Before the
DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration

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

COMMENTS OF CTIA

Thomas C. Power
Senior Vice President and General Counsel

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

John M. Marinho
Vice President, Technology and Cybersecurity

Melanie K. Tiano
Director, Cybersecurity and Privacy

CTIA
1400 Sixteenth Street, NW, Suite 600
Washington, DC 20036
(202) 785-0081
www.ctia.org

July 28, 2017

TABLE OF CONTENTS

I. INTRODUCTION AND SUMMARY. 1

II. NATIONAL CYBER POLICY HAS FOCUSED ON PARTNERSHIPS AND INNOVATION, LED BY THE WIRELESS AND INTERNET ECOSYSTEMS. 4

A. The Private Sector Has Been Doing Its Part To Secure the Nation's Communications Infrastructure. 4

B. Public-Private Partnerships and Voluntary Collaboration Must Remain the Bedrock of Federal Cyber Policy. 8

C. The Communications Sector Is Aggressively Addressing Security in Next Generation Networks. 9

III. INDUSTRY HAS BEEN ADDRESSING BOTNETS AND OTHER COMPLEX GLOBAL ATTACKS. 10

IV. "ATTACK MITIGATION" AND "ENDPOINT PREVENTION" ARE COMPLEMENTARY CONCEPTS THAT WILL IMPROVE AS ENDPOINT PROTECTION MATURES. 13

V. NTIA'S QUESTIONS REVEAL CREATIVE STEPS THAT CAN HELP MITIGATE RISKS OF BOTNETS AND DDOS ATTACKS 15

A. What Works: Public-Private Partnerships Should Be Protected and Expanded. 15

B. Gaps: Collaboration May Be Stymied by Fear of Liability and Regulatory Uncertainties.16

C. Addressing the Problem: NTIA Should Clarify Legal Uncertainties To Foster More Activity, and Promote International Law Enforcement. 19

D. Governance and Collaboration: NTIA Should Foster Wider Participation in U.S. Digital Strategy and Champion U.S. Leadership in International Standards. 21

E. Role of Government: The Government Should Improve Its Own Cyber Hygiene and Only Act Where Necessary To Fill a Gap in Market Activity. 22

F. International: The Global Nature of the Internet and Digital Supply Chain Make Global Coordination and U.S. Leadership Imperative. 24

G. Users: NTIA Should Think Big in Educating Consumers and Enterprise Users About Their Role in Our Digital Future. 26

VI. CONCLUSION. 28

Before the
DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration

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

COMMENTS OF CTIA

CTIA[1] responds to the Department of Commerce's and the National Telecommunications and Information Administration's ("NTIA's") Notice and Request for Public Comment on promoting action against botnets and other automated threats (the "*Request*").[2] The *Request* implements Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure."[3] CTIA appreciates the opportunity to provide input as NTIA helps the President address automated and distributed attacks, including botnets.

I. INTRODUCTION AND SUMMARY.

Cybersecurity is a top priority for the wireless and Internet industries. In recent years, countries around the world have faced major cyber attacks by criminals and agents of foreign governments, with attacks penetrating public and private infrastructure alike. Botnets have become a favored attack method, enabling rapid control of several thousand or even millions of

[1] CTIA® (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st century connected life. The association's members include wireless carriers, device manufacturers, suppliers as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. The association also coordinates the industry's voluntary best practices, hosts educational events that promote the wireless industry and co-produces the industry's leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

[2] *Request for Comments on Promoting Stakeholder Action on Botnets and Other Automated Threats,* 82 Fed. Reg. 27042 (Jun. 13, 2017) ("Request").

[3] Exec. Order No. 13800, 82 Fed. Reg. 22391 (May 11, 2017).

devices at one time. Automated and distributed attacks present a challenge to the future of innovation and connectivity. The President's interest is well-placed.

The communications and Internet ecosystems have been actively responding to botnets and other cybersecurity risks for years. Companies work with global peers in international standards bodies. They have partnered with the Department of Homeland Security ("DHS") in venues like the National Cybersecurity and Communications Integration Center ("NCCIC") and U.S. Computer Emergency Readiness Team ("US-CERT") for decades. The sector helped shape and has been implementing the National Institute of Standards and Technology's ("NIST's") *Framework for Improving Critical Infrastructure Cybersecurity* ("*Cybersecurity Framework*"). Companies use sophisticated filtering and other techniques to thwart attacks daily. And they are building new system architectures and software defined networks that will support enhanced security in Fifth Generation ("5G") wireless networks.

NTIA has a tremendous opportunity to support this work and help the United States develop a roadmap of short-term, mid-term, and long-term actions to address these attacks. The key to addressing threats posed by botnets is continued focus on attack mitigation, which has been successful, and a longer-term emphasis on endpoint prevention backed by thoughtful product development and consumer education. In preparing a report to the President, NTIA should:

- Describe the challenge, identify what government and industry are doing to address it, and place it in appropriate context. This includes explicit recognition that U.S. action alone cannot address this global challenge.

- Encourage broader U.S. government participation in international standards work, where other countries are advancing their preferences. The U.S. government must help U.S. industry champion open, transparent efforts to shape the future of 5G wireless networks.

- Capitalize on extensive private sector research, including the Communications Sector Coordination Council's ("CSCC") recent white paper on botnets,[4] which identifies opportunities and proposes actionable steps that ecosystem participants can take.

- Reinforce the importance of longstanding public-private partnerships instead of regulation.

- Look at how to include more manufacturers and developers in the hard work of improving endpoint security.

- Consider creative solutions to existing obstacles to collaboration, such as legal uncertainty about information-sharing and attack mitigation.

- Work to prevent divergent federal and state regulatory efforts, which can consume resources and foster uncertainty.

- Encourage the aggressive prosecution of cybercriminals and work to take down the infrastructure they exploit to harm our citizens and economy.

- Support cybersecurity workforce development, as needs are identified by industry.

- Promote a national consumer awareness campaign to prepare citizens for their role in securing the future digital economy.

- Champion the free market as the most effective way to promote innovation and security.

CTIA describes in Part II the longstanding partnerships that form the bedrock of federal cyber policy. In Part III, we describe the threat from automated and distributed attacks, and put it in context. Part IV addresses NTIA's focus on attack mitigation and endpoint prevention, explaining the criticality of secure endpoints. In Part V, we address the questions posed by NTIA, which illustrate opportunities for federal action.

[4] Communications Sector Coordinating Council, *Industry Technical White Paper* (July 17, 2017) ("CSCC White Paper"), https://docs.wixstatic.com/ugd/0a1552_18ae07afc1b04aa1bd13258087a9c77b.pdf.

