Before the
DEPARTMENT OF COMMERCE
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Washington, DC 20230

In the Matter of	)	
	)	
Promoting Stakeholder Action Against Botnets and Other Automated Threats	)	Docket No. 180103005-8005-01
	)	

COMMENTS OF THE CONSUMER TECHNOLOGY ASSOCIATION

Julie M. Kearney
Vice President, Regulatory Affairs
Brian Markwalter
Senior Vice President,
Research and Standards
Michael Bergman
Senior Director,
Technology and Standards
Consumer Technology Association
1919 Eads Street
Arlington, VA 22202
(703) 907-7644

February 12, 2018

TABLE OF CONTENTS

Before the
DEPARTMENT OF COMMERCE
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Washington, DC 20230

In the Matter of	)	
	)	
Promoting Stakeholder Action Against	)	Docket No. 180103005-8005-01
Botnets and Other Automated Threats	)	

COMMENTS OF THE CONSUMER TECHNOLOGY ASSOCIATION

The Consumer Technology Association ("CTA")[1] welcomes this opportunity to comment on the draft report on enhancing resilience against botnets and other automated distributed threats, prepared by the Departments of Commerce and Homeland Security and released on January 5, 2018.[2]

INTRODUCTION AND BACKGROUND

In its filing responding to the initial request for comments on this matter, CTA recommended that government work to advance four guiding principles:

- (i) cybersecurity is best ensured through market-driven solutions that reflect private sector leadership and innovation and that work globally;

[1] The Consumer Technology Association ("CTA")™ is the trade association representing the $351 billion U.S. consumer technology industry, which supports more than 15 million U.S. jobs. More than 2,200 companies – 80 percent 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

[2] *A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats*, Transmitted by the Secretary of Commerce and the Secretary of Homeland Security, Jan. 5, 2018 ("Draft Botnet Report"); *see also* Department of Commerce, National Telecommunications and Information Administration, *Promoting Stakeholder Action Against Botnets and Other Automated Threats*, Request for Public Comment, 83 Fed. Reg. 1342 (Jan. 11, 2018) ("RFC").

- (ii) cybersecurity is best ensured through dynamic, flexible approaches that are as nimble and adaptive as cyber threats, as opposed to static checklist compliance;

- (iii) cybersecurity is a shared responsibility among all players in the internet/communications ecosystem, and government should avoid facile solutions that rely on one or two particular components; and

- (iv) true cybersecurity will require mutually beneficial teamwork among governments, companies, and consumers with a real, active partnership that takes action against bad actors and elevates the contributions of private sector good actors.[3]

As CTA explained, these principles underlie the stakeholder-driven processes and industry-led solutions on which government has relied thus far to address cybersecurity challenges. CTA thus is pleased to see these same concepts reflected in the Draft Botnet Report, and in particular, in its six principal themes, which should be retained for the final report.[4]

The market innovations on display at CES® 2018, which CTA concluded just last month, underscored the continuing relevance and importance of these themes. CES is the global stage for innovation; it has been a proving ground for innovators and breakthrough technologies for more than fifty years. As it does each year, CES showcased the dynamic nature of technology today and the consumer benefits that are possible when companies innovate freely – as was demonstrated by the proliferation of smart, connected devices that were on display. More particularly, CES reinforced both the dynamism in the market for security innovations for those devices and platforms and the wide and diverse nature of the security ecosystem as a whole. It also provided further corroboration for CTA's previous observation that industry is already on the front lines of the nation's defense against malicious cyber threats.[5] These aspects of the ecosystem are critical premises for further approaches to cybersecurity.

---

[3] Comments of the Consumer Technology Association, Docket No. 170602536-7536-01, at 5 (filed July 28, 2017) ("CTA July Comments").

[4] Draft Botnet Report at 3.

[5] CTA July Comments at 4-5; *see also infra* (citing examples).

DISCUSSION

With the very recent experience of CES 2018 in mind, CTA offers three specific reactions to the Draft Botnet Report. The first of these reflects a recurring theme so fundamental to this matter that it bears repeating again – the continuing importance of inclusive processes that facilitate leadership by the private sector in place of top-down prescriptive regimes (Section I). Beyond that foundational principle, CTA provides additional reactions that highlight the ***supply side*** (Section II) and the ***demand side*** (Section III) of the market for security.

