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

In the Matter of)
)
Promoting Stakeholder Action Against) Docket No. 170602536-7536-01
Botnets and Other Automated Threats)

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

July 28, 2017

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. 170602536-7536-01
Botnets and Other Automated Threats	)	

COMMENTS OF THE CONSUMER TECHNOLOGY ASSOCIATION

The Consumer Technology Association ("CTA")[1] is pleased to respond to the National Telecommunications and Information Administration's ("NTIA") Request for Comment ("RFC") on actions that can be taken to address automated and distributed threats to the digital ecosystem, such as botnets.[2]

I. INTRODUCTION AND BACKGROUND

As NTIA considers the issues raised here in connection with the Administration's Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," it should keep in mind that in addressing cybersecurity threats that pose grave risks to our nation, we must aim to seize the unparalleled opportunity the U.S. government and other U.S. stakeholders in the internet and communications ecosystem have to reap the tremendous benefits that the Internet of Things ("IoT") can provide. It is possible – and desirable – for policymakers to protect American citizens through fostering innovative

[1] The Consumer Technology Association ("CTA")™ is the trade association representing the $321 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] Department of Commerce, National Telecommunications and Information Administration, *Promoting Stakeholder Action Against Botnets and Other Automated Threats,* Request for Comments, 82 Fed. Reg. 27,042 (June 13, 2017) ("RFC").

developments that bolster the U.S. economy and cement continued U.S. global leadership in technology and cybersecurity.

As the RFC notes, while the "open and distributed nature of the digital ecosystem has led to unprecedented growth and innovation in the digital economy" – led by CTA member companies – this growth and innovation have "been accompanied by risks that threaten to undermine that very ecosystem."[3] The significant increase in the market for smart, connected devices, combined with high-profile data breaches and cybersecurity incidents, has thrust the technology industry into a national conversation about the privacy and security of its products. As the RFC explains and CTA members fully recognize, "With connected devices/IoT, there is an urgent need for coordination and collaboration across a diverse set of ecosystem stakeholders."[4] Indeed, cyber threats are very real, and all stakeholders must address them seriously and substantively – most effectively by developing and launching dynamic and innovative solutions informed by intelligent cybersecurity standards and best practices.

CTA works with its members to manage this complex environment using a comprehensive strategy of member education, outreach to regulators, thoughtful responses to legislative initiatives, and promotion of effective industry self-regulatory frameworks and standards. For example, in addition to participating in NIST's recent proceeding on proposed revisions to its Cybersecurity Framework,[5] CTA has provided technical security guidance for a number of audiences, including a technical report (CTA TR-12) titled *Securing Connected*

[3] RFC at 27,042.

[4] *Id.*

[5] Comments of the Consumer Technology Association (filed Apr. 4, 2017), https://www.nist.gov/sites/default/files/documents/2017/04/19/2017-04-10_-_cta.pdf; *see also* Department of Commerce, National Institute for Standards and Technology, *Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity*, Request for Comments, 82 Fed. Reg. 8408 (Jan. 25, 2017).

Devices for Consumers in the Home,[6] security best practices and an online checklist for connected home dealers and professionals,[7] and has issued public service announcements in radio markets reaching 2.2 million people. Some CTA members are also members of industry groups that have developed cybersecurity resources for consumers and best practices for home security,[8] and some have collaborated with NIST on programs like its Cyber-Physical Systems Program and Cybersecurity for IoT Program.[9]

CTA welcomes this new opportunity to work with NTIA and the Department of Commerce ("the Department") to improve the resilience of the internet and communications ecosystem and encourage collaboration among stakeholders to that end. The government has an important role to play as a nimble convener and educator, rather than a static regulator. The RFC aptly notes that because "poorly considered action would likely create significant unnecessary costs and unintended consequences," the preference is for "substantial, carefully considered

[6] 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.

[7] 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.

[8] 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).

