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 USTELECOM ASSOCIATION

Jonathan Banks
Robert Mayer
601 New Jersey Avenue, NW
Suite 600
Washington, DC 20001
(202) 326-7300

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 Botnets and Other Automated Threats	)	Docket No. 170602536-7536-01
	)	

COMMENTS OF THE USTELECOM ASSOCIATION

The USTelecom Association is pleased to respond to the National Telecommunications and Information Administration's ("NTIA") Request for Comment ("RFC") on actions that stakeholders in the internet and communications ecosystem can take to address automated and distributed threats such as botnets.[1]

I. INTRODUCTION

A. USTELECOM STRONGLY SUPPORTS THE INDUSTRY-DRIVEN PROCESS THAT THE ADMINISTRATION HAS PROMOTED UNDER THIS INITIATIVE

USTelecom believes strongly that as a matter of first principle, industry-driven processes should be at the heart of cybersecurity policymaking. We therefore applaud the Administration for undertaking such a process aimed at reducing malicious botnets and other distributed and automated cyber threats as the centerpiece of Executive Order 13800, titled "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." This ongoing initiative is robust, ambitious, and multifaceted; yet, at the same time, it is also clear, coherent, and easily navigable by industry players who do not have unlimited personnel or resources to apply to policy processes. This is a policymaking model that we strongly support and seek to promote.

[1] 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").

First, we note that as with this RFC itself, the workshop on Enhancing Resilience of the Internet and Communications Ecosystem hosted at the National Institute of Standards and Technology's ("NIST") National Cybersecurity Center of Excellence ("NCCoE") on July 11-12 was a strikingly industry- and digital economy-oriented set of discussions and participants, characteristic of the Department of Commerce's ("Commerce") approach. As we discuss in greater detail in our answers to the questions below, this approach has been successful, for instance, in the process that NIST has instituted for industry to develop the Cybersecurity Framework and the ongoing IoT patching and updating multistakeholder process that NTIA is convening. Also, addressing the inherently international nature of this challenge – again, another Commerce trademark – was a prominent part of the discussions at the NIST workshop. It is not lost on USTelecom and its members that Commerce is the only Cabinet agency in the U.S. government whose primary core mission is promoting American business growth and innovation worldwide, and thus the Department is the natural part of government to convene broad industry-wide processes like these.

Similarly, we note the promise of the Department of Homeland Security's ("DHS") primary focus in its co-leadership of this initiative with Commerce on another industry-led effort: its task to the National Security Telecommunications Advisory Committee ("NSTAC") to provide an expedited report on the technical and operational recommendations to reduce malicious botnets. One of our leading members, AT&T, is the co-chair of that important initiative, which dovetails with and complements the Commerce-led workstreams. Our members' unique and productive relationship with DHS through NSTAC, the Communications Sector Coordinating Council ("CSCC"), and the National Coordinating Center/Communications

Information Sharing and Analysis Center ("NCC/Comm ISAC") is indicative of the role that DHS can play in promoting an industry-led approach to critical infrastructure cybersecurity.

In this process, the complementary and mutually reinforcing roles that Commerce and DHS play in interfacing with industry are clear and well-coordinated. This framework of industry leadership facilitated through government's convening capabilities provides a strong foundation for powerful industry-government collaboration not only with Commerce and DHS, but with other elements of government – including the Department of Justice ("DoJ") and the Federal Bureau of Investigation ("FBI"), as well as the two regulatory authorities that are being consulted on this particular initiative, the Federal Trade Commission ("FTC") and the Federal Communications Commission ("FCC").

In short, industry is active, at the table, and eager to show that processes like this bring real progress. We have high expectations that this particular initiative will develop into similar longer-term and ongoing industry-led processes rather than trending back toward traditional top-down prescriptive government requirements and regulations that inherently prevent a true partnership between industry and government. To that end, USTelecom is bringing this spirit and strong momentum of industry leadership to its response to this RFC to promote concrete examples of real-world solutions as well as potential collective improvements that involve mutual collaboration across segments of the ecosystem.

