Committee on Commerce, Science, and Transportation
Subcommittee on Security
Tuesday, April 30, 2019

Prepared Written Testimony of
Mike Bergman, Vice President, Technology and Standards,
Consumer Technology Association

I. Introduction

Thank you Chairman Sullivan, Ranking Member Markey and members of the Subcommittee for inviting me to testify today on strengthening the security of the Internet of Things (IoT). I am Mike Bergman, Vice President of Technology and Standards, of the Consumer Technology Association (CTA)™.[1]

CTA represents more than 2,200 member companies–80% are small businesses and startups; others are among the world's best-known brands–who comprise the $398 billion U.S. consumer technology industry. We also own and produce CES®, the world's gathering place for all who thrive on the business of consumer technologies. CTA welcomes the opportunity to provide input to the Subcommittee as it considers ways to strengthen IoT security. CTA stands for innovators, including many companies from large household names to entrepreneurial startups, whose products and services largely comprise the IoT.

Though CTA is the principal trade association representing the interests of the consumer technology industry, CTA also has a long history as a technical standards body going back to the 1920s. Our Technology and Standards program is accredited by ANSI, the American National Standards Institute, and includes more than 70 committees and over 1000 participants. As Vice President of Technology and Standards at CTA, my work is focused on this program. On a day-to-day basis, I work with technical leaders throughout the industry on technology standards issues. I also serve as a resource providing technical insights both within the association and for regulators and government leaders. Before joining CTA, I worked for over thirty years in a variety of product development and standards-setting roles across the consumer and computer technology industries.

In my role at CTA, as I will discuss in greater depth, I am deeply engaged in collaborative efforts among the technology industry and with the government to advance IoT security. These include

[1] Consumer Technology Association (CTA)™ is the trade association representing the $398 billion U.S. consumer technology industry, which supports more than 18 million U.S. jobs. More than 2,200 companies–80% are small businesses and startups; others are among the world's best-known brands–enjoy the benefits of CTA membership including policy advocacy, market research, technical education, industry promotion, standards development and the fostering of business and strategic relationships. CTA also owns and produces CES®, the world's gathering place for all who thrive on the business of consumer technologies. Profits from CES are reinvested into CTA's industry services.

ecosystem-wide industry initiatives, the National Institute of Standards and Technology's (NIST's) efforts to develop IoT core baseline security capabilities[2] and, more generally, advancing the Department of Commerce (DOC) and Department of Homeland Security's (DHS) "Road Map Toward Resilience Against Botnets" (DOC-DHS Road Map).[3]

II. Industry, in Close Coordination with Government Leaders, is Proactively Addressing IoT Cybersecurity Challenges

In recent years, the consumer technology ecosystem has grown ever more dynamic and complex. Consumers are increasingly incorporating technology in more aspects of their lives, and this consumer demand for anytime/anywhere connectivity will continue to drive the development of new innovation. The resulting proliferation of smart sensors and devices in our homes and cities (commonly referred to as the "Internet of Things") will enable tremendous consumer and public benefits over the coming years. This innovation also presents new challenges, especially regarding cybersecurity.

Industry has been working to address security for years. CTA has developed a number of consensus-based standards and tools, including helping manufacturers build more secure devices[4] and assess their internal processes for building in security[5] in addition to helping professionals install devices with more appropriate security-conscious settings.[6]

Building on the foundation we developed at CTA, we are working intensely with partners across the industry to secure the dynamic IoT ecosystem. In May 2018, we announced that we were working with the Council to Secure the Digital Economy (CSDE) to develop the International Anti-Botnet Guide (Guide). CSDE and CTA's members cover the entirety of the complex global Internet and communications ecosystem. We released the Guide in November 2018.[7] The Guide is a playbook that offers companies across the digital ecosystem a set of baseline tools, practices and processes they can adopt to help protect against the threat of botnets and other automated distributed attacks. The guide provides a flexible approach for IoT devices of varying

---

[2] *See* NIST, Draft Considerations for a Core IoT Cybersecurity Capabilities Baseline (Feb. 2019), https://www.nist.gov/sites/default/files/documents/2019/02/01/final_core_iot_cybersecurity_capabilities_baseline_considerations.pdf.

[3] A Road Map Toward Resilience Against Botnets (Nov. 29, 2018), available at https://www.ntia.doc.gov/blog/2018/road-map-building-more-resilient-internet.

[4] *See, e.g., "Securing Connected Devices for Consumers in the Home—A Manufacturer's Guide"* (CTA-TR-12CEB33), https://members.cta.tech/ctaPublicationDetails/?id=c12ebabe-84cd-e811-b96f-0003ff52809d

[5] BSIMM Assessment Survey, https://www.surveygizmo.com/s3/2849582/BSIMM6.

[6] *Connected Home Security System*, https://www.cta.tech/Membership/Member-Groups/TechHome-Division/Device-Security-Checklist.aspx

[7] CSDE, International Anti-Botnet Guide 2018, available at https://securingdigitaleconomy.org/wp-content/uploads/2018/11/CSDE-Anti-Botnet-Report-final.pdf.

processing capabilities and data types, providing companies with a range of options to appropriately address security risks. We committed to promoting implementation of the Guide's recommendations and updating it each year, and we are currently working on updates.