[9] CTA regularly engages regulators on these issues. *See, e.g.*, Comments of the Consumer Technology Association, *Connected Cars Workshop*, Project No. P275403 (FTC filed Apr. 28, 2017); Comments of the Consumer Technology Association, *The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things*, Docket No. 170105023-7023-01 (filed Mar. 13, 2017); Comments of the Consumer Technology Association f/k/a the Consumer Electronics Association, *The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things*, Docket No. 1603311306-6306-01 (filed June 2, 2016).

action," and that the government's approach "is most likely to be effective and efficient if built on engagement from all stakeholders across the ecosystem."[10]

By emphasizing a preference for industry-led processes, the RFC reflects the sensible approach embraced by the administration as a whole. CTA applauds NTIA for undertaking this initiative in a well-coordinated series of industry-led processes that collectively can serve as a model for future cybersecurity policymaking in the months and years to come. In addition to this RFC, the two other primary workstreams of this initiative both call on the expertise of private sector stakeholders: the July 11-12 workshop on Enhancing Resilience of the Internet and Communications Ecosystem hosted at NIST's National Cybersecurity Center of Excellence ("NCCoE"), and the Department of Homeland Security's ("DHS") directive tasking the National Security Telecommunications Advisory Committee ("NSTAC") with the delivery of a report on technical and operational solutions to the botnet challenge.

Industry is already on the front lines of the nation's defense against malicious cyber actors. Chip makers are offering secured system-on-a-chip components for IoT devices,[11] platform services are offered to provide end-to-end security and management of IoT devices,[12]

[10] RFC at 27,043.

[11] 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 are many, but they 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 (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/). Again, these are only a few examples.

[12] Samsung offers the Artik IoT ecosystem (http://developer.samsung.com/artik); Panasonic is providing a cloud services toolkit (http://shop.panasonic.com/about-us-latest-news-press-releases/10192015-

and many other segments are responding in similar fashion. With the NTIA, NIST, and DSH processes outlined above, the administration has rightly put industry at the forefront of the policymaking that undergirds this defense posture.

Through its previous and ongoing work in different areas, such as drone privacy and Internet of Things security upgradability and patching, NTIA likewise has demonstrated its ability to provide a forum in which stakeholders develop practices that address challenging and important cybersecurity issues. As discussed below, those efforts provide a vehicle for advancing collaboration with respect to botnet mitigation that has already been tested and can be leveraged immediately.

With these stakeholder-driven processes and industry solutions in mind, CTA recommends that NTIA and the Department advance four guiding principles that are common to a diverse variety of industry sectors:

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

(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.

These principles underlie much of CTA's responses to individual questions below.

cloudservicetoolkit.html); 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).

The RFC appropriately focuses on botnets because their automated, distributed attacks affect large sets of victims, create economically damaging disruption, and threaten the broader network and users beyond any one company or sector. CTA appreciates the RFC's recognition that "[t]he private sector is … playing a key role in tackling botnets," including ISP notifications to customers affected by an attack and standards bodies offering guidance on how to mitigate some attacks.[13] The RFC notes that technology providers "are innovating around tools to protect resources from DDoS attacks," such as working to eliminate application and software exploitable vulnerabilities.[14]

While the RFC gets a lot right, CTA cautions that the RFC's broad assertion about device security – specifically, that "IoT devices are often built and deployed without important security features and practices in place"[15] – is ripe for misinterpretation that would overlook the market-changing innovations driven by numerous manufacturers who are prioritizing security in designing and deploying their products in the global consumer technology marketplace. As noted above,[16] CTA member companies are taking bold leadership roles in implementing strong and innovative security practices for connected devices, including measures specific to combating botnets and other distributed and automated cyber threats.

In these comments, CTA brings to bear the experience of its members in addressing IoT security concerns in general, and botnet defenses in particular.

[13] RFC at 27,043.

[14] *Id.*

[15] *Id.*

[16] *See supra* at 4-5 & nn.11-12.

II. RESPONSES TO QUESTIONS IN THE RFC

A. Question 1: What works. What approaches (e.g., laws, policies, standards, best practices, technologies) work well for dealing with automated and distributed threats today? What mechanisms for cooperation with other organizations, either before or during an event, are already occurring?

As the Department has recognized through its groundbreaking work as a convener, cybersecurity demands a flexible approach. There is a consensus among security experts that traditional one-size-fits-all, prescriptive, compliance-based approaches limit growth potential, discourage evolution in best practices, and prevent the development of new security solutions. Innovation, especially for technology and cybersecurity, must come in all shapes and sizes.[17] Rapidly changing technologies require flexibility and constant industry adaptation that cannot be achieved through compliance with prescriptive rules. Indeed, locking in specific requirements would be counterproductive, potentially delaying or even derailing the launch of new security approaches.