B. USTELECOM STRONGLY SUPPORTS FOUR CORE GUIDING PRINCIPLES FOR CYBERSECURITY POLICYMAKING TO ENHANCE RESILIENCE OF THE INTERNET AND COMMUNICATIONS ECOSYSTEM

Many stakeholders and sectors of industry share – and promote – the following guiding principles for cybersecurity policy in general as particularly applicable to ecosystem-wide challenges such as those pertaining to reducing malicious botnets and other automated and distributed threats:

1. We must embrace private sector leadership and market-driven innovation, and actively seek to harness these dynamics as the primary engines of effective cybersecurity solutions that can be deployed globally.
2. Dynamic, flexible approaches to cybersecurity – rather than checklist compliance regulation – are a fundamental imperative to remain more nimble than the threat.
3. Cybersecurity is a shared responsibility of all players in the internet and communications ecosystem, and all stakeholders – including government, and enterprises, and consumers – must make improvements to address threats to the ecosystem. Therefore, government must move away from simplistic approaches that call on action from only one or two parts of the ecosystem.
4. Truly mutually beneficial teamwork between governments, companies, and consumers requires active partnership against bad actors, not top-down government requirements or punishment on the one hand or meaningless bromides about "public private partnership" on the other.

USTelecom strongly supports these principles as applicable to all aspects of cybersecurity policymaking, particularly in addressing ecosystem-wide challenges; therefore, they inform our responses below.

II. INTERNET SERVICE PROVIDERS' LEADERSHIP AND ACTION

A. BACKGROUND

The challenge of malicious botnets and other distributed and automated cyber threats can only effectively be addressed by the entire ecosystem, and USTelecom and its members readily accept the responsibility that internet service providers ("ISPs") have as an important part of the multilayered and distributed solutions to this multilayered and distributed challenge. ISPs' efforts in this area have been fundamental to our central role in the internet and communications

ecosystem for decades. As the government has increased its policy focus on cybersecurity in recent years, these efforts have grown to include formal policy initiatives such as the Industry Botnet Working Group ("IBG") that the White House convened in 2012.[2] The IBG developed nine principles that remain relevant today:

1. Share Cybersecurity Responsibilities
2. Coordinate Across Sectors
3. Confront the Problem Globally
4. Report Lessons Learned
5. Educate Users
6. Preserve Flexibility
7. Promote Innovation
8. Respect Privacy
9. Navigate the Legal Environment

The IBG was active for a period of time, but after establishing the nine principles, many key players in the ecosystem gradually stopped participating and the ISPs were left to implement the principles. This experience shows that the government's – in that case, the White House's – convening role is critical for keeping all players in the ecosystem at the table.

Still, leading ISPs advanced this initiative in a working group under the Communications Reliability, Security and Interoperability Council ("CSRIC"), an FCC-convened private sector advisory committee. Through this CSRIC effort, ISPs developed the Anti-Bot Code of Conduct ("ABC") for Internet Services Providers, which was subsequently promoted in a public

[2] *See* White House Announces Public-Private Partnership Initiatives to Combat Botnets, at http://2010-2014.commerce.gov/news/press-releases/2012/05/30/white-house-announces-public-private-partnership-initiatives-combat-b.html.

commitment by the country's largest ISPs, including USTelecom members.[3] In 2014, the FCC followed up with a Public Notice seeking a progress check on these and related issues. The FCC explicitly sought input from stakeholders throughout the internet and communications ecosystem,[4] but only ISPs responded to the FCC's call for information and engagement. Our members' in-depth technical presentations to FCC staff on these matters illuminated that ISPs' robust efforts at botnet reduction, while fundamental to our basic business operations and centrally important in the ecosystem, are not alone sufficient to address the challenge without activity and progress on these matters throughout the ecosystem.

B. ISPs' Activities and Operations

As detailed in the Industry Technical White Paper issued by the CSCC on July 17, 2017,[5] ISPs have worked to identify known botnet command and control sites, to filter or sinkhole traffic between infected computers and botnet hosts, and to identify end user computers communicating with known botnet hosts. Our members are able to block ports where appropriate and also notify consumers and provide remediation tools. For enterprise business customers, our members offer sophisticated managed security services and have built robust threat analytics to identify and stop threats before they reach the end user. We also work closely with law enforcement to shut down malicious botnet hosts.