I. GOVERNMENT SHOULD CONTINUE BUILDING CYBERSECURITY POLICY AROUND DYNAMIC, INCLUSIVE, MARKET-DRIVEN SOLUTIONS.

The Draft Botnet Report accurately observes that the policy domain is intertwined with the technical domains, encompassing public-private partnerships (including information-sharing arrangements), voluntary attestation or certification processes, standards and guidelines developed in multistakeholder fora, procurement policies (especially within the federal government), regulatory and legislative actions at the federal and/or state levels, and multi- and bi-lateral coordination/agreements to institutionalize international coordination and collaboration.[6] The intersection of these domains underscores the value of multistakeholder processes in addressing cybersecurity challenges.

CTA commends NTIA, NIST, and the Department of Homeland Security ("DHS") for their reliance on such broad-based, inclusive processes that emphasized the private sector's role and leveraged the value brought by industry's expertise and operational experience. This holds not just for the Draft Botnet Report, but also the agencies' approaches to cybersecurity challenges more generally – including the various multistakeholder processes conducted by NTIA, NIST's partnership with industry under its Cybersecurity for IoT Program to develop

[6] Draft Botnet Report at 9.

guidance on IoT security for federal agencies,[7] and the processes governing the National Security Telecommunications Advisory Committee ("NSTAC") as well as the IT and Communications Sector Coordinating Councils. We applaud DHS for focusing its efforts in this process on gaining the private sector expertise that came from expediting the NSTAC Report to the President on Internet and Communications Resilience. All of these agencies should continue to promote this dynamic model – including in subsequent activities that the final report to the President will recommend in May.

The Draft Botnet Report notes a potential role for regulatory and legislative actions, such as regulation related to procurement and "careful" enforcement action.[8] CTA continues to urge caution with respect to regulatory approaches generally, as they usually tend toward static, prescriptive compliance regimes that inhibit security innovation over time.[9] The final report should emphasize that such regulatory solutions are not only rarely effective, but are in fact usually counter-productive to the goal of security, and that government should instead focus on continuing to promote dynamic market-driven solutions.

II. INDUSTRY ADVANCES IN THE MARKET FOR CYBERSECURITY ARE ACCELERATING.

The Draft Botnet Report takes a promising, but still somewhat dour, view of existing security tools, stating that such tools are available in the marketplace but noting that they are not widely used for a variety of reasons – an observation that is encapsulated by the report's second

---

[7] NIST Cybersecurity for IoT Program, https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program.

[8] *See, e.g.*, Draft Botnet Report at 9, 22, 34; Action 2.3.

[9] CTA July Comments at 13-14; *see generally* Gary Shapiro, *How the Heavy Hand of Government Stifles the On Demand Economy*, TechDirt (Aug. 25, 2015), https://www.techdirt.com/articles/20150824/11370432049/how-heavy-hand-government-stifles-demand-economy.shtml.

theme.[10] Promoting awareness and demand for security tools that are developing in the market should be an important, and indeed central, focus of policy activity going forward (as also discussed *infra* Section III). To that end, policy efforts should recognize, and be oriented around promoting, the vitality and positive trajectory of marketplace activity in this space. Indeed, there are major opportunities for advancements, and it is crucial to preserve and further develop the environment that is yielding these possibilities.

In this respect, the Draft Botnet Report's emphasis on enterprises is important and should be retained in the final report,[11] as this segment of the marketplace is a focus of much industry activity. Again, as the draft notes, products and services for enhancing security are available now that were not possible even a few years ago, particularly at the gateway level. One such example is network management tools and devices ("NMDs"), a category of devices that act in a smart gateway fashion. NMDs come in a variety of flavors and forms. Most are hardware with software built in, but some can be software embedded in hardware or software only. Almost all, however, do some sort of blocking and limiting of access to certain websites, portals and VPNs that are risky for users. They also allow filtering of access to the Internet via scheduling, IP addresses, and mac addresses. Finally, some allow parental control support, allowing complete control of what devices connect to what internet sites and when.

