Consumer Technology Association

Additional submitted attachment is included below.

In the matter of:	Docket No. 20-FDAS-01
Regulations to Establish Standards for Flexible Demand Technologies for Appliances	December 14, 2020 Senate Bill 49 Flexible Demand Appliance Standards Workshop

COMMENTS OF THE CONSUMER TECHNOLOGY ASSOCIATION

The Consumer Technology Association (CTA®)[1] provides these comments following the

Energy Commission's "Senate Bill 49 Flexible Demand Appliance Standards Workshop" on

December 14, 2020. The workshop included a "Communication Technologies and

Cybersecurity" discussion, and CTA offers several comments on this topic. We also offer a few

comments on a CTA standard which was referenced during the workshop.

Cybersecurity

CTA commends the Energy Commission as well as other policymakers for continuing to

prioritize collaborative work with the private sector in addressing cybersecurity challenges and

privacy concerns, including as they relate to the internet of things (IoT). CTA and many of its

individual members are actively working with the National Institute of Standards and

Technology ("NIST"), the National Telecommunications and Information Administration

("NTIA"), the Department of Homeland Security ("DHS") and other government agencies, and

---

[1] As North America's largest technology trade association, CTA is the tech sector. Our members are the world's leading innovators - from startups to global brands - helping support more than 18 million American jobs. CTA owns and produces CES® - the largest, most influential tech event on the planet.

with other sectors of industry, to develop forward-looking solutions to security, privacy, and other emerging technological challenges, while also promoting innovation in the IoT and the broader digital ecosystem. CTA believes there is a need for a common baseline of security capabilities for all IoT devices. Recommendations and requirements for such capabilities that are in place in various jurisdictions worldwide have suffered from fragmentation.

Bringing consensus and harmonization to the current fragmentation will increase the market's ability to promote IoT security by creating efficiencies of scale in development, manufacturing, support, training, assessment and identification of IoT products with increased security controls. NIST's Core Baseline (NISTIR 8259A) will be a critical component of this effort. The public-private partnership that NIST has leveraged to develop its core baseline, along with the general requirements for "reasonable" IoT device security that are already present in state and federal law, provide the United States with a path forward on IoT security that can be shared and replicated internationally. This approach will advance IoT security throughout the marketplace, while also promoting the technological innovation that has been the engine of the U.S. economy.

At the same time, security requirements must recognize that all technologies – and all threats – are not created equal. As such, any government or regulatory framework must (1) include an analysis of risk and (2) give manufacturers the flexibility to adopt the baseline security principles that best enable them to respond to the evolving cyberthreat landscape. On the first point, one could reasonably expect that a data breach from a connected dog collar would cause less harm than a breach of a pacemaker or other medical equipment, for instance. Accordingly, a security framework should not mandate a single, static level of security across the board. Instead, a flexible approach that permits companies to address different types and levels

2

of risk would best ensure that companies can take the steps needed to secure equipment now and in the future.

Additionally, by allowing manufacturers to select amongst different options to demonstrate "reasonable" security measures, governments will better encourage the adoption of such protocols. For example, CTA co-leads, with USTelecom, the Council to Secure the Digital Economy ("CSDE"), a group of more than a dozen major ICTS companies deeply invested in the security of our communications infrastructure and connected products ecosystem.[2] CSDE has convened important discussions and produced tools to aid companies and governments alike. In 2019, through CSDE, CTA convened 20 major cybersecurity and technology organizations, industry associations, consortia, and standards bodies—all groups that convene their own security-focused memberships. This unprecedented industry effort, known as "Convene the Conveners" or "C2," sought to identify baseline security capabilities for the rapidly growing IoT marketplace to address four challenges:

- Promoting global harmonization to prevent fragmentation of security specifications and requirements;

- Working with emerging global market forces that naturally favor secure devices and systems;

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

- Assisting policy development internationally and in the United States, including at the state level.

The C2's efforts resulted in a voluntary industry consensus standard for IoT baseline security, CTA-2088.[3] Other groups, such as CTIA, offer cybersecurity certifications for IoT

---

[2] *See* Council to Secure the Digital Economy, Member Companies, https://securingdigitaleconomy.org/member-profiles (last visited Feb. 1, 2021).

[3] https://standards.cta.tech/apps/group_public/project/details.php?project_id=594.

devices.[4] CTA urges the Energy Commission to permit flexibility in demonstrating compliance with any reasonable security requirement it may choose to adopt. While baseline security is an important effort that CTA and its members support, one-size-fits-all solutions may impose requirements that are unworkable for certain industries or products and ultimately discourage innovation with little net benefit.

CTA-2045

The CTA-2045 ("Modular Communications Interface for Energy Management") standard was frequently referenced during the Commission's recent workshop, and we would like to provide additional information about the standard should it be helpful in this proceeding.

CTA-2045 was first published in 2013 to allow communication with end devices through a standardized interface compatible with multiple communications technologies. CTA-2045 was revised recently (and is now formally known as "CTA-2045-B") to distinguish between Level 1 and Level 2 certification requirements recommended by CTA. CTA does not certify products nor recommend certification bodies. Rather, recommended certification levels are described in Appendix F of the standard.[5]

CTA-2045 was produced through the consensus standard development process as required in American National Standards Institute (ANSI) Essential Requirements. CTA is an ANSI Accredited Standards Developing Organization.[6]

---

[4] https://www.ctia.org/news/ctia-iot-cybersecurity-certification-program-certifies-first-device.
[5] CTA-2045-B is available for free download at https://shop.cta.tech/collections/standards/products/modular-communications-interface-for-energy-management.
[6] *See* https://www.ansi.org/american-national-standards/ans-introduction/essential-requirements.

We appreciate the opportunity to participate in the Commission's recent workshop and look forward to further involvement in this proceeding.

Respectfully submitted,

CONSUMER TECHNOLOGY ASSOCIATION

By: /s/ Jamie Susskind
Jamie Susskind
Vice President, Regulatory Affairs
1919 South Eads Street
Arlington, VA 22202
(703) 907-7600
jsusskind@cta.tech

By: /s/ Veronica Lancaster
Veronica Lancaster, AStd
Vice President, Standards Program
vlancaster@cta.tech

By: /s/ Douglas Johnson
Douglas Johnson
Vice President, Technology Policy
djohnson@cta.tech

February 3, 2021