---

[3] *See* CSRIC III Working Group 7 Final Report, U.S. Anti-Bot Code of Conduct (ABCs) for Internet Service Providers (ISPs), March 2012, at https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-ReportFinal.pdf, and Final Report, Barrier and Metric Considerations, March 2013, at https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG7_Report_March_%202013.pdf.

[4] *See* FCC Public Safety and Homeland Security Bureau Requests Comment on Implementation of CSRIC III Cybersecurity Best Practices, July 25, 2014, at https://apps.fcc.gov/edocs_public/attachmatch/DA-14-1066A1.pdf ("[the FCC] seeks comment from ISPs, the Internet community, consumer organizations, and the broader public on the implementation and effectiveness of the CSRIC III recommendations and/or alternatives that stakeholders have developed since the time of the CSRIC's original work to address these challenges. The purpose of this Public Notice is to promote a robust, stakeholder-driven discourse drawing on broad perspectives from throughout the cyber ecosystem to provide the communications sector and the Commission new information, insights and situational awareness regarding innovative solutions to these particular cyber risks.").

[5] Communications Sector Coordinating Council, Industry Technical White Paper, July 17, 2017, at https://www.comms-scc.org/botnets.

Notwithstanding these significant efforts that are core to our operations, there remain crucial challenges and limitations on those efforts that ISPs are not in a position to address. For example, an increasing percentage of internet traffic today is encrypted, and blocking tactics are a tool suited to targeted circumstances rather than wide-scale deployment; further, although most large U.S. network service providers have implemented IP filtering or source address validation using IETF best common practices such as BCP 38 and 84, even these solutions are not foolproof, as over 30 percent of the overall IP address space can still be spoofed.[6]

In many cases, more aggressive automated action on the part of ISPs to mitigate botnets is fraught with risks. Often, a "command & control" server for a botnet is not completely under the control of the malicious bot herder, and therefore blindly applying a botnet mitigation method such as filtering the IP address would prevent all the services that share the resource (e.g. DNS, shared server, or service) from being accessible. In short, without full knowledge of the device, application and traffic flowing between the network service provider and customer, a network service cannot blindly filter the traffic to that end-point without potentially violating service level agreements or negatively impacting critical services.

C. CALL FOR ECOSYSTEM-WIDE PROGRESS

Rather than focusing exclusively on how to mitigate botnet attacks once they are underway, all stakeholders in the internet and communications ecosystem must take bold new steps to prevent them in the first place. ISPs have implemented and will continue to implement powerful measures to secure against botnets and other cyber threats, but ISP efforts alone cannot sufficiently address these threats and vulnerabilities. This is a span of control issue and requires

[6] *See* Cisco Public White Paper, *Encrypted Traffic Analytics* (© 2017), at https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/nb-09-encrytd-traf-anlytcs-wp-cte-en.pdf (noting that Gartner estimates that 80 percent of internet traffic will be encrypted by 2019); and Center for Applied Internet Data Analysis, *State of IP Spoofing*, at https://spoofer.caida.org/summary.php.

the involvement of the entire ecosystem as the dynamic and innovative internet economy deploys devices and applications outside the control capabilities of an ISP at an increasingly rapid pace.

We welcome the active participation of other important players in the internet and communications ecosystem. To be clear, we readily accept ISPs' important role in addressing these challenge, and we are pleased that the attention this initiative under the Executive Order has brought to this issue has increased the depth of understanding that malicious botnets and other automated and distributed cyber threats constitute an ecosystem-wide challenge that requires a holistic ecosystem-wide suite of distributed and multilayered solutions. To that end, we reaffirm the CSCC Industry Technical White Paper's six recommendations for attack mitigation[7] and three recommendations to improve endpoint security,[8] and we offer the following further comment in response to the seven questions in NTIA's RFC.

III. ADDRESSING THE QUESTIONS IN THE REQUEST FOR COMMENT

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?

