Testimony of Robert Mayer

Senior Vice-President Cybersecurity, USTelecom

before the Senate Commerce Security Subcommittee

Cybersecurity of the Internet of Things

April 30, 2019

Chairman Sullivan, Ranking Member Markey, and other distinguished Members of the Subcommittee, thank you for the opportunity to testify at today's hearing on the cybersecurity of the Internet of Things. My name is Robert Mayer and I am the Senior Vice-President of Cybersecurity at USTelecom, the trade association that represents a diverse membership that ranges from large publicly traded global communications providers to small companies and cooperatives all of whom are committed to the security of the digital ecosystem as an essential driver of innovation, economic growth, public safety, our national security and other societal benefits.

The Internet of Things (IoT), a broad term referring to many categories of devices that connect to the internet, holds the promise of great benefits for modern society, both as a consumer-driven economic force that improves quality of life and as powerful sets of tools designed to increase efficiencies in measurable ways across businesses, governments, and non-profits. Today, we already see those benefits in diverse areas such as energy management, manufacturing, health care, and transportation to name a few. Yet, with 30 billion connected devices expected within a few short years and further exponential growth a virtual certainty, securing the IoT is among the chief cybersecurity challenges we face today.

There is growing evidence of stakeholders taking actions to improve the security of their products and the infrastructure supporting the digital ecosystem. For example, USTelecom members use botnet detection and filtering techniques; provide IoT managed security services; and collaborate with security researchers and law enforcement to limit the destructive

potential of IoT botnets. AT&T and Ericsson recently launched an IoT security testing program aimed at improving device security.

Networks at every level are evolving to accommodate exponential growth in traffic associated with billions of new end-point devices. The introduction of 5G and the associated architecture will allow industry to incorporate security measures into more layers than in previous generations. ISPs, security vendors and other infrastructure providers are developing improved security offerings, such as firewalls that more intelligently identify authorized users and attackers.

Commitment to ecosystem-wide solutions led to establishment by USTelecom in 2018 of the Council to Secure the Digital Economy (CSDE). Created in partnership with ITI, CSDE is led by 12 global ICT companies whose mission is to identify sophisticated and evolving cyber threats and the security practices that, if widely adopted, would materially contribute to the resiliency and sustainability of the global digital economy.

In November 2018, the CSDE and our strategic partner the Consumer Technology Association published the *International Anti-Botnet Guide* which is included with this testimony. The Guide discusses the problems inherent to IoT security and contains sets of baseline practices and advanced capabilities that are directly relevant to securing connected devices and the enabling infrastructure.

We are doing all of this because we have seen ample evidence of IoT security vulnerabilities and the potential harm to individuals, enterprises, government institutions and society writ large. We have seen that cameras can be used to invade their owners' privacy.[i] Confidential personal and business information can be stolen through seemingly innocuous IoT devices, such as thermometers.[ii] Deeply personal objects, from children's toys[iii] to baby heart monitors[iv] have been shown to be vulnerable to hackers. Vehicles can potentially be manipulated to cause deadly traffic accidents.[v] Hackers can manipulate temperature in smart homes,[vi] and whole

buildings have lost heat in the middle of winter.[vii] Concerns of this kind can have a massive influence on public perception of technologies, and if not addressed in meaningful ways, trust in the digital ecosystem will erode, causing unpredictable levels of disruption and economic harm.

Government has a vital role in supporting industry initiatives and the evolving standards and practices that are necessary to combat this growing threat. It is our view that voluntary, prioritized, flexible and cost-effective solutions embodied in the NIST Cybersecurity Framework can be effectively applied in the IoT space. We are also mindful that many states are pursuing legislation in this area and we are concerned that a patchwork quilt of state compliance requirements will add complexity, confusion and costs to an already challenging global landscape. In the digital ecosystem, no jurisdiction exists totally independent of others. Therefore, recommendations aimed at setting standards in one part of the ecosystem, while ignoring the others, are misjudging the scope and nature of the IoT security challenge.

In closing, we are strongly supportive of U.S. government and industry collaboration on IoT security at the federal level, through the highly successful public-private partnership model. The very nature of this challenge requires a highly adaptive and evolving response in as close to real-time as possible. That level of innovation and operational implementation can only be realized when policies are carefully aligned with market dynamics.

I look forward to answering your questions.

---

[i] Ms. Smith, *Hijacked Nest Devices Highlight the Insecurity of the IoT,* CSO (Feb. 4, 2019), https://www.csoonline.com/article/3338136/hijacked-nest-devices-highlight-the-insecurity-of-the-iot.html.

[ii] Oscar Williams-Grut, *Hackers Once Stole a Casino's High-roller Database Through a Thermometer in the Lobby Fish Tank*, BUSINESS INSIDER (Apr. 15, 2018), https://www.businessinsider.com/hackers-stole-a-casinos-database-through-a-thermometer-in-the-lobby-fish-tank-2018-4.

[iii] Glenn McDonald, *Strange and Scary IoT Hacks: Child's Plays*, NETWORK WORLD (July 3, 2018), https://www.networkworld.com/article/3285968/strange-and-scary-iot-hacks.html#slide3; Glenn McDonald, *Strange and Scary IoT Hacks: Toy Stories*, NETWORK WORLD (July 3, 2018), https://www.networkworld.com/article/3285968/strange-and-scary-iot-hacks.html#slide4.

[iv] Iain Thomson, *Wi-Fi Baby Heart Monitor may Have the Worst IoT Security of 2016*, THE REGISTER, (Oct. 13, 2016), https://www.theregister.co.uk/2016/10/13/possibly_worst_iot_security_failure_yet.

[v] Andrew Meola, *Consumers Don't Care if Their Connected Car can Get Hacked – Here's Why That's a Problem*, BUSINESS INSIDER (Mar. 7, 2016), https://www.businessinsider.com/smart-car-hacking-major-problem-for-iot-internet-of-things-2016-3 ("Hackers could potentially crash a compromised car, but they are more likely to exploit IoT devices to gain entry to corporate and government networks and databases.").

[vi] Luke Denne et al., *We Hired Ethical Hackers to Hack a Family's Smart Home — Here's How It Turned Out*, CBC NEWS (Sept. 28, 2018),)https://www.cbc.ca/news/technology/smart-home-hack-marketplace-1.4837963.

[vii] Lee Mathews, *Hackers Use DDoS Attack To Cut Heat To Apartment*, FORBES (Nov. 7, 2016), https://www.forbes.com/sites/leemathews/2016/11/07/ddos-attack-leaves-finnish-apartments-without-heat/#2b7483fb1a09.