II. NATIONAL CYBER POLICY HAS FOCUSED ON PARTNERSHIPS AND INNOVATION, LED BY THE WIRELESS AND INTERNET ECOSYSTEMS.

The wireless and Internet industries are leading on cybersecurity, through public-private partnerships in the United States and globally. Incentives for the communications sector to manage cyber risk are aligned to promote voluntary action. For efforts to succeed, cybersecurity policy must continue to emphasize collaboration and risk-management, and avoid prescriptive regulation.

A. The Private Sector Has Been Doing Its Part To Secure the Nation's Communications Infrastructure.

NTIA aptly recognizes the private sector's role, observing that:

> [t]he private sector is also playing a key role in tackling botnets. Internet service providers in the United States and around the world have been experimenting with how to notify customers that their devices may be involved in an attack. Standards bodies have offered guidance on how to mitigate some styles of attacks. Technology providers are innovating around tools to protect resources from DDoS attacks. Application and software manufacturers are working to eliminate exploitable vulnerabilities. This community has worked hard to address the threats over the last decade.[5]

Cybercrime imposes considerable costs on the private sector.[6] Due to the recent Mirai botnet attack, Dyn lost an estimated 8% of its business,[7] and the impact on Mirai-affected sites is estimate to have averaged $22,000 per minute of downtime.[8] Other attacks deprive companies of

[5] Request at 27043 (internal citation omitted).

[6] NIST, *Impacts: Cybersecurity*, https://www.nist.gov/industry-impacts/cybersecurity (explaining that cyberattacks cost businesses $400B per year).

[7] Sam Varghese, *DDoS attack on Dyn costly for company: claim*, iTWire, (Feb. 6, 2017), https://www.itwire.com/security/76717-ddos-attack-on-dyn-costly-for-company-claim.html.

[8] Ponemon Institute & Radware, *Cyber Security on the Offense: A Study of IT Security Experts*, at 1 (Nov. 2012), https://security.radware.com/uploadedfiles/resources_and_content/attack_tools/cybersecurityontheoffense.pdf.

the benefits of their investments, as in the Sony hack, or their data, as with WannaCry. Attacks have real costs for businesses and customers.

For the communications sector, cybersecurity is key to network viability. Companies are eager to bring consumers ultra-fast, high capacity, and secure Internet services that will change how Americans receive health care, shop, commute, and interact with our environment, among other things. To achieve this, companies start with security in designing technologies (*i.e.*, software-defined networks, new authentication methods, integrated hardware and software products); we invest in research and development; and we respond to threats. There has been a 3,198% increase in vulnerability scans of IoT devices over the past 3 years.[9]

Industry commitment to security is evident in a variety of efforts. One example is the *U.S. Anti-Bot Code of Conduct (ABCs) for Internet Service Providers (ISPs)* ("*Anti-Botnet Code of Conduct*").[10] Although the threat landscape has since changed, the *Anti-Botnet Code of Conduct* —the product of the Federal Communications Commission's ("FCC's") Communications Security, Reliability, and Interoperability Council ("CSRIC") III—helped ISPs improve security and identified risks posed by bots. It encouraged education, particularly with enterprise users, and revealed challenges in consumer notification. In addition:

- Industry works with domestic and international standards bodies—like 3rd Generation Partnership Project ("3GPP"), Institute of Electrical and Electronics Engineers, Inc. ("IEEE"), oneM2M Partners ("oneM2M"), Alliance for Telecommunications Industry Solutions ("ATIS"), and GSM Association ("GSMA").

[9] Chris Boyer, *How the Public Safety Bureau Paper Gets Cybersecurity Wrong*, AT&T Public Policy Blog (Jan. 25, 2017), https://www.attpublicpolicy.com/cybersecurity/how-the-public-safety-bureaupaper-gets-cybersecurity-wrong/.

[10] Communications Security Reliability and Interoperability Council (CSRIC) III, *U.S. Anti-Bot Code of Conduct (ABCs) for Internet Service Providers (ISPs)*, Final Report, WG 7 (Mar. 2012), https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-ReportFinal.pdf.

- Companies receive and provide federal agency input, for example, at the FCC's CSRIC and Technological Advisory Council ("TAC"). CSRIC V in 2017-18 will explore topics from public safety to secure hardware and software-security by design, WiFi, workforce, information sharing, and network timing single source risk reduction.[11]

- Businesses use NIST's *Cybersecurity Framework*.[12] In the communications sector, CSRIC IV spent 2014 and 2015 with approximately 100 subject-matter experts mapping the *Cybersecurity Framework*.[13]

- Industry groups like CTIA's Cybersecurity Working Group ("CSWG") address issues like automated indicator sharing, authentication, and distributed attacks. We respond to changes in the market. For example, the ecosystem is constantly refining how to communicate vulnerability information among Operating System ("OS") providers, manufacturers, and carriers.[14]

This work is effective. As Dr. Charles Clancy testified to Congress, U.S. networks are secure, particularly relative to other countries.[15] For example, "an average of 0.03% of smartphones per week—out of tens of millions of mobile devices on the Verizon network—were

[11] FCC, Open Data, *CSRIC Best Practices*, https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/data.

[12] NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[13] *See* CSRIC IV, *Cybersecurity Risk Management and Best Practices*, Final Report, WG 4 (Mar. 2015), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

[14] *See* Android, *Android Security Bulletin—August 2016* (Aug. 1, 2016), https://source.android.com/security/bulletin/2016-08-01.html; CVE Details, *Google Android: List of Security Vulnerabilities*, https://www.cvedetails.com/vulnerability-list/vendor_id-1224/product_id-19997/Google-Android.html.

[15] *Promoting Security in Wireless Technology, Hearing Before the House Energy and Commerce Committee, Communications and Technology Subcommittee*, 115th Congress (June 13, 2017) (statement of Dr. Charles Clancy), http://docs.house.gov/meetings/IF/IF16/20170613/106104/HHRG-115-IF16-Transcript-20170613.pdf ("[T]he United States has the most secure wireless infrastructure in the world."). Indeed, a recent ITU report ranked the United States in the top three countries in the Americas region, noting, in particular, its capacity building and cooperation with other countries in coordinating cybersecurity. ITU-D, *Global Cybersecurity Index (GCI) 2017*, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf.

infected with ‘higher-grade’ malicious code. This is an even tinier fraction than the overall 0.68% infection rate reported.”[16]

Industry collaboration has helped the United States take down botnets. In July 2017, the Department of Justice (“DOJ”) took down two major online marketplaces, AlphaBay and Hansa, with cooperation from foreign governments.[17] The Federal Bureau of Investigation (“FBI”) led an extensive effort to dismantle the Kelihos botnet this year—a global network of tens of thousands of infected computers that facilitated malicious activities, like harvesting login credentials, distributing hundreds of millions of spam e-mails, and installing ransomware.[18] In 2015, the FBI disrupted the Dridex botnet, a banking Trojan that breached thousands of organizations across the globe and caused more than $30.5 million in losses.[19] More can be done to strengthen law enforcement’s ability to disrupt and dismantle botnets. Efforts to streamline the Mutual Legal Assistance Treaty (“MLAT”) process are key. DOJ has a great resource in the Computer Crime and Intellectual Property Section (“CCIPS”) of the Criminal Division, and each of the U.S. Attorney’s offices can play a role.