The NIST Cybersecurity Framework process has been successful because it has given the private sector ownership of cyber risk management. USTelecom and our members led the most in-depth and far-reaching effort to implement the Framework to date: the groundbreaking initiative under the CSRIC IV Working Group 4 (WG 4) from 2014 to 2015 through which over 100 cybersecurity experts developed guidance for companies in all five segments of the

[7] *See* CSCC Industry Technical White Paper, July 17, 2017, *supra* at note 5, recommendations for Attack Mitigation: (1) Encourage continued migration to all IPV6. (2) Ensure that shared cyber threat information is actionable and tailored to meet the needs of recipients. (3) Include pre-negotiated provisions for traffic filtering in transit and peering agreements. (4) Streamline the law enforcement takedown process. (5) Encourage ICANN, registries and registrars to adopt the fast flux mitigation techniques. (6) Adapt and apply machine learning to the detection of botnets.
[8] *See* CSCC Industry Technical White Paper, July 17, 2017, *supra* at note 5, recommendations for Endpoint Prevention: (1) Ensure all end points including IoT devices adhere to industry developed security standards. (2) Ensure end-points are running up-to-date software. (3) IoT devices should use network isolation or network-based filtering techniques for any communications to cloud-based services.

communications sector to use the Framework.[9] Similarly, as mentioned above, the NTIA multistakeholder processes on vulnerability research/disclosure and IoT security patching/updating are models for future work to tackle discrete problems (including important aspects of the botnet challenge), and DHS's engagement with the NSTAC and the CSCC provide additional venues for industry leadership.

These processes provide a model for cybersecurity policymaking. In this botnet reduction initiative and beyond, further processes like these will give the private sector stakeholders whose own interests are on the line the ability to develop solutions that they own, that work for them in the real world, and that they can adapt to meet fast-changing cybersecurity needs. The contrary approach – rigid, prescriptive requirements dictated by government – is antithetical to the ongoing, ever-improving processes that are necessary to secure cyberspace. We need dynamic solutions that are always looking for a better answer to threats that are always improving. Minimum proficiency checklists are the opposite of what is needed.

Along the same lines of market-oriented solutions, the demand side of this market can be very powerful. ISPs have high security standards that we expect our vendors to implement, and we utilize risk management programs that are benchmarked against the Cybersecurity Framework and attain external security certifications such as ISO27001. As part of these efforts, we seek suppliers who deliver products and services that perform to best practices to ensure network integrity. Thus critical infrastructure demand for secure products and services is an engine for driving the market to address the botnet issue and other security threats.

B. QUESTION 2: GAPS. WHAT ARE THE GAPS IN THE EXISTING APPROACHES TO DEALING WITH AUTOMATED AND DISTRIBUTED THREATS? WHAT NO LONGER

[9] *See* CSRIC IV Working Group 4 Final Report, Cybersecurity Risk Management and Best Practices, March 2015, at https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf. The five segments of the communications sector that the Working Group 4 report analyzed individually include wireline, wireless, cable, broadcast, and satellite communications.

WORKS? WHAT ARE THE IMPEDIMENTS TO CLOSING THOSE GAPS? WHAT ARE THE OBSTACLES TO COLLABORATION ACROSS THE ECOSYSTEM?

The primary gaps in existing approaches to this challenge pertain to situational awareness between the components of the ecosystem regarding both the threats themselves and also the roles of the relevant players in addressing those threats. In order for the ecosystem to develop an "immune system"-type of capability to address these distributed threats, stakeholders throughout the ecosystem need to be collectively better poised for coordinated action than the malicious actors are. Given the dynamism of the threat, market-driven solutions are the best way to address these challenges, because the only defenses that can constantly adapt as quickly as the threat are market-driven solutions.

Developing and deploying these solutions will require efficient teamwork – collaboration by design – which requires each team member to be aware of how responsibility is spread among them. Collaboration by design must account for the highly diverse and distributed complexity of the internet and communications ecosystem in all its human and automated components. This intricate system is composed of disparate players from throughout the private sector consumer and enterprise marketplace, academia, civil society, local governments and national governments worldwide. In virtually all cases, the individual stakeholders who comprise this ecosystem do not know each other and will never meet except through common use of the Internet Protocol; still, we must collectively design and implement collaborative processes such that these disparate stakeholders are exquisitely well prepared at all times to spring into action and play their specific roles in meeting cyber threats.

ISPs have unique visibility on these dynamics, but there are technical, legal, and practical obstacles to simplistic solutions that would rely exclusively on ISPs. For instance, an overwhelming amount of botnet traffic comes from unsecured end-points from outside the

United States that are not receiving software updates. This underscores the need for U.S. government international diplomatic leadership and also consistent support for market solutions that harness the dynamism and innovation of the global marketplace for information and communications technology.