Security innovation for consumers also is exploding. Again, CES 2018 provided ample illustration. For instance, Samsung announced at CES that they are incorporating their defense-grade KNOX security technologies into Smart TVs and appliances in addition to mobile

[10] Draft Botnet Report at 3 ("Effective tools exist, but are not widely used."); *see also, e.g., id.* at 16 (observing that "current best practices are fairly effective, if imperfect, and result in devices that are reasonably secure upon delivery" but that these practices "are implemented inconsistently").

[11] *See, e.g., id.* at 12-14 (defining "enterprises" as "medium and large businesses, government agencies, and academic institutions").

devices.[12] Cujo used CES as a platform for announcing its "Platform for Network Operators," which consists of device intelligence, network security, and advanced parental controls.[13] Bitdefender demonstrated its Bitdefender BOX 2, which simply plugs into a home router to protect homes from online threats.[14] CES also showcased a new generation of routers with advanced security features.[15]

Meanwhile, as CTA described in its original comments and elsewhere, industry also is on the front lines of the nation's defense against malicious cyber actors with offerings to consumers and small businesses.[16] Chip makers are offering secured system-on-a-chip components for IoT devices,[17] platform services are offered to provide end-to-end security and management of IoT

---

[12] News Release, *Samsung Delivers Vision for Open and Intelligent IoT Experiences to Simplify Everyday Life*, Jan. 8, 2018, https://news.samsung.com/us/samsung-vision-iot-experiences-ces2018-press-conference/.

[13] *CUJO AI at CES: two great achievements to celebrate*, Jan. 12, 2018, https://www.getcujo.com/blog/ces-2018/; Alistair Charlton, *Best of CES 2018*, Jan. 10, 2018, https://www.gearbrain.com/best-products-of-ces-2018-2524144794.html ("Cujo's updated security platform is aimed at protecting every device you own from being hacked … We like how Cujo is talking with internet service providers to deeply integrate its protection products into customer's homes.").

[14] *See, e.g.*, Bitdefender: Latest News, *Bitdefender to Showcase Evolution of Smart Home Security at CES 2018*, Dec. 14, 2017, https://www.bitdefender.com/news/bitdefender-to-showcase-evolution-of-smart-home-security-at-ces-2018-3405.html.

[15] *See, e.g.*, Tercius Bufete, *In 2018, Wifi Routers Learn New Tricks*, Consumer Reports, Jan. 10, 2018, https://www.consumerreports.org/wireless-routers/what-to-expect-from-routers-in-2018/?loginMethod=auto ("A small number of routers with security software built in have been introduced in recent years, including the Norton Core that was launched at CES in 2017. But in 2018 the trend is accelerating as more companies introduce routers that incorporate the kind of anti-malware tools we're used to running on our computers.").

[16] CTA July Comments at 4-5.

[17] ARM's TrustZone standard is widely used by ARM licensees to provide security-hardened solutions (http://www.arm.com/products/processors/technologies/trustzone/index.php). Additional examples include the AMD Platform Security Processor (PSP) category of products, *see* Caroline Hayes, *Deeper Dive – IoT Security*, Chip Design Magazine, June 30, 2014, http://chipdesignmag.com/sld/blog/2014/06/30/deeper-dive-iot-security/ (interview with AMD's Steve Kester), and many Freescale ARM-based products

devices,[18] and many other segments are responding in similar fashion. For example, Samsung is promoting security of the broader IoT marketplace by offering its ARTIK platform as well as the opportunity for third-party devices to connect to the Samsung SmartThings Cloud if they meet certain baseline security requirements.[19]

A standard for "Manufacturer Usage Description" (or "MUD") that Cisco and other companies are promoting is premised on giving a device a secure means to say what it should be allowed to do on the network, so that the gateway and ISP can recognize when the device starts acting out-of-character (*e.g.*, when it becomes part of a botnet).[20] The idea is that the device is given a secure means to say what it should be allowed to do on the network, so that the gateway and ISP can recognize when the device starts acting out-of-character (*e.g.*, when it becomes part

---

(http://www.freescale.com/about/technology-programs/security-technology/trusted-systems-technology:NETWORK_SECURITY_INT_SEC). Intel's TrustLite security framework provides hardware to protect software on low-cost embedded devices (https://securityledger.com/2015/11/intel-updates-iot-platform-with-security-in-mind/); Altera FPGAs and SoCs support hardware crypto acceleration and secure remote in-field upgrades with AES encryption (https://www.altera.com/solutions/technology/iot/overview.html); and Analog Devices (ADI) has connectivity products for IoT with features such as hardware acceleration for cryptography (http://design.avnet.com/axiom/analog-devices/).