In contrast, the NTIA multistakeholder processes on vulnerability research and disclosure and IoT security patching and updating have empowered stakeholders to step forward and provide meaningful advances on these issues.[18] Similarly, the NIST-led process through which industry and numerous stakeholders developed the NIST Cybersecurity Framework embodies the sort of approach that encourages effective cybersecurity practices and innovation and, consequently, can help the U.S. unleash economic growth and maintain its global leadership role in technology. CTA's membership includes manufacturers occupying various parts of the supply

[17] *See, e.g.*, Department of Commerce, *Stakeholder Engagement on Cybersecurity in the Digital Ecosystem*, 80 Fed. Reg. 14360 (Mar. 19, 2015) (recognizing that traditional regulation in this context is "difficult and inefficient" in light of the "pace of innovation in the highly dynamic digital ecosystem").

[18] *See, e.g.*, NTIA Multistakeholder Process: Internet of Things (IoT) Security Upgradeability and Patching, https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security (providing research reports and other materials prepared by working groups); NTIA Multistakeholder Process: Cybersecurity Vulnerabilities, https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities (same).

chain and service providers relying on multiple technologies, and ranges from large household names to entrepreneurial startups. As a result of this diverse membership, CTA recognizes many of the benefits of the NIST Cybersecurity Framework's common language and non-regulatory, flexible approach to cyber risk management. Through industry input, the voluntary guidance can evolve with the technology industry and create a step-by-step process for establishing strong cyber hygiene. Companies can utilize and adapt this approach in response to the constantly evolving threat environment. Such processes can be a vehicle to empower the experts and the most directly interested parties to develop solutions that actually work, that can be implemented, and that the stakeholders themselves can own.

The NIST Cybersecurity Framework does not constitute a complete solution to the challenge for companies to develop design and develop secure products, nor is it intended to do so. To meet this need, there are a number of complementary process guidelines and toolkits available from the many expert organizations in industry, such as the BSIMM[19] and Microsoft SDL.[20] Still, the process by which NIST facilitated industry's development of Cybersecurity Framework is an excellent example of the kind of role the government can play to give the private sector active ownership of cyber risk management. It therefore serves as one model for the best way to address the security challenges associated with the IoT – through industry insights and expertise.

In short, these past efforts set the stage for moving forward with this initiative to reduce malicious botnets and other automated and distributed threats. Coordinated with parallel industry-led efforts such as the NSTAC report and recommendations on technical and

[19] *See* Synopsys Software Integrity Group, Building Security In Maturity Model, https://www.bsimm.com.

[20] *See* Microsoft Security Development Lifecycle, https://www.microsoft.com/en-us/sdl.

operational solutions to the botnet challenge, these processes should provide the engine for the relevant parts of the broader botnet reduction initiative and should pave the way for follow-on inquiries that build on this ongoing work. Industry-driven policy processes like these allow the private sector companies that are closest to the front lines of the operational cybersecurity challenges to take the lead in developing effective cybersecurity policies. The government should make these types of processes central to cybersecurity policymaking.

B. Question 2: Gaps. What are the gaps in the existing approaches to dealing with automated and distributed threats? What no longer works? What are the impediments to closing those gaps? What are the obstacles to collaboration across the ecosystem?

Gaps in information and awareness among different stakeholders in the ecosystem – government, vendors, service providers, device manufacturers, software developers, end users, and myriad other players – present a significant challenge in addressing cyber threats. When some stakeholders individually, or all stakeholders collectively, are less informed than the malicious actors who seek to cause harm, it is difficult – if not impossible – to effectively respond to threats.

Within the United States, education and awareness is a challenge that must be addressed holistically. No single entity can reach out to all the necessary parties—from manufacturers to retailers to installers to consumers. CTA works to educate member companies and the broader public, but much more needs to be done to close these gaps, in a broad public-private partnership. Internationally, other nations must address this challenge in partnership with the United States. Approximately 90 percent of the devices that enabled the Mirai botnet's attack on Dyn were located outside the United States[21] – and were developed, manufactured, sold, and

[21] *See, e.g.*, Imperva Incapsula, *Breaking Down Mirai: An IoT Botnet DDoS Analysis*, Figure 3 (Oct. 26, 2016), https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html.

distributed outside the United States by companies that do not perform to the standards that CTA members promote.[22] The lack of basic security in some parts of the global ecosystem, such as using default or weak "admin" account authentication,[23] makes clear the need for a more global education push. CTA, and organizations like CTA, can reach broad elements of the ecosystem, but more must be done in well-coordinated industry-government efforts globally.