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?

Per Question 1, we recommend that, in the immediate future, government and industry stakeholders should invest resources into Commerce's NIST, NCCoE and NTIA processes and DHS's NSTAC and SCC processes.

Further, per the CSCC's recommendation to streamline bot takedown processes, DoJ and FBI should use a similar industry-led model, coordinated closely with Commerce, DHS, and the State Department so as to avoid duplicating efforts, to further develop the productive relationship that exists between ISPs and law enforcement on these operations.[10] The increasing ubiquity of connected devices in homes and enterprises underscores the need for this productive relationship to continue to advance in the future; a takedown of a botnet that controls IoT devices, for instance, could disrupt consumers' and businesses' connected environments in complex practical and even physical ways that are far more complex than the effects of a takedown in the pre-IoT era (*e.g.*, temporary loss of internet connectivity to individual computers).

Additionally, Commerce should convene similar industry-driven processes to promote the design and deployment throughout the global market of applications, services, and end-points

[10] Individual USTelecom members generally feel that botnet takedown activities with law enforcement have become increasingly well-coordinated and efficient in recent years, including an improved understanding of ISP operational and legal needs in various takedown circumstances.

that perform to the highest standards and cybersecurity best practices such as supporting automated software updates and providing updates as needed in a timely manner. As discussed further below, government and industry should initiate further efforts to advance new distributed approaches such as the promising solutions that are developing in the market in the space between the ISPs and devices such as manufacturer usage descriptions (or "MUDs"), "smart routers," middleware, cloud-based IoT security solutions, and network isolation and filtering.

Over the longer term, we recommend that these government-facilitated private sector-driven processes should be the foundation and engine of all policymaking activities regarding cybersecurity; as such, the government should invest in sufficient funding and government employees to enable these processes. There is a vast disparity between the funding and personnel applied to government-only cyber activities as compared to the funding and personnel dedicated to industry-facing activities at Commerce, DHS and DoJ/FBI. While we recognize the importance of government cybersecurity capabilities, the gross shortfall in investment in the parts of the government that support industry-driven cybersecurity processes and industry-government collaboration constitutes a long term threat to our national security, as it creates a bottleneck for crucial industry input and solutions.

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?

The broad internet and communications ecosystem was a major focus area in the CSRIC WG4 effort to adapt the Cybersecurity Framework to various communication segments, and a sub-group leading this effort identified 27 unique ecosystem categories (e.g., hardware vendors, operating-system vendors, backbone network operators) that together form a complex system of

cybersecurity interdependencies.[11] A clear take-away from this effort was that effective management of cybersecurity risk requires significant participation from multiple stakeholders from the enterprise level up through the broader sector level. However, the various responsibilities of the 27 components of the ecosystem identified in the WG4 report are unclear and in most cases altogether unknown. This creates a scenario that is ripe for the fallacy of utopian solutions narrowly focused on one or two components of the ecosystem – for instance, that ISPs can simply be empowered to shut down all botnets, or that devices can be universally secure, or that consumers can become omniscient. We call for a follow-up NTIA multistakeholder process to look specifically at the questions of which stakeholders are legally and financially responsible for what – in other words, how specifically do the stakeholders "share responsibility"?

End-point devices are obviously crucial to this challenge, and concerted efforts in industry to promote NIST and NTIA stakeholder driven consensus processes to improve device security would be valuable. The same is true for software applications providers, which have a key role to play in ecosystem and need to have a prominent seat at the table. As with other important components of the ecosystem, namely ISPs, prescriptive and static compliance requirements are not the answer for devices and software. Compliance checklists for these elements could be a perilous path toward compliance checklists for other players as well.

As with other in-depth discussions of these issues, the NIST/NCCoE workshop on July 11-12 illuminated that there is no single panacea to this challenge; instead, it is an ecosystem-wide challenge with a need for multi-layered and distributed solutions. There were many comments at the workshop that began with a focus on single solutions, but those discussions ultimately illuminated the practical complexity of fully implementing any single solution, and

[11] CSRIC IV Working Group 4 Final Report, Cybersecurity Risk Management and Best Practices, March 2015, *supra* at note 9.

the futility of any one approach as a sufficient solution. Instead of an exclusive focus on one or two sets of stakeholders – important as ISPs and devices are to meeting this challenge – there are also promising solutions that are developing in the market in the space between the ISPs and devices such as those noted above in Question 3. In the coming year and beyond, Commerce should charter a well-coordinated industry-led effort to explore the possibilities – and also the limits – of this growing competitive market and promote promising solutions.