[18] Intel has the Intel IoT Platform (https://www.intel.com/content/www/us/en/internet-of-things/iot-platform.html); IBM has the Watson IoT platform (https://www.ibm.com/internet-of-things/platform/watson-iot-platform/); NXP has the QorIQ Platform (http://www.nxp.com/products/microcontrollers-and-processors/arm-processors/qoriq-layerscape-arm-processors/development-resources/qoriq-layerscape-secure-platform-securing-the-complete-product-lifecycle:SECURE-PLATFORM); and Microsoft has the Azure suite (https://docs.microsoft.com/en-us/azure/iot-suite/iot-suite-security-deployment).

[19] Samsung's ARTIK enables secure device registration based on a hardware root of trust that supports a secure operating environment and securely connects devices to the cloud using TLS and certificates issued by a trusted certificate authority. *See* Samsung ARTIK IoT Platform, https://www.artik.io/.

[20] *See, e.g.*, Marc Blackmer, *Scaling Security for The Internet of Things with MUD*, The Security Ledger, Oct. 14, 2016, https://securityledger.com/2016/10/mud-scaling-security-for-the-internet-of-things/.

of a botnet).[21] The final report should reflect these innovations while also noting that more are likely to follow.

In particular, large enterprises of all types, both government and private sector, can collectively drive the demand side of the market for security by seeking and investing in innovative security solutions like these in their suite of network and device platforms. CTA is considering new ways to further highlight and advance these promising developments, and in the coming weeks we plan to engage with NTIA, NIST, and DHS to develop actionable steps to advance this promising market.

III. INCREASED SECURITY AWARENESS IS A VALID GOAL THAT REQUIRES PRAGMATIC AND CREATIVE SOLUTIONS.

The Draft Botnet Report recognizes that tools like those described above are available but indicates that they are underutilized for a number of reasons, including but not limited to a lack of awareness in the home consumer and small business market. CTA agrees that increased awareness in the marketplace is important. In CTA's view, addressing this challenge requires not just consideration of transparency and disclosure, but an increase in ***consciousness*** about the benefits to consumers and small businesses of buying secure products and platforms. CTA requests that that this aspect of awareness be captured in the final report.

Achieving such an increased consciousness about security requires particular attention to what constitutes effective information and notice to consumers and small businesses who are not – and do not wish to be and will never be – primarily focused on the security capabilities of the devices and platforms they purchase. For this part of the market, device and platform suppliers should redouble their marketing efforts to clarify for their buyers the benefits of purchasing secure products.

[21] *See* https://datatracker.ietf.org/doc/draft-ietf-opsawg-mud/ (MUD formal standard status).

CTA has considerable experience in this area, which should inform the final botnet report. Indeed, CTA has provided technical security guidance for a number of audiences. For instance, CTA has issued a technical report (CTA TR-12) titled *Securing Connected Devices for Consumers in the Home,*[22] security best practices and an online checklist for connected home dealers and professionals,[23] and consumer PSAs in radio markets reaching 2.2 million people. Likewise, some CTA members are members of industry groups that have developed cybersecurity resources for consumers and best practices for home security,[24] and some have collaborated with NIST on programs like its Cyber-Physical Systems Program and Cybersecurity for IoT Program.

We have learned from these experiences that over-notification can be a problem, as the Federal Trade Commission ("FTC") explained in its comments in NTIA's multistakeholder process on patching and upgradability.[25] Specifically, the FTC astutely observed that "effective

[22] CTA Technical Report: Securing Connected Devices for Consumers in the Home, CTA-TR-12 (Nov. 2015), https://standards.cta.tech/kwspub/published_docs/CTA-TR-12-Final.pdf. A revision of this document will be published in March 2018 as CTA-CEB-33.

