Before the
**NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION**
**U.S. Department of Commerce**
Washington, DC 20004

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

**COMMENTS OF THE**
**TELECOMMUNICATIONS INDUSTRY ASSOCIATION**

## I. INTRODUCTION

The Telecommunications Industry Association (TIA)[1] respectfully submits these comments in response to the National Telecommunications & Information Administration's (NTIA's) Request for Comments on Promoting Stakeholder Action Against Botnets and Other Automated Threats.[2]

First and foremost, TIA appreciates NTIA's inclusive approach to gathering industry expertise and insights in addressing the critical issue of automated and distributed threats. Partnership across the ecosystem is vital to mitigating and combatting these threats, and an industry-oriented approach is indispensable to this partnership. We see NTIA's RFC as a beginning of this collaborative process, and TIA looks forward to participating at all stages.

As our world grows increasingly interconnected and cyber threats become more prominent and sophisticated, policymakers must foster a resilient cyber environment by promoting good cyber hygiene; national and international communication, across both industry and government; and adaptable mechanisms for responding to cyber threats. Advances in technology pay unforeseeable dividends in our quality of life, but maintaining trust in the security of information and systems is critical to promoting the use of these technologies and preventing catastrophic breaches to the network. As the Internet is a shared resource, building and maintaining cyber resilience is a shared responsibility. The degree to which industry and government collaborate to secure the cyber ecosystem will decide the safety of our data and the degree to which society can reap the benefits of living in the digital age.

Cyber resiliency requires industry-driven, dynamic, flexible risk management. Rigid regulatory requirements that by their nature will be unable to keep up with rapidly evolving technologies and threats would require industry to focus on obsolete security requirements rather than facing the actual threat at

[1] TIA is the leading trade association for the information and communications technology ("ICT") industry, representing companies that manufacture or supply products and services used in global communications across all technology platforms. TIA represents its members on the full range of policy issues affecting the ICT industry and forges consensus on industry standards. Additionally, as an ANSI-accredited organization, TIA writes and maintains voluntary industry standards and specifications, as well as formulates technical positions for presentation on behalf of the United States in certain international standards fora.

[2] Request for Comments on Promoting Stakeholder Action Against Botnets and Other Automated Threats, NTIA, Docket No. 170602536-7536-01 (June 8, 2017) ("RFC").

hand, effectively making systems less secure. Policymakers should continue to strengthen the broader cyber ecosystem through multistakeholder efforts to develop common understanding of cyber risk management, promote best practices, and provide sufficient resources to address current and emerging threats.

Ecosystem-wide threats like botnets demand a collaborative, grassroots approach to develop resiliency across the ecosystem. Cyber resiliency requires security by design and intentionality regarding what gets connected and what does not, but must also account for the reality that nearly all devices and systems are vulnerable to compromise by sophisticated actors. In order to reap the incalculable benefits of the Internet of Things (IoT), policymakers and enterprises must operate from a risk-based mindset while balancing the goal of mitigating damage after attacks occur with the practical challenges of doing so.

Analogous to good public health practices, we should not seek to achieve a perfectly sterile environment. Instead, government and industry should work towards a cyber resilient ecosystem that is sufficiently secure to deter attackers. To do so will require widespread collaboration that fosters and utilizes the diverse technical solutions developing in a burgeoning competitive marketplace.

EO 13800's direction to federal agencies, prioritizing holistic attention to risk management through implementation of the Cybersecurity Framework ("CSF" or "Framework"), developed by industry in a process convened and facilitated by NIST, is a good start on the path to promoting cyber resiliency.[3] In the near term, government should continue this effort to lead by example in modernizing its own cybersecurity risk management, while working to facilitate market solutions. Government multistakeholder processes are well-suited to foster common language and understanding about these challenges and solutions. Long term cyber resiliency will require workforce training, international collaboration, and investment in research and development of next generation technologies.

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

**A Flexible, Consensus-Based Approach:** Experience shows that a flexible and consensus-based approach is more effective than strict mandates. Particularly when addressing the rapidly-shifting, international nature of automated and distributed threats, successful approaches will encourage participants in the ecosystem to opt in and even compete for better solutions rather than comply with a mandatory bare minimum. Building and maintaining a resilient network is a shared responsibility across all segments of the ecosystem – no one industry or group can secure the network alone. Therefore, the path towards solutions must be shared as well.