Beyond its crucial convening role, government can also promote important assistance for the private sector (particularly small and mid-sized businesses) to implement secure solutions and support industry efforts to build consumer and enterprise awareness of the threats and simple steps they can take to mitigate the risks. Government is also necessary for the international collaboration and coordination that is imperative to addressing this global challenge.

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?

Stepping back from the specifics articulated above, the government's fundamental and primary role must be to support the companies that are our country's front line defenders against sophisticated criminal and nation-state adversaries. Government must always be unequivocally on the same side as its industry partners, working in supportive partnership against malicious adversaries rather than a top-down hierarchical relationship based on compliance and mandates.

This fundamental imperative has many components. One in particular that is specific to ISPs, particularly given the possible transition to FTC jurisdiction of FCC data security rules adopted in 2016, is that government should avoid undermining the public-private partnership with "punish the victim" enforcement actions and lawsuits against companies that have been attacked by criminals and our country's enemies. Industry players who choose to work proactively in constructive, candid partnership with the government to address these threats

should be granted formal protection against legal liabilities that may arise from the risks that they are working with the government to defend against. The Cybersecurity Information Sharing Act ("CISA")[12] provides an important statutory grounding for protections with regard to sharing digital diagnostics and threat information, but we need to go beyond tactical information sharing to in-depth strategic collaboration against advanced cyber threats. This type of partnership simply cannot take place in an environment in which companies are concerned about potential liabilities or how their own government might punish them if they are unsuccessful in defending themselves against the world's most sophisticated organized crime groups and nation-state intelligence services.

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?

One fact that should undergird and guide all policymaking in this arena is that distributed and automated cyber threats are a global problem that cannot be addressed solely with domestic U.S. solutions. To make that point more concrete, USTelecom member NTT, a global Tier 1 provider based in Japan and providing IP backbone service worldwide, estimates that 60 percent of the Mirai IoT botnet attack came from IP addresses in Asia.[13] It is futile to think that the United States can solve this problem alone. Instead, in the words of NTT, malicious botnets are "an international problem which requires global cooperation." In practice, this means active and ongoing coordination by allied governments and their private sector companies, for instance, to advance international peering agreements to allow for streamlined international law enforcement takedowns and reduction in international bot-driven traffic from insecure devices.

[12] Cybersecurity Information Sharing Act of 2015, enacted December 18, 2015 as part of omnibus legislation, Pub. L. No. 114-113.
[13] NTT Comments on Promoting Stakeholder Action Against Botnets and Other Automated Threats, July 21, 2017.

G. QUESTION 7: END USERS. WHAT CAN BE DONE TO EDUCATE AND EMPOWER USERS AND DECISION-MAKERS, INCLUDING ENTERPRISES AND END CONSUMERS?

USTelecom and other industry partners are poised to develop cross-sector solutions to these challenges that draw on the market power of billions of consumers and hundreds of thousands of enterprise customers worldwide. We need government's convening power to bring together relevant players such as network/routing and cloud providers, device manufacturers and software developers to work with ISPs to develop well-informed and truly effective approaches regarding notice to consumers and enterprise end-users, managed security services for enterprises, and home network approaches to securing IoT devices. We propose that Commerce convene this industry-led effort, in close coordination with DHS and DoJ/FBI.

IV. CONCLUSION

In closing, we restate the imperative of shared responsibility. In the words of the CSCC Industry Technical White Paper: "It is a fallacy to believe that any single component of the internet ecosystem has the ability to mitigate the threat from botnets and other automated systems."[14] To the contrary, each and every component is implicated by such threats and able to contribute to the process of addressing them. USTelecom and our members cannot solve these challenges alone, but we are eager to help lead industry toward collaborative solutions.

[14] *See* CSCC Industry Technical White Paper, July 17, 2017, *supra* at note 5.