[16] *See* Verizon, *2015 Data Breach Investigations Report*, at 19-20 (2015), http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report_2015_en_xg.pdf.

[17] Joe Uchill, *DOJ takes down dark net marketplaces*, The Hill (July 20, 2017, 10:37 AM), http://thehill.com/policy/cybersecurity/342904-doj-takes-credit-for-dark-net-markets-demise.

[18] Press Release, DOJ, *Justice Department Announces Actions to Dismantle Kelihos Botnet* (Apr. 10, 2017), https://www.justice.gov/opa/pr/justice-department-announces-actions-dismantle-kelihos-botnet-0.

[19] John Leyden, *FBI takes down Dridex botnet, seizes servers, arrests suspect*, The Register (Oct. 14, 2015), https://www.theregister.co.uk/2015/10/14/dridex_botnet_takedown/.

B. Public-Private Partnerships and Voluntary Collaboration Must Remain the Bedrock of Federal Cyber Policy.

Years ago, some legislators debated prescriptive cybersecurity obligations. But Congress and former President Obama concluded that the public and private sectors need to collaborate on voluntary efforts to secure critical infrastructure. In that vein, NIST created the *Cybersecurity Framework*, now under revision.[20] And Congress passed the Cybersecurity Information Sharing Act of 2015 ("CISA") to increase voluntary information-sharing.[21] Partnerships abound:[22]

- The CSCC enables critical infrastructure owners and operators, their trade associations, and other industry representatives to interact on a wide range of sector-specific strategies, policies, and activities. The CSCC just released an important white paper on botnets.[23]
- The NCCIC and US-CERT support real-time collaboration with communications and information technology companies.
- The National Security Telecommunications Advisory Committee ("NSTAC"), a committee of communications, network, and information technology companies appointed by the President, makes recommendations about security.
- CSRIC, an advisory committee to the FCC, makes recommendations to promote the security, reliability, and resiliency of communications systems.

Calls for prescriptive regulation are misguided because reporting obligations and regulatory oversight are more likely to impede than promote innovation. Cybersecurity risks evolve, so pre-defined solutions become obsolete. Regulations can provide bad actors with a roadmap for attack. And the ecosystem involves global players; domestic regulation cannot

[20] *See* NIST, *Framework for Improving Critical Infrastructure Cybersecurity, Draft Version 1.1 with Markup* (proposed Jan. 10, 2017) (*"Framework Draft Version 1.1*"), https://www.nist.gov/file/344211.

[21] Pub. L. 114-113, 6 U.S.C. § 1501.

[22] *See generally* CTIA, *Today's Mobile Cybersecurity: Information Sharing* (Sept. 2014) ("*CTIA White Paper on Information Sharing*"), https://www.ctia.org/docs/default-source/default-document-library/ctia_informationsharing.pdf.

[23] CSCC White Paper.

reflect differences and assign responsibility. The best way to address cybersecurity is through voluntary risk management and information sharing. Momentum must continue in that direction.

C. The Communications Sector Is Aggressively Addressing Security in Next Generation Networks.

Global communications companies are working on the next wave of technology, including a transition to all-digital, 5G technology, and the Internet of Things ("IoT"). Industry is putting in place enhanced security and network design, like improved encryption, distributed and secure architecture, and decentralized and adaptive security.[24]

- **Software-defined networking (SDN)** will improve security. SDN is an emerging architecture that decouples the network control and forwarding functions, enabling network control to become directly programmable. The architecture, combined with open, easily-programmable interfaces, makes it easier to mix and match solutions from different vendors and develop new capabilities, including for security. SDN will help network operators respond to threats due to the operator's central view of the network.

- **Network slicing** will allow 5G network operators to provide networks on an as-a-service basis. With network slicing, a single physical layer can be partitioned into multiple virtual networks, allowing operators to support different types of services for different customer segments. Operators can customize security for particular network slices to dynamically respond to threats.

- **Network virtualization** includes built-in security advantages, including isolation and multitenancy, segmentation, distribution firewalling, and service insertion and chaining.

5G is not a silver bullet. It will not solve the challenge of unmanaged or poorly designed devices and will not improve consumer awareness. Nor will the transition to IPv6 provide a perfect solution, particularly for mobile devices. IPv6 is promising and in some ways more secure than IPv4, but it may raise its own security challenges. With this relatively new network infrastructure and increasingly ubiquitous encryption, operators will vary in their ability to

[24] *See generally* CTIA, *Protecting America's Wireless Networks* (Apr. 2017), https://www.ctia.org/docs/default-source/default-document-library/protecting-americas-wireless-networks.pdf.

distinguish distributed denial-of-service ("DDoS") attacks from benign traffic. Endpoint security is key, as network-based solutions cannot address the challenge alone.

Diverse stakeholders must be involved. Operators are working internationally on efforts like blacklisting, which would benefit from additional participation. We have implemented GSMA best practices, such as network monitoring and filtering to mitigate issues, including those surrounding Signaling System 7 ("SS7"). The Broadband Internet Technical Advisory Group ("BITAG") issued in 2016 its *Internet of Things Security and Privacy Recommendations*[25] providing IoT device recommendations, including software best practices, authentication, encryption, and the critical role of the supply chain. As we saw at CTIA's Cybersecurity Summit in April 2017,[26] government and industry leaders agree that substantial progress is being made to address future challenges.

III. INDUSTRY HAS BEEN ADDRESSING BOTNETS AND OTHER COMPLEX GLOBAL ATTACKS.

Botnets are a fast-developing international challenge, facilitated by low user awareness and insecure endpoints. But botnets are not new. A "bot" is a type of malicious software – or malware – that allows an attacker to take control of an infected device. It is "a program that is installed on a system in order to enable that system to automatically (or semi-automatically) perform a task or set of tasks typically under the command and control of a remote administrator."[27] A "botnet," in turn, is a "network of Internet-connected end-user computing

[25] Broadband Internet Technical Advisory Group, *Internet of Things (IoT) Security and Privacy Recommendations* (Nov. 2016), https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf.