[23] CTA, Welcome to the Connected Home Security Checklist Tool, https://www.cta.tech/Membership/Divisions-Councils/TechHome-Division/Device-Security-Checklist.aspx; TechHome (a Division of Consumer Technology Association), Recommended Best Practices for Securing Home Systems (Dec. 2015), https://www.cta.tech/cta/media/Membership/PDFs/Recommended-Best-Practices-for-Securing-Home-Systems-v16.pdf.

[24] Consumer Technology Association, *Internet of Things: A Framework for the Next Administration*, at 8 n.100 (Nov. 2016), http://www.cta.tech/cta/media/policyImages/policyPDFs/CTA-Internet-of-Things-A-Framework-for-the-Next-Administration.pdf (noting resources developed by the National Cyber Security Alliance and the WiFi Alliance, both of which share some members with CTA).

[25] Federal Trade Commission Public Comment on "Communicating IoT Device Security Update Capability to Improve Transparency for Consumers," Communicating Upgradability and Improving Transparency Working Group, Multistakeholder Process on Internet of Things Security Upgradability and Patching, NTIA, June 19, 2017, https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-comment-national-

notification is difficult to get right. Poor disclosures, including overly extensive disclosures, can actually impede consumers' ability to make informed choices."[26]

Thus, any approach to certification and labeling that might follow the recommendation in Action 5.1 regarding "voluntary informational tools for home IoT devices" should undertake a careful, sophisticated analysis of the potential benefits of these tools. At present, there is no consensus on how to achieve that effectively. To the contrary, certification and labeling are evolving art forms both globally and domestically, and the final report should reflect that reality. For instance, different countries have taken varying approaches to the issue. Among those countries that have put in place some form of a certification and/or labeling regime, some are voluntary (such as in the European Union[27] and South Korea[28]), some are mandatory (such as in China[29]), and some apply differently to different ecosystem components (placing requirements only on government contractors, as in the UK,[30] or on "critical" infrastructure, as in China). And of course, many of these initiatives are pending – for instance, there are draft bills or proposals in Thailand[31] and Vietnam,[32] on which further action reportedly is not expected until later in 2018 – highlighting the evolving nature of thinking on these informational programs.

---

telecommunications-information-administration-communicating-iot-device-security/170619ntiaiotcomment.pdf.

[26] *Id.* at 6 (citations omitted).

[27] General Data Protection Regulation 2016/679, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC.

[28] Act on the Promotion of IT Network Use and Information Protection, etc., https://iapp.org/media/pdf/knowledge_center/S-Korea_IC_Network_Act.pdf.

[29] 2016 Cybersecurity Law, http://www.chinalawtranslate.com/cybersecuritylaw/?lang=en.

[30] Cyber Essentials Scheme, https://www.gov.uk/government/publications/cyber-essentials-scheme-overview.

[31] Draft National Cybersecurity Act, https://thainetizen.org/wp-content/uploads/2015/03/cybersecurity-bill-20150106-en.pdf; Komsan Tortermvasana, *Telmin picks Thailand as hub for ASEAN cybersecurity training*, Bangkok Post, Dec. 6, 2017,

In the United States, approaches to the issue of informational outreach are evolving as well. For example, the Federal Communications Commission ("FCC") has been working for several years to implement a congressional directive to permit optional electronic labeling (or "e-labeling") in place of physical labels, paper inserts, and paper manuals.[33] In that context, CTA has emphasized that flexibility and optionality are paramount.[34] That admonition is certainly applicable in this context, too.

Given these complexities, CTA recommends that efforts to increase awareness in this context start with patching – specifically, promoting and implementing the consensus recommendations from the patching and upgradability multistakeholder process about communicating patching/upgrading capabilities to consumers.[35] More broadly, CTA is exploring additional novel ways to promote security awareness and consciousness among consumers that take into account the advantages and disadvantages of approaches that currently

---

https://www.bangkokpost.com/tech/local-news/1373131/telmin-picks-thailand-as-hub-for-asean-cybersecurity-training.

