Chairman John Thune
Written Questions for the Record to
Mr. Douglas Davis
"The Connected World: Examining the Internet of Things"
Senate Committee on Commerce, Science, and Transportation
Wednesday, February 11, 2015

Question 1 - Mr. Davis, Intel is opposed to FCC reclassification of broadband service under Title II of the Communications Act, a view that I share. Do you think that reclassification could harm growth of the Internet of Things? If so, how?

***Response*:** As a world leader in computing and communications technologies, Intel wants net neutrality rules that foster an open, accessible Internet *and* affordable, high quality broadband. Therefore, we support FCC rules regarding disclosure, blocking and discrimination. We filed Reply Comments in the FCC's Open Access proceeding opposing reclassification of broadband providers as utilities under Title II, because we believe it is not necessary and could discourage expensive and risky "last mile" broadband investment. Specifically, as to IoT, Intel wants both open *and* high-quality connectivity for all. With a projected 50 billion connected devices by 2020, investment in ubiquitous, faster and more affordable Internet connectivity will be even more critical. In that regard, we generally believe that "light touch" regulation promotes more broadband investment while still protecting open access, and thus we encourage the FCC to implement its Title II authority in a light touch manner.

Question 2 - Mr. Davis, these days, hacking and security concerns are seemingly always on the front pages. Data breaches have affected many millions of consumers and some of the largest corporations in this country. Consumers are right to be excited about the benefits of the Internet of Things to their lives, but it is reasonable to be concerned about whether IoT opens consumers up to potential harm by cyber criminals. What steps is the technology industry generally, and Intel specifically, taking to secure IoT devices?

***Response*:** Security must be a foundational building block for IoT in order to establish consumer trust – whether that consumer is a business, government, or an individual. Intel believes we can provide robust consumer protections, while enabling IoT investment and innovation that will improve the economy and GDP. (Of note, primary economic drivers of IoT will be commercial and industrial use cases, not consumer-facing applications.) For trusted data exchange in an IoT ecosystem, data generated by devices and existing infrastructure must be able to be shared between the cloud, the network, and intelligent devices for analysis – enabling users to aggregate, filter, and share data from the edge to the cloud with robust protection. For this reason, security is fundamental to Intel's IoT roadmap.

As discussed in my Prepared Statement for the Record (pp. 4-6), Intel believes that it is critical to integrate security into hardware *and* software from the smallest devices at the edge of the network to the most advanced server in the cloud and all gateways and devices in between.

These multi-level security capabilities create redundancies which prevent intrusions and enable a robust, secure, trusted end-to-end IoT solution. Intel's *hardware* will provide transistor-level security on the actual compute device itself at the outset (rather than layering it on top at latter point in design cycle with other, less secure external features). This means each compute device can have an irremovable identification which prevents any non-approved device from accessing the network. Intel's IoT solutions also will employ advanced hardware level capabilities – "whitelisting" (prevents harmful apps from being activated) and "blacklisting" (blocks list of known malware from entering device or network). Intel Security also integrates advanced *software* level security capabilities which enables the software to identify threats and proactively notify users and/or automatically quarantines devices that could be at risk. With this combination of transistor-level security, plus advanced hardware and software level security, Intel will protect IoT assets and data in ways few others can.

With respect to the technology industry generally, Intel and other technology companies collaborate with government, non-governmental organizations, and other private industry stakeholders to improve cybersecurity in a way that promotes innovation, protects citizens' privacy and civil liberties, and preserves the promise of the Internet as a driver of global economic development and social interaction. A recent example of such collaboration is the Cybersecurity Framework led by the National Institute of Standards and Technology (NIST). Executive Order 13636 (issued in February 2013) directed NIST to work with stakeholders to develop a voluntary framework – based on existing standards, guidelines, and practices – for reducing cyber risks to critical infrastructure. Intel and other technology companies worked collaboratively with other private industries and U.S. government partners to develop the Framework. Intel then took it a step further by creating, implementing and publishing a case study that encourages use of the Framework as a process and risk management tool.