[26] CTIA, *CTIA Cybersecurity Summit 2017*, https://www.youtube.com/watch?v=7hGtQXnecvA

[27] CSCC White Paper at 7.

devices infected with bot malware that are remotely controlled by third parties for nefarious purposes."[28] Historically, botnets have been used to propagate spam,[29] but they can be programmed to do many things: coordinate DDoS attacks, automate identity theft, or host illegal content.[30] Botnets' core characteristics should inform policy.

- **Botnets are transnational, with infected devices in different countries, many of which are non-Western, emerging markets**. In the recent Mirai botnet, "IP addresses of Mirai-infected devices were spotted in 164 countries."[31] Botnet activity is moving to emerging markets and developing countries. In Mirai, "[t]he botnet IPs [we]re highly dispersed, appearing even in such remote locations as Montenegro, Tajikistan and Somalia."[32] According to one study, less than 11% of Mirai-infected devices identified were in the United States.[33] With other recent attacks, like Petya, U.S. networks—and the nation as a whole—emerged relatively unscathed. While no networks are impenetrable, our relative success to date is a testament to the security efforts of U.S. networks. This requires a collaborative approach to detection and mitigation.
- **Creators of botnets are skilled at hiding and have varied motives**. As CSRIC explained, "[b]ots are frequently used as part of coordinated Distributed Denial of Service (DDoS) attacks for criminal, political, or other motivations."[34] Efforts must include rigorous law enforcement on a global scale.
- **Botnets exploit the Internet's design, where intelligence is in devices rather than in the network**.[35] They take advantage of the Internet's core properties, such as its global reach, accessibility, and ability to support a seemingly inexhaustible range of uses. This is why we must include endpoint security and device design in botnet strategy.

[28] *Id.*

[29] Internet Society, *Botnets: An Internet Society Public Policy Briefing* (Oct. 30, 2015) ("ISOC Policy Brief"), https://www.internetsociety.org/sites/default/files/ISOC-PolicyBrief-Botnets-20151030-nb.pdf.

[30] European Network and Information Security Agency, *Botnets: Detection, Measurement, Disinfection, & Defence*, at 4 (Mar. 7, 2011), https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence.

[31] Ben Herzberg, Dima Bekerman & Igal Zeifman, *Breaking Down Mirai: An IoT DDoS Botnet Analysis*, Imperva Incapsula (Oct. 26, 2016), https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html.

[32] *Id.*

[33] *Id.*

[34] CSRIC III, Final Report, WG 4 at 8.

[35] *See* ISOC Policy Brief at 2-3.

Hackers have been using botnets maliciously since as early as 2000 by gaining access to unsecured personal computers. Viruses, worms, and email spam plagued early Internet users. Most personal computers were not secured and companies racing to join the dot-com wave did not always address security. However, industry and operators responded. Through the Messaging, Malware and Mobile Anti-Abuse Working Group ("M3AAWG"), industry worked against botnets, malware, spam, viruses, DoS attacks, and other online exploitation.[36] CSRIC developed its *Anti-Botnet Code of Conduct*. Others addressed phishing, pharming, email spoofing, and spyware.[37] These efforts improved security and the Internet experience for users.

The rise of IoT malware is reminiscent of the Internet's early days, but what is different now is the number of connected objects and how users interact with those objects. The IoT promises 20 billion connected objects by 2020, each with its own IP address.[38] While end users may eventually notice and remediate a computer infection, some IoT devices are meant to function with minimal user interaction and "do not have a user interface (UI); are designed to run autonomously; and are connected either directly or indirectly to the Internet."[39] Unless educated, an end user may have no reason to think their IoT device is part of a botnet.

[36] M3AAWG, *Because Effective Anti-Abuse Collaboration Requires a Trusted Global Form*, https://www.m3aawg.org/about-m3aawg. The organization initially started as MAAWG, the Messaging Anti-Abuse Working Group. The organization changed its name to M3AAWG in 2012 to better reflect its scope of work.

[37] For example, the Anti-Phishing Working Group focused on eliminating the fraud and identity theft from phishing; the Anti-Spyware Coalition was dedicated to building a consensus on definitions and best practices around spyware and other unwanted technologies; and the International Botnet Taskforce brought together public and private sector computer security specialists to share best practices, tools, and training to combat botnets.

[38] Liam Tung, *IoT devices will outnumber the world's population this year for the first time*, ZDNet (Feb. 7, 2017), http://www.zdnet.com/article/iot-devices-will-outnumber-the-worlds-population-this-year-for-the-first-time.

[39] CSCC White Paper at 8.

IV. "ATTACK MITIGATION" AND "ENDPOINT PREVENTION" ARE COMPLEMENTARY CONCEPTS THAT WILL IMPROVE AS ENDPOINT PROTECTION MATURES.

NTIA identifies where it thinks progress can be made: attack mitigation and endpoint prevention. Attack mitigation involves "minimizing the impact of botnet behavior by rapidly identifying and disrupting malicious behaviors."[40] Endpoint prevention is "securing endpoints, especially IoT devices, and reducing vulnerabilities" through actions focused on the device.[41] Industry is effective at attack mitigation, but cannot address automated, distributed attacks alone by providing "clean pipes." Endpoint protection must improve.

With respect to attack mitigation, industry focuses on response and resiliency. Network operators filter known botnet traffic and protect network infrastructure. Techniques include spoofing the source IP address in attack packets as well as using Access Control Lists, traffic policing, black holing, and sink holing. Network operators have invested in systems to "scrub" out DDoS attacks. Scrubbing diverts a botnet victim's traffic through a scrubber to filter out malicious traffic before placing it on the operator's network.[42] Network operators also provide tools for customers: endpoint anti-virus software and home gateways with integrated security. Some operators offer managed security services including firewalls, mobile device management, threat analysis and event detection, secure VPN connectivity, and DDoS scrubbing. Resiliency is another part of mitigation, and is standard practice at the Internet infrastructure and service provider level, which faces more than 120,000 DDoS attacks every week. For operators,

[40] Request at 27043.

[41] *Id.*

[42] Although effective, network operators do not have the capacity to scrub all of their traffic all of the time, and should not be expected to do so.

identifying botnet traffic is not the primary challenge. Rather, operators must mitigate the impact of malicious traffic and, if necessary, remediate the endpoint.