Overcoming these gaps requires effective teamwork and collaboration, information sharing about the threats and solutions, and awareness of which players are responsible for what actions and when. Industry and government must work together to promote clarity on these matters, regarding both understanding the specific contours of the threats and also in promoting dynamic solutions that the market can employ to address those threats. As discussed above in Question 1 and below in Questions 3 and 7, CTA believes that industry-driven processes convened and facilitated by the Department are a highly effective way to direct the action that will achieve these goals.

C. Question 3: Addressing the problem. What laws, policies, standards, practices, technologies, and other investments will have a tangible impact on reducing risks and harms of botnets? What tangible steps to reduce risks and harms of botnets can be taken in the near term? What emerging or long term approaches may be promising with more attention, research, and investment? What are the public policy implications of the various approaches? How might these be managed, balanced, or minimized?

In the near term, the NTIA multistakeholder processes on vulnerability research and disclosure and IoT security patching and updating provide forums to carry out additional botnet reduction initiatives. Put simply, there is no value in reinventing or duplicating a process that is

[22] *See, e.g.*, Krebs on Security, *Who Makes the IoT Things Under Attack?*, Oct. 3, 2016, https://krebsonsecurity.com/2016/10/who-makes-the-iot-things-under-attack/; *Dahua Releases Statement on Mirai Botnet Attack*, SDM Magazine, Oct. 24, 2016, http://www.sdmmag.com/articles/93040-dahua-releases-statement-on-mirai-botnet-attack.

[23] *See, e.g.*, Krebs on Security, *Dahua, Hickvision IoT Devices Under Siege*, Mar. 10, 2017, https://krebsonsecurity.com/2017/03/dahua-hikvision-iot-devices-under-siege/.

delivering stakeholder consensus on important market-oriented advances. Just two weeks ago, stakeholders reached consensus on recommendations for device manufacturers to communicate IoT device security update capabilities to consumers in order to create a more informed and security-minded marketplace for IoT devices.[24] In the coming months, CTA will be working with NTIA and stakeholders to promote adoption of these recommendations.

In the longer term, CTA recommends that the Department closely review the NSTAC report when it is available and coordinate with DHS and other agencies to undertake additional new multistakeholder processes to address botnets. Issues that would benefit from discussion in an NTIA-led multistakeholder process include:

1. The economics, incentives, and barriers regarding "security by design" at the front end of product development.
2. The open source community's possible role in advancing IoT security and botnet reduction through advances in software.
3. Advances that chip manufacturers may be able to contribute to the foundation of the market for secure IoT devices.
4. Solutions that are developing at the local area network level such as smart home routers and at the internet access level, such as manufacturer usage descriptions.
5. Developing solutions on the consumer side of the ecosystem regarding "orphan device" and "end of life" challenges for IoT devices.

The government also should consider longer-term solutions, most importantly institutionalizing its support for and promotion of private sector-driven processes like the NTIA multistakeholder processes and the NIST Cybersecurity Framework, as well as advisory committees such as the NSTAC, the Communications Security, Reliability, and Interoperability

[24] *See* NTIA Multistakeholder Process: Internet of Things (IoT) Security Upgradeability and Patching, Working Group recommendations on Communicating IoT Device Security Update Capability to Improve Transparency for Consumers, https://www.ntia.doc.gov/files/ntia/publications/draft_communicating_iot_security_update_capability_-_jul_14_2017_-_ntia_multistakeholder_process.pdf.

Council ("CSRIC"),[25] and others. Processes like these should be the beginning foundation – and remain at the center – of all policymaking activities regarding cybersecurity. As such, they should be fully funded and should have the enthusiastic support of the U.S. government at every level, from the White House to Cabinet Secretaries and agency heads to career civil servants.

Additionally, government should continue to support industry research and development and do everything possible to facilitate the launch of new, innovative products that will enhance security, such as block chain technology. To do so, policymakers should seek opportunities to advance education on global design and manufacturing.

Finally, as discussed further below in Question 5, the government should also develop formal legal mechanisms for companies that choose to engage candidly with government to defend against cyber criminals and nation state adversaries to do so without fear of exposing themselves to legal risk.

D. Question 4: Governance and collaboration. What stakeholders should be involved in developing and executing policies, standards, best practices, and technologies? What roles should they play? How can stakeholders collaborate across roles and sectors, and what should this collaboration look like, in practical terms?