[32] The Law on Cybersecurity, Draft 1 June 2017, https://chambermaster.blob.core.windows.net/userfiles/UserFiles/chambers/9078/File/Vietnam-Draft-Cyber-Security-Law_English-20160621.docx; *Vietnam unveils 10,000-strong cyber unit to combat 'wrong views'*, Reuters, Dec. 26, 2017, https://www.reuters.com/article/us-vietnam-security-cyber/vietnam-unveils-10000-strong-cyber-unit-to-combat-wrong-views-idUSKBN1EK0XN. Just last week, Singapore passed a bill addressing these issues. Jalelah Abu Baker, *Cybersecurity Bill passed in Parliament; MPs raise questions on privacy, cost*, Channel NewsAsia, Feb. 5, 2018, https://www.channelnewsasia.com/news/singapore/cybersecurity-bill-passed-in-parliament-mps-raise-questions-on-9929208.

[33] *See Amendment of Parts 0, 1, 2, 15 and 18 of the Commission's Rules Regarding Authorization of Radiofrequency Equipment*, First Report and Order, ET Docket No. 15-170, FCC 17-93 (rel. July 14, 2017).

[34] *See generally, e.g.*, Comments of the Consumer Electronics Association, ET Docket No. 15-270, RM-11673 (FCC filed Oct. 9, 2015).

[35] NTIA, Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching, https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security.

are being explored while also soliciting new ideas. As with our efforts to advance the market for NMDs mentioned above, in the coming weeks CTA will engage with NTIA, NIST, and DHS to develop actionable steps to achieve these consumer-oriented security goals.

Finally, turning to increasing security awareness and capability in industry, the overall market for secure devices and IoT platforms would benefit from an in-depth analysis of the component supply chain for IoT devices. Many companies take a rigorous and disciplined approach to device security. However, it is also possible for a developer to produce an IoT device without considering security. While such developers and their employers are responsible for the products they produce, there is significant leverage available to improve IoT security by addressing the IoT ecosystem at this component level.

At the IoT product level (sometimes referred to as the "shrink-wrapped product" level), there are potentially hundreds of thousands of companies and millions of developers. However, the number of IoT system-on-a-chip ("SoC") device offerings is much more limited; dozens of companies offer perhaps a few hundred such products. The developer may choose a full IoT platform solution as a starting point, including security features such as end-to-end security and management of IoT devices, as mentioned above in Section II. Or the developer may choose a SoC where the manufacturer makes available a working sample design. This "reference design" typically includes circuit schematics, component list or bill-of-materials, and source code. A single reference design may be used in hundreds of final products. Another resource for the IoT device developer is open source software; developers often choose such resources as free "starting points" for commercial products. These three development entry points – IoT platforms, manufacturer's reference designs, and open source software – overlap somewhat; for example, manufacturer's reference designs sometimes use open source software.

The three development entry points, however, provide high-leverage access to the development world of the IoT, potentially influencing hundreds of thousands of development projects and many millions of connected devices. This perspective can be invaluable in considering next steps, such as the development of an IoT Device Profile as considered in Action 1.1. Therefore, when developing such a Profile, we recommend considering its usability when working with these lower-level but higher-leverage points. Here again, in the coming weeks, CTA will engage with NTIA, NIST, and DHS to develop actionable recommendations to advance the market's understanding of these issues.

While CTA considers various options for each of these areas, we generally recommend that, over the longer term, NTIA, NIST, and DHS retain coordinated leadership roles in convening private sector input on these issues, allocating responsibility (and sharing it with other agencies) depending on the specific issue. For instance, NTIA could take the lead with respect to security labeling and promoting the market for NMDs, perhaps in association with the FTC, and with the coordinated assistance of NIST and DHS. Meanwhile, NIST could have primary responsibility for the more technical task of analyzing the elements of the device component ecosystem and developing broader security guidance based on this analysis – again, with the coordinated assistance of NTIA and DHS.

CTA looks forward to exploring these and related ideas in the next few weeks and months, including at the forthcoming workshop to be hosted by NIST.

CONCLUSION

CTA looks forward to partnering with NTIA, NIST, DHS, and the other agencies involved in this effort to advance these important initiatives.

Respectfully submitted,

CONSUMER TECHNOLOGY ASSOCIATION

By: */s/ Julie M. Kearney*

Julie M. Kearney
Vice President, Regulatory Affairs
Brian Markwalter
Senior Vice President,
Research and Standards
Michael Bergman
Senior Director,
Technology and Standards
Consumer Technology Association
1919 Eads Street
Arlington, VA 22202
(703) 907-7644

February 12, 2018