership with industry, can help address this obstacle and drive U.S. IoT competitiveness. The national strategy should declare IoT investment, innovation and competitiveness a U.S. priority and set forth an expeditious process and timeline for adoption of IoT technology across key market sectors. Intel believes that collaboration between government and industry is critical to address IoT scalability and expedite broader adoption of IoT solutions in America. Without a clear strategic vision, the U.S. risks falling behind other countries in reaping the vast economic and societal benefits of the IoT, along with the benefits that accrue from creating and owning the expertise driving the global IoT ecosystem. A national plan with concrete milestones will ensure that the U.S. leads the world – and increases GDP from the IoT – for decades to come. Moreover, coordination across government agencies is essential to prevent a patchwork of inconsistent policies which could disrupt IoT's transformative potential. The Secretary of Commerce's recommendations to Congress, pursuant to the SMART IOT Act, should provide the framework for working with industry to timely develop and adopt an impactful U.S. National IoT Strategy, including promoting *scalable* federal government IoT projects and investment aligned with agency missions that can highlight U.S leadership and demonstrate the benefits of IoT use cases.

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?

We concur with your assessment that ISACs have been successful in many instances in coordinating information sharing between private sector critical infrastructures and the government. Indeed, Intel and the technology industry contribute to significant cybersecurity public-private partnerships with the federal government, including information sharing, analysis, and emergency response. Examples include the DoD's Defense Industrial Base Cybersecurity Informational Sharing Program (cybersecurity information sharing and incident reporting); the Information Technology Information Sharing and Analysis Center (sharing of cybersecurity threats and insights); and DHS' Sector Coordinating Councils (coordination of critical infrastructure security and resilience).

The IoT study prescribed in the SMART IOT Act focuses on cataloguing industry stakeholders, including those who develop IoT devices, government agencies with jurisdiction over industry sectors engaged in IoT, a comprehensive list of public-private partnerships focused on IoT, industry bodies engaged in establishing regulations, guidelines and best practices that pertain to IoT. The collection of this data, along with the continued coordination and collaboration of the public and private sectors on federal IoT policy and adoption, is an appropriate first step when considering the feasibility of establishing an IoT ISAC or whether sector-specific ISACs similar to the examples above may be more actionable given the breadth of the IoT.

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

While some parts of the IoT are included in sectors defined as critical infrastructure, other are not. For example, both a smart thermostat in a home and the smart grid are considered part of the IoT environment, but only the latter is considered critical infrastructure by DHS.

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?

The SMART IOT Act directs the Secretary of Commerce to develop the IoT study and provide recommendations to Congress, among which could be laying the groundwork to help determine vulnerabilities should the Secretary recommend this. Most important in this effort,

the federal government should continue to initiate and support multi-stakeholder activities and working groups, collaborate with industry to understand evolving threats and continually develop best practices for IoT security.

The Department of Commerce and its agencies, such as the National Institute of Standards and Technology (NIST) and the National Telecommunications Industry Administration (NTIA), as well as the Department of Homeland Security (DHS), are appropriate entities for such efforts. Intel participated(es) in NIST's Cyber-Physical Systems Public Working Group including the cybersecurity subgroup, as well as NTIA's multi-stakeholder processes on Cybersecurity Vulnerabilities and IoT Security Upgradability and Patching. These are examples of public-private collaboration to address important security needs, while maintaining the necessary flexibility to adapt to new threats that rigid regulatory approaches would not provide.

Congress also should urge the Federal Trade Commission, Small Business Administration and Federal Communications Commission – with input from industry – to develop complementary cybersecurity "hygiene" education and awareness outreach initiatives for consumers and small businesses.

3. In your testimony you spoke about IoT and what it means for healthcare. As an OBGYN and Chairman of the Health Subcommittee, I am interested to learn more about Sickbay and what it is doing at Texas Children's Hospital. Can you talk a little bit about the health monitoring they are doing? I'm interested to hear how this is impacting patient care.

Intel shares your interest in the application of IoT technology to improve patient-centered care. IoT solution Sickbay, an FDA-cleared Clinical Intelligence Platform, is using Intel technology to enable real-time, data-driven medicine. The Sickbay platform continuously captures patients' bedside data from any medical device or system and transforms that data into web-based clinical applications that make data actionable – enabling patient care teams to make better, faster decisions. This allows medical teams to predict patient health deterioration before it occurs and ultimately save lives. The solution has been implemented at six healthcare institutions to date. Texas Children's Hospital pioneered the creation of a remote consult room that enables the viewing of real-time data from cardiac monitors and vents. Texas Children's Hospital has used Sickbay to collect data on 302 beds over 4.5 years, which included 2.1 million patients. More information is available on our website at: https://solutionsdirectory.intel.com/solutions-directory/sickbay-clinical-intelligence-platform.