Although network operators are continuously improving, they cannot be expected to solve the problem by providing “clean pipes.” *First*, the notion that individual operators can or should prevent the delivery of all malicious traffic is unreasonable. Internet traffic is originated and routed around the world by numerous providers of varying trustworthiness. Often, botnets and their command and control servers are outside an operator’s control or visibility. *Second*, endeavoring to satisfy a “clean pipes” mandate would require large scale monitoring and content review, which operators are not in a position to implement (both due to resources and the increase in encrypted traffic), and which consumers likely do not want. Worse, it may not be effective. Botnets generating a small amount of traffic may not trigger network monitoring thresholds. Conversely, botnets generating large amounts of traffic may overwhelm resources. There also is a potential for false positives because malicious traffic often looks normal, so action could harm end users. *Third*, even where accurate detection is possible, mitigation will vary from network to network due to differences in service level agreements with customers.

Fundamentally, a meaningful response requires better endpoint prevention. IoT devices are attractive targets because end users often cannot tell when a device has been compromised or remediate because of lack of access to device hardware or software. Once a device is infected, network solutions can only do so much. The market must encourage secure devices, thoughtful product development, and education. As the Federal Trade Commission (“FTC”) notes, there is no single solution because "what constitutes reasonable security for a given device will depend on a number of factors."[43] But this does not mean we cannot improve device security.

The challenge in endpoint security is that development methods have tradeoffs. On one hand, less secure devices can be offered at a lower price. On the other hand, manufacturers that do not do enough at the outset may face costly efforts to remedy deficiencies or respond to enforcement activities. Competing design goals also can complicate security: open and accessible platforms promote interoperability and economies of scale, but are harder to secure. Endpoint protection requires investment from manufacturers. In the meantime, network operators are doing their part by enabling over-the-air updates for patches and working on OS update processes. These efforts will be most effective if those selling IoT devices and services build in security, guided by standards and best practices.

V. NTIA'S QUESTIONS REVEAL CREATIVE STEPS THAT CAN HELP MITIGATE RISKS OF BOTNETS AND DDOS ATTACKS.

NTIA seeks input on approaches to automated, distributed threats, as well as the role of government, international issues and end users. The breadth of questions reflects the scope of the challenge, as well as the opportunity for creative approaches.

A. What Works: Public-Private Partnerships Should Be Protected and Expanded.

NTIA asks what works for dealing with automated and distributed threats. There is widespread agreement that public-private partnerships are effective. And, ultimately, innovation will be the most effective solution to evolving threats, so government should support any activities that promote innovation.

[43] FTC, *Internet of Things: Privacy & Security in a Connected World*, Staff Report (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

The government has task forces and inter-agency groups to facilitate collaboration with the private sector. NIST's voluntary *Cybersecurity Framework* has been a key contribution and is the paradigmatic example of effective public-private collaboration. The *Cybersecurity Framework* provides a guide to risk management, and identifies leading practices that have been successful. As the *Framework* is updated, it is important that NTIA and NIST prioritize voluntary, collaborative efforts, like the NCCIC, NSTAC, CSRIC, and others. Examples include DHS's US-CERT. This operational arm of the NCCIC facilitates information sharing.[44] The Department of Defense's Cyber Crime Center focuses on training and research impacting government agencies and private companies in the defense sector.[45] Likewise, ISACs have made advances in information sharing. NTIA should focus on strengthening these voluntary relationships.

Ultimately, though, innovation is the best "existing approach" to help mitigate attacks. The most effective tool will continue to be private sector innovation. As discussed, 5G holds great promise for increased security and will help with attack mitigation and endpoint prevention. To protect this work, the government should preserve industry's flexibility to innovate and respond to threats.

B. Gaps: Collaboration May Be Stymied by Fear of Liability and Regulatory Uncertainties.

The *Request* asks about gaps in current approaches and obstacles to collaboration across the ecosystem. In CTIA members' experience, collaboration *within* the communications sector works well. Among other things, the sector has made significant effort in the FCC's CSRIC to

[44] *See* U.S. Computer Emergency Readiness Team, *About Us*, https://www.us-cert.gov/about-us.

[45] Department of Defense, Cyber Crime Center, *Fact Sheet: DoD Cyber Crime Center (DC3)*, http://www.dc3.mil/data/uploads/DC3-Fact-Sheet.pdf.

apply the NIST *Cybersecurity Framework* and develop best practices. Nonetheless, we see three obstacles to collaboration: fear of liability from information-sharing and collaboration *outside* the communications sector; concern about the legal ability of network operators to take action in response to a DDoS attack on other entities; and uncoordinated action at the federal and state level. In each area, the gap arises from uncertainty about liability or regulatory overhang. To further foster a spirit of openness about vulnerabilities and collaboration, NTIA should consider ways to remove uncertainty.

First, companies have legitimate fear of liability from information-sharing about vulnerabilities. Recent history confirms risk in discussing device, operating system, and software vulnerabilities. A troubling example occurred when a broker and security researcher apparently teamed up to short the stock of a medical device manufacturer and publicly release a vulnerability in a medical device.[46] Likewise, risk of lawsuits complicate disclosures, as illustrated by pending litigation over claimed product vulnerabilities—even absent a breach or demonstrable harm.[47] While potentially useful, vulnerability disclosure programs or "bug bounties" are not a panacea, and some models focus more on protecting hackers than on risks companies face.[48] Companies may benefit from working with researchers, but do not want to be exploited by demands for payment, public recognition, or unreasonably rapid resolution.

[46] *See* Jordan Robertson and Michael Riley, *Carson Block's Attack on St. Jude Reveals a New Front in Hacking for Profit*, Bloomberg (Aug. 25, 2016), https://www.bloomberg.com/news/articles/2016-08-25/in-an-unorthodox-move-hacking-firm-teams-up-with-short-sellers; Linette Lopez, *Carson Block has a new short, and his reasoning is super creepy*, Business Insider (Aug. 25, 2016), http://www.businessinsider.com/muddy-waters-shorts-st-jude-2016-8.

[47] *See* Andy Greenburg, *Chrysler and Harman Hit With Class Action After Jeep Hack*, Wired.com (Aug. 4, 2015), https://www.wired.com/2015/08/chrysler-harman-hit-class-action-complaint-jeep-hack/.

[48] *See, e.g.*, Megan Brown and Matthew Gardner, *Considering a Vulnerability Disclosure*

Second, with respect to attack response, legal uncertainties about taking defensive action persist, despite the helpful passage of CISA. While "hacking back" is problematic and often unwise (due to unintended consequences and collateral damage), any uncertainty about defensive steps operators can take may have a chilling effect on rapid action to address attacks. For example, members' experience with the 2016 Mirai attack suggests challenges remain when it comes to mitigation, particularly where the victim is not the carrier or ISP network. The Mirai botnet targeted the network edge, attacking a DNS service company.[49] Although network operators could see malicious traffic and offered assistance, they could not act without permission from affected entities.