**Industry Collaboration:** Private industry stakeholders have a history of working collaboratively to address these ecosystem issues. As an ANSI-accredited standard setting organization, TIA has brought industry stakeholders together to develop technical solutions for a wide range of ICT challenges. Industry

[3] *See* Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, (May 11, 2017) (EO 13800); *see also* NIST, The Framework for Improving Critical Infrastructure Cybersecurity (Feb. 12, 2014).

stakeholders, including TIA and its members, continue to put considerable time and effort into developing standards in IoT cybersecurity specifically.[4] In addition to work on technical standards, TIA hosts a cybersecurity working group (CWG) that brings TIA members together to inform, connect, and advocate on cybersecurity policy. TIA's CWG continues to bring together industry and policymakers across various segments of the government to talk about challenges and opportunities for securing the IoT ecosystem, and to educate more broadly on cybersecurity (both within TIA and to external audiences).[5]

**Government-Facilitated Multistakeholder Processes:** Additionally, many government-facilitated stakeholder-driven approaches are already making strides to build cyber resiliency. The Department of Homeland Security's National Security Telecommunications Advisory Committee (NSTAC) as well as the Information Technology and Communications Sector Coordinating Councils convene industry stakeholders to provide recommendations regarding the nation's emergency preparedness and critical infrastructure security.[6]

Likewise, as noted above, the Cybersecurity Framework already accommodates a wide variety of organizations' differing cybersecurity needs across the broad landscape of the economy and provides a common language for addressing cybersecurity threats.[7] As TIA has noted elsewhere, the Framework has carefully balanced the development of meaningful communication tools with the need for a flexible, voluntary risk management process.[8] Beyond the Framework itself, NIST's workshops bring stakeholders together from all over the globe to address pressing issues contributing to automated and distributed threats such as securing the supply chain and authentication.[9] As NIST's work continues, TIA looks forward to continued partnership. Similarly, NTIA's ongoing multistakeholder processes, which have brought stakeholders together to address issues related to patching and updatability, and vulnerability disclosure, for example, offer a tested mechanism for further collaboration.[10] TIA and many of its members participate in this process and look forward to leaning on the useful work these processes produce.

NTIA already has the momentum to kick start such an approach here. As agencies work to meet the botnet reduction initiative laid out in EO 13800, NTIA's multistakeholder process could serve as an invaluable forum for the massive amount of work that needs to be done in this space. NTIA has a proven process for bringing a wide range of stakeholders together. There is no reason why that process could not be used to advance the goals underlying the EO.

---

[4] *See generally* Cisco, Manufacturer Usage Description ("MUD"); oneM2M, Published Specifications; NTIA, IoT Standards Catalog, Draft.

[5] TIA Securing the IoT (June 8, 2017) (bringing together industry experts, government, and cybersecurity thought leaders to discuss automated and distributed threats). The video recording was distributed broadly throughout TIA's membership, circulated on the Hill, and published on TIA's Facebook page and website. TIA's CWG also hosted a Cybersecurity Policy Briefing in May 2017, which educated TIA's widespread membership (many beyond the beltway and some international) on the cyber threat landscape, current policy initiatives, and how TIA member companies can engage in the process.

[6] *See* About NSTAC; *see also* IT Sector Coordinating Council, US Communications Sector Coordinating Council.

[7] *See* NIST, The Framework for Improving Critical Infrastructure Cybersecurity (Feb. 12, 2014).

[8] TIA Comments on Framework Version 1.1, at 2 (April 10, 2017).

[9] NIST Cybersecurity Framework Workshop 2017 (July 21, 2017).

[10] *See e.g.* NTIA Multistakeholder Process on Internet of Things (IoT) Security Upgradability and Patching.

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

Despite the volume of great work being done across the cybersecurity stakeholder community, several major issue areas still create obstacles to innovation and collaboration.

**The Economic Model:** First and perhaps foremost, cybersecurity is seen by many enterprises as an expense. In addition to basic capital, adequate risk management systems require significant staff time and resources. For some companies (especially startups) for whom cost can be prohibitive, any efforts to encourage better cybersecurity practices need to focus on lowering the costs and clarifying the financial benefits of implementing such practices.