Last month, through the CSDE, we convened 18 major cybersecurity and technology organizations, industry associations, consortia and standards bodies—all groups that convene their own memberships ("Convene the Conveners," or C2). This unprecedented industry effort to identify baseline security capabilities for the rapidly growing IoT marketplace aims to address four challenges:

1. Promoting global harmonization vs. fragmentation of security specifications/requirements.

2. Working with emerging global market forces that naturally favor secure devices and systems.

3. Developing a coherent common language on these issues that is compelling to various policy and technical audiences.

4. Influencing policy development in Europe, the U.S. (including at the state level) and elsewhere.

Through this effort and other avenues, we and many of our member companies are collaborating closely with leaders at the National Telecommunications and Information Administration (NTIA), NIST, DHS and other government agencies.[8] We believe these agencies play important roles in developing trust in emerging technologies, such as the IoT. In this regard, we commend the Senate Commerce Committee for its essential role in promoting the NIST Cybersecurity Framework (Cybersecurity Framework)[9] and supporting the Framework's development, including the support of the Cybersecurity Enhancement Act of 2014.[10] CTA and its members strongly support the collaborative processes through which NIST has worked with the industry to develop and update the Cybersecurity Framework, as well as the NIST-convened, industry-supported efforts set forth in the DOC-DHS Road Map.

III. Market Forces Are Combining With Public-Private Cooperation for Major Gains

Companies in the retail sector are increasingly concerned about protecting their customers. They want customers to feel comfortable when they buy products, and they want the market for IoT devices to be something where consumers can engage freely. These companies are

[8] For instance, CTA has engaged, and will continue to engage, NIST in its important efforts to develop IoT security baseline capabilities.

[9] *See* NIST, Cybersecurity Framework, https://www.nist.gov/cyberframework.

[10] *Cybersecurity Enhancement Act of 2014*, Pub. L. No. 113-274, 128 Stat. 2971 (2014).

working internally and with CTA to develop ways to promote security among their manufacturing suppliers.

Retailers suggest that retailer-manufacturer conversations–discussions that ultimately result in supplier agreements–should be based in accepted industry standards. The largest retailers are looking to industry and government for guidance on standards and best practices. Retailers say they need a common, industry-accepted way to identify acceptable baseline security with their suppliers. NIST, as part of the DOC-DHS Road Map, is developing a list of core baseline security capabilities for IoT through a public multi-stakeholder process that will advance these market developments.[11]

In turn, our C2 effort with the CSDE is driving industry consensus for these security capabilities. Our effort will inform NIST and other U.S. government efforts on IoT security and advance the broader market developments that are already underway.

IV. Government and Industry Speaking With One Voice on Consensus-Based Standards Can Best Address Global IoT Cybersecurity Challenges

CTA believes that the U.S. government should continue to play its critical role in convening activities among different ecosystem stakeholders. NIST's work related to cybersecurity is illustrative of the productive role government can play in these efforts. The Cybersecurity Framework has been an incredibly successful and important public-private partnership, and NIST's guidance on IoT security baseline capabilities has the potential to have a similar impact. CTA believes the Committee should continue to support this approach.

Ultimately, dynamic solutions driven by powerful market forces are the best answer to global, systemic challenges to IoT security. CSDE, C2 and other ongoing industry efforts demonstrate that industry is committed to these dynamic solutions based on the conviction that these solutions can work. Specifically, IoT security solutions must include and rely on:

- *Ecosystem-wide consensus.* We are seeking a baseline security consensus that includes all major stakeholders globally, not just a single industry sector, association, vertical or national/regional jurisdiction. A key pillar of market-driven IoT security is achieving technical consensus on security specifications that, in turn, can be assessed and communicated to buyers and other market participants.
- *Voluntary standards and best practices.* We are taking on this challenge voluntarily for industry's own interests in a global marketplace. In contrast, prescriptive compliance-based regulations in various jurisdictions would handicap these efforts.
- *Standards that scale.* We believe that security specifications driven by powerful global market demands and fueled by ever-improving security innovations of technical experts

[11] *See* NIST, Draft Considerations for a Core IoT Cybersecurity Capabilities Baseline (Feb. 2019), https://www.nist.gov/sites/default/files/documents/2019/02/01/final_core_iot_cybersecurity_capabilities_baseline_considerations.pdf.

are the best method to advance IoT security. Government policies should be structured to promote this dynamic. In contrast, regulatory requirements that would differ by jurisdiction would inhibit security.

It is critical to recognize IoT security is not a domestic problem in the U.S. that can be solved merely by domestic solutions. The October 2016 Mirai botnet attack on Dyn that took down many of the most popular websites on the U.S. and UK internet was global: 89.1% of the enormous inbound attack traffic came from devices installed outside the U.S.[12] In other words, enhancing the security of devices in the U.S. alone would not have prevented the Mirai attack or substantially mitigated its impact.

IoT security is not merely a U.S. interest. Other government bodies around the globe are seeking answers including the European Union Agency for Network and Information Security, the United Kingdom's Department for Digital, Culture, Media and Sport and Japan's Ministry of Economy, Trade and Industry. This international interest in IoT security also underscores the importance of a common approach.

Market-driven security solutions, promoted by government leaders and agencies, can best address the global IoT security challenge at scale. With cooperation between CDSE, CTA, NIST, NTIA, industry, retailers and assessment bodies all moving in the same direction and with the same strategy, the message coming from the U.S. in international fora is clear, meaningful and impactful. We encourage the Committee to continue to champion this approach.

V. Conclusion

In summary, industry is working with government to make significant and rapid progress in navigating the expeditious and effective possible path to national and global IoT security. This Subcommittee has and will continue to play an important role in building the foundation for this progress. We ask that the Subcommittee continue to support and promote the groundbreaking efforts underway at NIST, DHS, DOC and other agencies, as well as across the industry, that are providing formal processes and structures to lead the global IoT to a secure future.

[12] *See* Internet Protocol (IP) address analysis by Imperva, Breaking Down Mirai: An IoT DDoS Botnet Analysis (Oct. 2016), https://www.imperva.com/blog/malware-analysis-mirai-ddos-botnet/