Finally, uncoordinated government efforts create an uncertain regulatory environment and a patchwork of burdensome expectations that can interfere with collaboration and innovation. For example, a recent FCC rule requiring millimeter wave licensees to publicly disclose network security plans[50] threatens to saddle carriers with burdens but offer little obvious improvement in security because companies already work with their sector-specific agency,

Program? Recent Push Raises Questions for General Counsel, CircleID (Feb. 10, 2017), http://www.circleid.com/posts/20170210_considering_a_vulnerability_disclosure_program/

[49] *See, generally* Tim Greene, *How the Dyn DDos attack unfolded*, NetworkWorld (Oct. 21, 2016, 4:52 PM), http://www.networkworld.com/article/3134057/security/how-the-dyn-ddos-attack-unfolded.html ("ThousandEyes observed peering relationships between Dyn and internet providers breaking during the day, either because the connections failed or one or both parties decided it was in their best interests to do so."); Redfive Security and Fortalice, *Black 5 Client Advisory: Dyn/DDoS Attack* (Oct. 26, 2016), http://www.red5security.com/news_media_34_3921121624.pdf (urging that companies "[a]dd DDoS protection to an existing SLA with your ISP."). Chester Wisniewski, *Mirai, Mirai, on the wall—through the looking glass of the attack on Dyn*, Naked Security by Sophos (Oct. 24, 2016), https://nakedsecurity.sophos.com/2016/10/24/mirai-mirai-on-the-wall-through-the-looking-glass-of-the-attack-on-dyn/.

[50] 47 C.F.R. § 30.8.

DHS, on security.[51] The challenge of overlapping effort arises from state action as well, which can be duplicative and burdensome. States have considered operational security regulations and others focus on data security,[52] but divergent activity may undermine a national Internet ecosystem.

C. Addressing the Problem: NTIA Should Clarify Legal Uncertainties To Foster More Activity, and Promote International Law Enforcement.

The *Request* asks about laws, policies, standards, technologies, and investments that will reduce the risks and harms of botnets. Botnet mitigation raises complex legal issues, made more difficult by obstacles identified above. Fortunately, the government can help.

First, the government can provide clear rules of the road so that companies can confidently take action and share information without concern about legal liability. The FCC's attempted privacy rules illustrate some of the complexity associated with privacy and other regulation. Were they not invalidated by Congress, the rules would have treated as customer proprietary network information ("CPNI") or personally identifiable information IP addresses, MAC addresses, device identifiers, and port information, among other things. This could have

[51] Several entities sought reconsideration of the rule for various reasons. *See* Petition for Reconsideration of CTIA, *Use of Spectrum Bands Above 24 GHz For Mobile Radio Services,* GN Docket No. 14-177 (Dec. 14, 2016), https://www.ctia.org/docs/default-source/fcc-filings/161214---ctia-spectrum-frontiers-petition-for-reconsideration.pdf?sfvrsn=2.

[52] For example Connecticut has pursued cyber regulation for public utilities (State of Connecticut, Public Utilities Regulatory Authority, *Cybersecurity and Connecticut's Public Utilities* (Apr. 12, 2014), http://www.ct.gov/pura/lib/pura/electric/cyber_report_041414.pdf), and New York adopted regulation for financial services companies (New York State, Department of Financial Services, *Cybersecurity Requirements for Financial Services Companies* (Mar. 1, 2017), https://www.governor.ny.gov/sites/governor.ny.gov/files/atoms/files/Cybersecurity_Requirements_Financial_Services_23NYCRR500.pdf). The National Conference of State Legislatures lists dozens of cyber and privacy related laws considered in 2016. NCSL, *Cybersecurity Legislation 2016* (Dec. 8, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2016.aspx.

had a chilling effect on efforts to exchange data for security purposes.[53] For example, DNS query data is valuable for detecting Internet abuse, including botnets and malware, but it has been suggested that a carrier's flexibility to use query data in this manner could run afoul of CPNI regulations. The FCC tried to clarify that its rules would not stand in the way of cybersecurity efforts, but its solution, focusing on reasonableness and reminding carriers to be careful of enforceable obligations, was vague and did not provide carriers with a high degree of comfort.[54] This would have preserved uncertainty. Likewise, the FCC has taken steps to make clear on robocalling abatement efforts that action to prevent fraud is not unlawful.[55] These clarifications confirm that legal uncertainties accompany information-sharing. The government should remove such uncertainties by clarifying legal obligations and creating safe harbors.

Second, NTIA should consider clear authorizations and immunity for action to mitigate attacks. Legal uncertainty can slow action as companies consider whether activity is consistent with various legal obligations. Options include clarifications of the Consumer Fraud and Abuse Act and federal restrictions on sharing CPNI.

[53] It is important to note that while the FCC rules were invalidated, several states have introduced similar legislation which could likewise pose cybersecurity risks. For example California Broadband Internet Privacy Act, A.B. 375 (Ca. 2017) (introduced Feb. 9, 2017) (pending), *available at* https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.

[54] *See Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Report and Order, FCC 16-148, WC Docket No. 16-106, ¶¶ 213-14 (Nov. 2, 2016) ("caution[ing] that carriers using or sharing customer PI pursuant to this section of the rules should remain vigilant about limiting such use and sharing to the purposes of protecting their networks and users, and complying with their data security requirements." And "carriers should not disclose more information than is reasonable to achieve this purpose, and should take reasonable steps to ensure that the parties with which they share information use this information only for the purposes for which it was disclosed.").

[55] *See Advanced Methods to Target and Eliminate Unlawful Robocalls*, Notice of Proposed Rulemaking and Notice of Inquiry, 32 FCC Rcd 230682 (Mar. 23, 2017) (proposing rules to facilitate voice service providers in blocking illegal robocalls).

Finally, the United States must not overlook those who cause harm by focusing too much on the very operators and manufacturers whose products and services are victimized by attacks. DDoS and other automated attacks do not "just happen." They are perpetrated by bad actors around the world. Global enforcement and legal consequences are vital, even if they cannot root out the problem entirely. NTIA should encourage the President to ensure that DOJ and the Department of State continue and expand on recent botnet take-downs.

D. Governance and Collaboration: NTIA Should Foster Wider Participation in U.S. Digital Strategy and Champion U.S. Leadership in International Standards.

NTIA asks about stakeholder roles in developing policies and standards. Mitigating botnets is a responsibility shared by government, network operators, manufacturers, software vendors, online service providers, the technical community, and end users. Endpoint protection will be critical, so it is important to bring manufacturers to the table. NTIA also can help ensure that agencies like NIST are responsive to industry needs. And NTIA should emphasize international leadership to preserve open markets and transparent standards processes.