As discussed above in response to Question 2 regarding gaps, there is a need to clarify the roles and responsibilities of the various players in the consumer IoT ecosystem. In general, every stakeholder in the internet and communications ecosystem has a role to play in addressing this challenge. The RFC focuses on "two broad approaches where substantial progress can be made" that directly apply to CTA's diverse membership: (1) attack mitigation – minimizing impact of botnet behavior by rapidly identifying and disrupting malicious behaviors, including

[25] CSRIC advises and makes recommendations to the Federal Communications Commission for promoting the security, reliability, and resiliency of the nation's communications systems. *See* Communications Security, Reliability, and Interoperability Council VI, https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council.

potential of filtering or coordinated network management, empowering market actors to better protect potential targets, and reducing known and emerging risks; and (2) endpoint prevention – securing endpoints, especially IoT devices, and reducing vulnerabilities, including fostering prompt adoption of secure development practices, developing practical plans to rapidly deal with newly discovered vulnerabilities, and supporting adoption of new technology to better control and safeguard devices at the local network level.

Addressing distributed threats requires distributed solutions – including those that fit fully within the attack mitigation and endpoint prevention approaches, as well as those that are developing in the dynamic and innovative cross-sector markets between and around them. Devices and networks need to work against unauthorized traffic in order to reduce the severity of botnet attacks. On the device side, manufacturers have a valuable role to play in advancing security innovations and best practices in design and deployment, push security updates, and other advances. On the network side, industry should continue exploring approaches like manufacturer usage description, "smart routers" and related techniques that make the network aware of the types of traffic that should come from uncompromised devices. The government can best encourage these developments by providing room for the market to drive advancements and innovations in these areas, without tipping the scale toward any particular approach or technology. Further industry-driven processes convened by NIST and NTIA to these ends would be valuable.

E. Question 5: Policy and the role of government. What specific roles should the Federal government play? What incentives or other policies can drive change?

Government's primary role should be very clear and reliable – namely, to support the companies and consumers that are on the front lines of this criminal and national security challenge. The nation's infrastructure, supply chains, and connected services and devices will be more securely protected when government serves as a nimble convener and facilitator of industry-driven processes, rather than a top-down regulator of static compliance requirements. Government should continue and augment the processes that comprise this botnet reduction initiative, guided by the principles for cybersecurity policy highlighted above.

Additionally, at a fundamental level, government must always be on the same team as its private sector partners as they face sophisticated criminals and nation state adversaries. This means that when government knows of a software vulnerability that can be exploited, it must work with the company in question to address that vulnerability. This also means that the government should endeavor to avoid undercutting private sector companies with "punish the victim" enforcement actions and lawsuits. Companies should have the option to work candidly with the government to address these threats, in exchange for protection against legal liabilities and related risks.

Policymakers and regulators should also avoid creating regulatory "silos" that confuse industry and consumers with inconsistent regulatory approaches. Instead, regulatory responsibilities should be clarified and streamlined in order to avoid duplication among agencies. CTA supports implementation of a consistent approach on privacy and security, building on the expertise of cross-cutting agencies such as the FTC, NIST, NTIA, and other agencies, as appropriate – again, always guided by the market-oriented principles and industry-driven processes articulated above. In this regard, CTA believes that the FTC's explicit support for NTIA's multistakeholder process on IoT security patching and updating is an encouraging sign for future collaboration.[26]

[26] *See* FTC Public Comment on "Communication IoT Device Security Update Capability to Improve Transparency for Consumers" to the Communicating Upgradability and Improving Transparency Working Group, Multistakeholder Process on Internet of Things Security Upgradability and Patching, NTIA, at 5-6, https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-comment-national-

In addition, the government should incentivize industry to prevent vulnerabilities from being coded. For instance, the government should support industry in strengthening efforts among security professionals to look for vulnerabilities and anomalies that have not yet been detected, and work to provide remediation in coding.[27]

While prevention of vulnerabilities in coding should be a top priority, as the next layer of remediation, government can promote the identification of security vulnerabilities before they are exploited. Beyond the NTIA multistakeholder process on vulnerability research and disclosure mentioned above,[28] other examples that may have relevance in this context are "bug bounty" programs that allow security researchers to identify vulnerabilities in software devices for a reward; and similarly "bug notification" programs that allow security researchers to identify such vulnerabilities but do not necessarily include a monetary reward. The U.S. government has promoted such competition through the Department of Defense's "Hack the Pentagon" program; more than 1,400 hackers participated in the first program and identified 138 legitimate vulnerabilities.[29] The program was widely considered a success and a value based on its low cost, and was quickly replicated.[30] Additional proactive approaches that prevent vulnerabilities in the first place, and, to a lesser extent, reactive bug bounty and bug notification programs could

telecommunications-information-administration-communicating-iot-device-security/170619ntiaiotcomment.pdf ("FTC IoT Patching Comment") ("[T]he Commission commends the inclusive voluntary multistakeholder process in which industry, government, and consumer representatives have developed the Elements of Updatability. … Voluntary, consensus-based guidelines developed through such processes can have a strong advantage over government regulation in that they can be adapted to specific circumstances and can be updated relatively easily over time.").