**The Language Barrier:** There is a language barrier to crafting a unified approach to cyber resilience. The unparalleled diversity of those responsible for building and maintaining the ecosystem (spanning hundreds of spoken languages, a multitude of professional disciplines, culture, and more), contributes to the rich potential of the Internet, but at the same time it presents an immense challenge to crafting a coordinated approach to cyber resiliency. The government has already done a significant amount to break this barrier down, most notably in convening industry to develop the Framework, but could perhaps do more to help bridge those divides through additional multistakeholder efforts. We have already benefitted from much of this work and must build on that work in the years ahead.

**Barriers to Information Sharing**: TIA sees three primary barriers to information sharing: resources, return on investment, and regulation. Like cybersecurity in the broader sense, information sharing is expensive. Collecting and analyzing data, even internally, requires significant time, money, and personnel that many companies cannot afford to allocate. Given the opportunity cost of allocating these resources to sharing information (between departments, across industry, or with the government), there is not always a clear return on that investment, which most private enterprises require to justify expenses to boards and shareholders. Finally, when asked to share information with government entities, companies must tread a careful line in speaking to their regulators. Information sharing has different implications depending on the agency – while the FBI may want an ISP to maintain all evidence related to a breach so that it can build a case against an attacker, DHS may want the breach patched as soon as possible. Even those agencies without rulemaking or enforcement authority often strive to operate in transparent processes which make shared information public and available for other regulators.

**The International Problem:** As specifically outlined in Question 6 of the RFC, botnets are an ecosystem issue requiring an international effort to address. At the recent NIST Workshop on *Enhancing Resilience of the Internet and Communications Ecosystem*, Georgia Tech Professor David Dagon spoke about disparate incentives for enhancing cybersecurity between countries whose economies rely heavily on the Internet and those that do not. As the Communications Sector Coordinating Council notes, most botnet traffic is initiated from outside the United States.[11] While U.S. law enforcement may be able to identify from which country an attack originates and may even be able to pinpoint the attacking entity itself, it can also be difficult to bring local laws to bear. With respect to insecure devices, most relevant supply chains are exceedingly complex and in the scope of those chains attackers will exploit the weakest

[11] CSCC Industry Technical White Paper at 13 (July 17, 2017).

defense. For protective measures to work, different components of the supply chain must have similar information and awareness. TIA has noted elsewhere that the global nature of ICT requires international and industry-driven best practices and standards.[12] As automated and distributed cyber threats are international in nature, a U.S.-only approach will prove inadequate. International agreement on such issues, while vital, can be complex and difficult to achieve.

**IV.** ***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?

**Improve Government Cybersecurity Practices:** Modernizing the government's own IT systems and cybersecurity risk management processes is a critical immediate step. In addition to protecting the safety of our nation's systems, by getting their own houses in order, policymakers can educate themselves and promote good cybersecurity practices through procurement processes. By requiring federal agencies to start using the Cybersecurity Framework, EO 13800 has taken a step in this direction. Of course, the modernization of government IT systems will require ongoing work beyond this initial action.

**Facilitate a Competitive Cybersecurity Market:** As discussed above, existing approaches like the NTIA multistakeholder processes offer a viable near-term solution. Companies all over the globe are working to develop smart forms of network management and technologies at the edge to diminish the propagation of botnets. For example, Samsung and IBM recently partnered to develop ADEPT (Autonomous Decentralized Peer-to-Peer Telemetry), which uses blockchain technology to build a distributed network of IoT devices, providing a secure, low-cost way for devices to interact.[13] Through development of ADEPT, the partnership hopes to enable self-maintaining IoT devices to signal operational issues, retrieve patches, and more.[14] At the network level, Cisco's ASA Botnet Traffic Filter complements existing endpoint security solutions by monitoring network ports for rogue activity and detecting infected internal endpoints sending command and control traffic back to a host on the Internet.[15] The Ericsson Security Manager transitions security from the traditional manual and reactive approach to an automated, predictive approach in which the security management function and policy orchestration engine dynamically deploy and adjust security controls and related configurations in real time to meet changing threats.[16] These are just a few examples. In the near term, NTIA could accelerate these and other solutions through its multistakeholder process. By convening experts to develop a better understanding of the challenges and opportunities in developing market solutions, NTIA can foster cyber resiliency across the ecosystem.