First, NTIA should focus on expanding stakeholder engagement to include more of the entities who are central to endpoint protection: manufacturers and others in the device supply chain. Work is underway in several important non-regulatory settings, such as at DHS in the NCC, NCCIC, and Comm-ISAC, and the FCC's CSRIC, focused on the communications sector. NTIA should consider how to engage additional manufacturers and providers whose products are linked to Internet security.

Second, the government can better leverage NIST activities on standards and best practices for Internet and mobile security. Following the successful *Cybersecurity Framework*, NIST and its National Cybersecurity Center of Excellence ("NCCoE") have taken on increasing activities affecting the private sector. This expansion of their mission should be closely coordinated with industry, as NIST work helps inform U.S. and global policy and standards. Some global standards work, as noted below, could benefit from more U.S. leadership. Thus, the government may want to include the private sector more in setting NIST and NCCoE priorities, to ensure that work on botnets or other distributed attacks[56] reflects the needs of U.S. industry and its expertise. This will ensure that NIST's work can best contribute to international discussions about responses to botnets and other automated, distributed attacks.

Third, as explained below, the United States should be active in global work on botnets, because the challenge cannot be met in the United States alone. Some of the greatest challenges to addressing DDoS attacks come from different domestic and foreign policy approaches, which require international cooperation. Likewise, cyberthreats are not U.S.-specific, and some solutions depend on ubiquitous deployment by the global ecosystem. For example, DNSSEC and BGP approaches can depend upon actions outside of operator control to be effective. Ubiquitous deployment of many security solutions can only be achieved through global consensus, not domestic regulation or post-hoc accountability efforts. As explained below, the United States should take a leading role in the various international standards and other bodies.

E. Role of Government: The Government Should Improve Its Own Cyber Hygiene and Only Act Where Necessary To Fill a Gap in Market Activity.

NTIA asks about roles for the federal government. Government can support strategic solutions that combine the resources of government and industry. It should (1) take efforts to

[56] NIST has looked at botnets in the past. *See, e.g.*, NIST, *Technical Aspects of Botnets Workshop* (May 2012), https://www.nist.gov/news-events/events/2012/05/technical-aspects-botnets-workshop; NIST, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*, Special Publication 800-83 Revision 1 (July 2013), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf.

ensure proper cyber hygiene is being practiced throughout the federal government, (2) avoid regulation and remain a convener of stakeholders; and (3) focus action where private sector abilities are limited, such as on workforce, law enforcement, and resolving regulatory uncertainty.

NTIA should advise the President that it is critical for government agencies to focus on cybersecurity as they modernize federal systems. Federal data breaches still are commonplace and federal mobile management requires immediate attention. There are things the federal government can do *right now* to improve, particularly given uncoordinated security practices and reported lax behavior by end users.[57] Unfortunately, government action is sometimes poorly prioritized. For example, some agencies are looking at using "bug bounty" programs, which invite hackers to seek out vulnerabilities, before agencies have a solid grip on basic cyber hygiene or use of enterprise mobile management.

With respect to the private sector, government should remain a convener and avoid regulation. NIST's *Cybersecurity Framework* effort is well-known, but NTIA likewise plays an important role because it, too, is non-regulatory.[58] Other agencies are good conveners, including DHS. These efforts should be protected and strengthened. Most fundamentally, the government, should focus on that which the market cannot do effectively on its own:

- The government should promote workforce development, which is critical to our digital future. Cisco puts the number of unfilled cybersecurity jobs globally at 1

[57] *See* Lookout, *State of Federal BYOD Report* at 3 (Aug. 2015) (nearly 40% of government employees ignore policies prohibiting mobile device use, putting sensitive data at risk, and 7% of government users report bringing jailbroken phones to work).

[58] For example, NTIA convened a multistakeholder process on security upgradability for the IoT (NTIA, Public Notice of open meeting (Sept. 19, 2016), https://www.ntia.doc.gov/files/ntia/publications/2016-22459.pdf) among others on technology policy.

million.[59] CSRIC V addressed cyber workforce.[60] NIST's effort on workforce under the President's Executive Order[61] will be important, as the government can shape national policy with grants, tax incentives, and skilled immigration, as well as higher education policy.

- The government should prosecute cybercrime aggressively, working with international partners to build and drive international norms. The government is uniquely positioned to investigate cybercriminals, collect foreign intelligence on cyberthreats, and protect companies that share information with the government.

- The government should harmonize federal activity in a non-regulatory posture. Agencies have varied interests in cybersecurity, and uncoordinated state and federal efforts create uncertainty. NTIA should lead efforts to simplify processes, avoid duplication, and curtail multiple frameworks.

As NTIA advises the President on the role of government, it should note that private innovation has been key to meeting social and technology challenges. Government should continue to play a supportive role.

F. International: The Global Nature of the Internet and Digital Supply Chain Make Global Coordination and U.S. Leadership Imperative.

NTIA asks how the global nature of the Internet should affect its approach. Cyber threats do not recognize borders. There are vast differences in law and policy across countries, and the global digital supply chain means no amount of security in U.S. devices and networks can fully address the threat. The global botnet risk is best countered by international cooperation and U.S. leadership in the development of consensus, open standards for Internet and mobile security.

[59] Cisco, *Mitigating the Cybersecurity Skills Shortage: Top Insights and Action from Cisco Security Advisory Services*, at 2 (2015), http://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-talent.pdf.

[60] CSRIC V, *Cybersecurity Workforce Development Best Practices Recommendations*, Final Report, WG 7 (Mar. 2017), https://www.fcc.gov/files/csric5-wg7-finalreport031517pdf.

[61] *See* Press Release, NIST Seeks Comments on Growing, Sustaining the Nation's Cybersecurity Workforce (July 10, 2017), https://www.nist.gov/news-events/news/2017/07/nist-seeks-comments-growing-sustaining-nations-cybersecurity-workforce.

NIST should continue to conduct outreach internationally for its *Cybersecurity Framework*, which is scalable across borders. Widespread adoption will create a common language and facilitate collaboration.