[27] *See, e.g.*, DevSecOps: Security as Code, http://www.devsecops.org/.

[28] *See* NTIA Multistakeholder Process: Cybersecurity Vulnerabilities, *supra* note 18.

[29] *See* Hack the Pentagon, https://www.hackerone.com/resources/hack-the-pentagon.

[30] *See* Announcing Hack the Army, https://www.hackerone.com/blog/announcing-hack-the-army.

help the federal government and other stakeholders both prevent and address vulnerabilities that can be exploited to form botnets.

Finally, the federal government should be clear that regulating IoT devices on a state level would restrict and harm industry and innovation – including security innovation – without offering appreciable benefits to consumers.

F. Question 6: International. How does the inherently global nature of the internet and the digital supply chain affect how we should approach this problem? How can solutions explicitly address the international aspects of this issue?

Distributed and automated cyber threats do not respect borders. As discussed above in Question 3, approximately 90 percent of the devices that enabled the Mirai botnet attack were located outside the United States and were developed and deployed outside the United States by companies whose security practices fall short of the high standards that CTA members promote.[31] This is a global market challenge, and therefore, the United States and other advanced market-based economies with strong legal institutions must address this challenge together. No single country can solve this problem alone, but formal well-coordinated multifaceted efforts by multiple like-minded governments, and the innovative private sector companies that drive their economies, can change the terrain to defend against malicious botnets.

G. Question 7: End users. What can be done to educate and empower users and decision-makers, including enterprises and end consumers?

Consumer awareness is an important element of promoting a dynamic market for secure products, and as described above, CTA has a successful history of engaging in consumer education campaigns regarding the potential and the limitations of technology.[32] In that regard,

[31] *See supra* notes 21-23 and accompanying text.

[32] *See supra* notes 6-8 and accompanying text (describing select CTA efforts including technical report (CTA TR-12) titled *Securing Connected Devices for Consumers in the Home*).

CTA has seen what works and what does not when it comes to notifications. For instance, in many cases, too much notice to consumers may well be too much of a good thing. In this respect, CTA agrees with the FTC's warnings about over-notification.[33] Additionally, as proposals for so-called "nutrition labels" appear to have garnered some appeal, we caution that such approaches to consumer notification can suffer from key shortcomings – in particular, inflexibility that does not evolve with technology.

As noted above, CTA strongly supports efforts to promote effective means of informing consumers of key security considerations such as those the consensus recommendations produced last week in NTIA's multistakeholder process on IoT security patching and updating.[34] We will be promoting adoption of these recommendations in the months ahead. More broadly, CTA looks forward to working with NTIA, other relevant government agencies, and other industry stakeholders in the coming months and beyond to advance truly effective consumer education and awareness initiatives and to empower consumers in their role in advancing the nation's cybersecurity.

III. CONCLUSION: SHARED RESPONSIBILITY AND NEXT STEPS

Protecting our nation's cybersecurity must be a shared responsibility throughout the internet/communications ecosystem, and government should avoid facile solutions that rely on one or two particular components. The challenges are further complicated by the international nature of the threat and the need to work across borders. Each player in the internet and communications ecosystem has an important role to play, and CTA and its members commit to

[33] *See* FTC IoT Patching Comment at 6 ("Poor disclosures, including overly extensive disclosures, can actually impede consumers' ability to make informed choices."); *id.* at 9-10 ("[T]he more extraneous information consumers receive, the more likely they are to feel overburdened by choice and ignore critical information.").

[34] *See* Working Group recommendations on Communicating IoT Device Security Update Capability to Improve Transparency for Consumers, *supra* note 24.

being an important part of finding solutions to these challenges. CTA pledges to engage in these processes throughout the remainder of this year and beyond to make progress on some of the hardest questions our nation faces.

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

July 28, 2017