---

[12] *See* TIA Comments on NIST Framework v1.1.
[13] *See* IBM ADEPT Practitioner Perspective – Pre Publication Draft (Jan. 7, 2015).
[14] *Id.*
[15] Cisco ASA Botnet Traffic Filter.
[16] Ericsson Security Management.

**Invest in Research & Development:** As multistakeholder efforts present an important immediate step, they must be matched with resources to drive innovation forward. With the advent of distributed trust technologies and developments in quantum computing, our systems are on the verge of major change. To remain competitive in international markets and defend against foreign adversaries, the United States must invest in and encourage investment in cutting edge ICT research. The government should prioritize funding for NIST and NTIA and should consider grants for public/private research and development.

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

As noted above, TIA believes that collaboration by all stakeholders in the ecosystem is imperative and that it should be broadly inclusive and widely representative. Every stakeholder has a role to play in sharing the responsibility of bringing security and resiliency to the ecosystem. TIA and its members embrace this shared responsibility.

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

**Be an Example:** As noted above, choices the government makes through procurement processes and behavior ripple throughout the ecosystem. For many major ICT companies, government agencies and institutions are the most significant customer base. Even in areas where the government does not represent the largest customer, however, by developing good cyber risk management processes and modernizing IT systems, the government can better protect the people it serves, help train a sophisticated cyber workforce, and demonstrate American commitment to the shared responsibility of cyber resiliency abroad.

**Convene and Facilitate:** Government should act as a convener and facilitator, rather than imposing a singular, inflexible regime that would govern all stakeholders' activities in a one-size-fits-all fashion. Where industry leads in technical innovation and expertise, government is in a good position to bring diverse stakeholders together to exchange information and build on each other's ideas. As noted above, existing multistakeholder processes are already driving positive changes in this regard, and these processes are particularly well-suited to addressing ecosystem-wide issues like botnet reduction.

**Share Information:** Additionally, government may often be in the best position to learn of information that is valuable to the private sector's ability to respond to threats. The government should demonstrate its willingness to share that information. Specific moves like formalizing the interagency vulnerabilities equities process would be a great start.

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

While no one country can solve the botnet threat by itself, the U.S. can lead the way. As discussed above, industry is already working to develop diverse technical solutions to build cyber

resiliency and collaborate across sectors. TIA and its members engage in a number of forms of international outreach and help facilitate international dialogue. The government can provide valuable help by improving its own security and by promoting good cybersecurity practices internationally. Given the need for immense international coordination, agreement with respect to policy at the nation-state level is paramount.

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

Enhanced awareness of threats across every segment of the ecosystem is critical to promoting better cybersecurity practices and developing a workforce ready for the future. User education should be achieved flexibly rather than through a one-size-fits-all regime like labelling, which focuses solely on specific pieces of the stack. Much is already being done to educate in this space, and certainly both consumers and enterprises have an important role to play as stakeholders in the ecosystem. As government and industry work to enhance cyber resiliency and empower smart cybersecurity decision-making, technologists should also focus on developing solutions that move the burden of securing the network away from the end user and toward smart, self-reliant systems.

## IX. CONCLUSION

As policymakers move forward in response to EO 13800, government efforts should focus on leading by example and facilitating the burgeoning competitive cybersecurity risk management market. By modernizing agency risk management practices, government can use procurement to foster innovation, train sophisticated cybersecurity professionals, and demonstrate its commitment to the shared responsibility of cyber resiliency. In the near term, government should capitalize on its existing expertise as a facilitator of industry stakeholders to drive market solutions and lower cybersecurity costs. In addition to being international advocates for good cyber hygiene and a common risk management approach, policymakers across the government should prioritize funding and incentives for research and development in cybersecurity in the United States.

TIA thanks NTIA for its leadership on these issues and looks forward to continued collaboration in the months ahead.

Respectfully submitted,

TELECOMMUNICATIONS INDUSTRY ASSOCIATION

By: */s/ Savannah Schaefer*
Savannah Schaefer
Sr. Manager, Government Affairs
Telecommunications Industry Association
1320 N Courthouse Rd Suite 200
Arlington, VA 22201

July 28, 2017