NTIA should reinvigorate U.S. global leadership by intensifying efforts to promote international norms consistent with U.S. approaches. One of the most important roles for the U.S. government is to lead on the global stage, through international networks of law enforcement, diplomatic engagement, and active participation in standards work across the world. This includes harmonizing laws to facilitate cooperation, promoting stiff penalties for trafficking in malware and botnets, discouraging regulation that may limit interoperability and competition, and championing standards development in voluntary, open, and consensus-based bodies.[62] On this last point, CTIA wishes to make a specific request of NTIA and the Administration: at a time of global competition for leadership of the world's Internet and mobile future, the United States must be a strong voice at the table. Other countries and their companies are actively participating, sending large delegations of company and government representatives whose presence shapes outcomes.[63] Some are adopting prescriptive cybersecurity regimes that aim to help their national and regional economies. The U.S. private sector cannot shoulder alone the burden of advocating U.S. interests in governing bodies for communications network standards, Internet governance, and the like. The President should make a strong commitment to

[62] U.S. standards divorced from the global effort will not drive meaningful change. NTIA should ensure that the United States is engaged internationally so that the United States does not become isolated from global standards development and product development.

[63] *See, e.g.*, L. Lucas, *Huawei aims to help set 5G standards*, Financial Times (Nov. 29, 2016) https://www.ft.com/content/f84f968c-b45c-11e6-961e-a1acd97f622d (describing Huawei success in shaping 5G standards, and work by "European governments" who also have "jumped on the 5G bandwagon").

international engagement on technical standards and international cybersecurity practices, and coordinate the work of the Departments of State and Commerce to that end.

G. Users: NTIA Should Think Big in Educating Consumers and Enterprise Users About Their Role in Our Digital Future.

Finally, NTIA asks how to empower users and decision makers. We are on the cusp of a sea change of connectivity; end users will need to be responsible digital citizens. Many attacks still use social engineering and other "low-tech" methods, meaning that user behavior can have direct effects on system security. This is particularly true in enterprises, like the government, where compromise of a single user can have grievous consequences for the organization.[64] As in other public campaigns—to prevent forest fires, reduce smoking, or increase seatbelt use—government and industry can help prepare citizens for a world in which their choices affect others.

This can work. The private sector invests resources to educate consumers and it pays off. A recent CTIA-commissioned Harris Poll demonstrates that consumers are adopting advanced security following industry work to raise awareness. Sixty-nine percent of wireless consumers were using PINs/passwords on their smartphones in 2016, up thirteen percent from 2015 and up thirty-eight percent from the first survey in 2012.[65] Seventy-seven percent of wireless consumers report that they run software updates every or almost every time they are offered.[66]

[64] As noted above, one study showed that nearly 40% of government employees ignore mobile device policies and 7% of government users report bringing jailbroken phones to work. *See* Lookout, *State of Federal BYOD Report* at 3.

[65] *See Smartphone users are becoming more aware of security features*, Business Insider (Aug.3, 2016, 8:30 PM), http://static3.businessinsider.com/smartphone-users-are-becoming-more-aware-of-security-features-2016-8.

[66] *See* CTIA, *Protecting America's Wireless Networks* (Apr. 2017), https://www.ctia.org/docs/default-source/default-document-library/protecting-americas-wireless-networks.pdf.

The government should consider an aggressive, national effort to raise awareness. Federal and state agencies offer cyber tips, including the FBI[67], FTC,[68] FCC,[69] and DHS.[70] While some are common sense, other pointers are sophisticated, like FBI advice that connected toy purchasers should "[r]esearch where user data is stored – with the company, third party services, or both – and whether any publicly available reporting exists on their reputation and posture for cyber security."[71] Advice like this can get lost in a cacophony of messages, and it is unclear how consumers are to receive and act on it. Government should resist the urge to mandate uniform disclosures which may foster a false sense of security or fail to keep pace.

[67] Press Release I-071717-PSA, FBI, *Consumer Notice: Internet-Connected Toys Could Present Privacy and Contact Concerns for Children* (July 17, 2017), https://www.ic3.gov/media/2017/170717.aspx; Staff, *FBI Issues Warning on IoT Toy Security*, DarkReading (July 17, 2017), http://www.darkreading.com/cloud/fbi-issues-warning-on-iot-toy-security/d/d-id/1329373.

[68] The FTC offers consumer tips as well as industry guidance: FTC, *Careful Connections: Building Security in the Internet of Things* (Jan. 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf; FTC, Consumer Information, *Using IP Cameras Safely* (Aug. 2013), https://www.consumer.ftc.gov/articles/0382-using-ip-cameras-safely; FTC, Consumer Information, *Understanding Mobile Apps* (Feb. 2017), https://www.consumer.ftc.gov/articles/0018-understanding-mobile-apps; FTC, Consumer Information, *Securing Your Wireless Network* (Sept. 2015), https://www.consumer.ftc.gov/articles/0013-securing-your-wireless-network; Whitney Merrill, *Advanced password tips and tricks*, FTC, Consumer Information Blog (July 30, 2015), https://www.consumer.ftc.gov/blog/advanced-password-tips-and-tricks (password guidance).

[69] FCC, *Wireless Connections and Bluetooth Security Tips* (Oct. 25, 2016), https://www.fcc.gov/consumers/guides/how-protect-yourself-online (wireless and bluetooth security tips); FCC, Cybersecurity Tips for International Travelers (Nov. 2, 2016), https://www.fcc.gov/consumers/guides/cybersecurity-tips-international-travelers (cyber tips for international travelers).

[70] DHS, US-CERT, *Tips*, https://www.us-cert.gov/ncas/tips (Tips describe and offer advice about common security issues for non-technical computer users, on issues like rootkits, botnets, DOS attacks and many other topics); DHS, US-CERT, *Security Tip (ST04-002) Choosing and Protecting Passwords* (Oct. 1, 2016), https://www.us-cert.gov/ncas/tips/ST04-002 (password tips).

[71] Press Release I-071717-PSA, FBI.

Instead, NTIA should work with companies, associations, non-profits, states, and the FTC, to raise awareness of consumers' role in securing devices, patching, and managing end of life device transitions.

VI. CONCLUSION.

CTIA encourages NTIA to advise the President that extensive work on botnets and automated, distributed attacks is underway. As the world approaches a connected, digital future, the United States must think about how to promote innovation. It may require creativity to remove obstacles to information sharing and vulnerability management. Government should not turn reflexively to regulation. Instead, it should prosecute cybercrime, facilitate collaboration, and remove some of the obstacles to private action, such as from litigation and regulatory overhang. It can lead a national discussion about digital citizenship and security. And it should champion the free market and promote innovation on the global stage.

Respectfully Submitted,

/s/ Thomas C. Power
Thomas C. Power
Senior Vice President and General Counsel

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

John M. Marinho
Vice President, Technology and Cybersecurity

Melanie K. Tiano
Director, Cybersecurity and Privacy

CTIA
1400 Sixteenth Street, NW, Suite 600
Washington, DC 20036
(202) 785-0081
www.ctia.org

July 28, 2017