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. 180103005–8005–01
	)	
	)	

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 ("RFC") on the draft Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats.[2]

TIA supports the open and collaborative approach that the Departments of Commerce and Homeland Security haven taken to gather industry expertise and insights in addressing the critical issue of automated and distributed threats. As TIA noted in its response to NTIA's original RFC under this initiative, "[p]artnership across the ecosystem is vital to mitigating and combatting these threats, and an industry-oriented approach is indispensable to this partnership."[3] As NTIA works to enhance and refine the Draft Report, TIA and its members will continue to collaborate on the work ahead.

Overall, we find the Draft Report to be a significant first step forward in promoting stakeholder action to address botnets. The most significant work still lies ahead, and we think the Draft Report can be improved with several refinements, but we want to begin by emphasizing the importance of this first step. The Draft Report effectively targets how policymakers and stakeholders alike should collaborate to address automated, distributed threats and ecosystem-wide cybersecurity challenges more broadly. As a vital foundation, the Draft Report acknowledges cybersecurity risk management as a shared responsibility between all participants in the ecosystem and emphasizes the need for widespread collaboration to

[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. 180103005–8005–01 (January 11, 2018) ("RFC"); A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats (January 5, 2018) ("Draft Report").

[3] Comments of the Telecommunications Industry Association, NTIA Request for Comments Promoting Stakeholder Action Against Botnets and Other Automated Threats, (July 28, 2017) at 1.

address threats and foster resiliency.[4] The Draft Report recognizes that "global action will require globally accepted security standards and practices" and that those standards should be "flexible, appropriately timed, open, voluntary, industry-driven, and global in nature."[5] The Draft Report effectively prioritizes immediate steps by directing government to lead by example and by placing particular focus on increasing large enterprise security risk management to drive the demand side of the security market.[6] The Draft Report outlines fundamental steps for long term improvement by prioritizing education, outreach, resource development for small and medium sized businesses and consumers, as well as investment in basic cybersecurity research and development.[7]

As discussed in greater detail below, TIA suggests several key refinements in the final draft of this report:

- First, while the Draft Report generally takes a holistic view of the Internet infrastructure ecosystem and advocates shared responsibility among participants in that ecosystem, the final report should maintain that holistic approach throughout by focusing on securing the product *environment* with an eye toward security-by-design throughout the development cycle and component elements of various products, as opposed to relying solely on the security of individual end products.

- Second, while it recognizes the vital role of industry led initiatives to develop standards and best practices, the final report should make clear that any approach to develop security assurance or certification programs should be industry-driven, geared toward harnessing market drivers for security, and take care to avoid creating a false sense of security or calcifying into static compliance checklists that require companies to comply backwards rather than innovate forward.

- Third, as it discusses the important priority of securing federal IoT, the final report should make clear that these guidelines and profiles should be developed in an open collaboration with industry, should be based on risk management principles and technology neutrality, maintain a mechanism for refreshing guidelines to keep apace of emerging technologies and security innovation, and should make clear that specific requirements should not be hardcoded into statute.

---

[4] *See e.g.* Draft Report at 3 (identifying a principle theme that "[a]utomated, distributed attacks are an ecosystem-wide challenge" and that "[n]o single stakeholder community can address the problem in isolation").
[5] Draft Report at 16. *See also* Draft Report at 3 (identifying a principle theme that "automated, distributed attacks are a global problem" and that "[i]ncreasing the resilience of the Internet and communications ecosystem against these threats will require coordinated action with international partners").
[6] *See e.g.* Draft Report at 29 (identifying Action 2.3 that "[t]he federal government should lead by example and demonstrate practicality of technologies, creating market incentives for early adopters"). *See generally* Draft Report at 23-28 (discussing Goal 1 to "[i]dentify a clear pathway toward an adaptable, sustainable, and secure technology marketplace").
[7] *See e.g.* Draft Report at 26-27 (identifying in Action 1.3 that "where applicable, government should prioritize the application of research and development (R&D) funds and technology transition efforts to support advancement in DDoS prevention and mitigation, as well as foundational technologies to prevent botnet creation"); *id.* at 35-38 (discussing Goal 5 to "[i]ncrease awareness and education across the ecosystem").

Finally, as government and industry stakeholders collaborate to address current and future cybersecurity threats, we should take a process-based approach in the direction of our policy efforts: identifying risks faced (as this report does), directing resources to priority areas of focus, responding in a timely fashion as areas of weakness are exploited, and continuing to reevaluate our approach over time as the technology landscape changes. In the near term, government can build on the momentum catalyzed by Executive Order 13800. As one crucial overarching actionable next step, the final report should build on the success of this process to date by launching follow-on multi-stakeholder workstreams with a clear playbook of agency roles and responsibilities so that industry can continue to drive innovative advances in cybersecurity policy that dovetail with the security innovations that are accelerating in the market.

I. AS THE DEPARTMENTS DEVELOP THE FINAL REPORT, TIA SUGGESTS SEVERAL AREAS FOR REFINEMENT.

a. Maintain a holistic, shared responsibility approach throughout all aspects of the final report.

The final report should focus on securing the product *environment* with an eye toward security-by-design throughout the development cycle, rather than relying solely on the security of individual end products. While the Draft Report identifies and discusses an important goal in increasing product security over time, some language focuses too narrowly on the product itself rather than encouraging a holistic risk assessment approach. For example, Principle Theme #3 states that "[p]roducts should be secured during all stages of the lifecycle."[8] However, as the Draft Report accurately notes, legacy technologies pervade the Internet ecosystem and will take some time to transition out of the market.[9] Security-by-design is the ideal toward which we strive in product development, but taking concurrent steps to secure the broader product environment holistically promotes technology neutrality, and fosters opportunities for innovative security services and gateway technologies to manage risk. In the near term the final report should recommend new government-industry collaboration to secure the product environment, platform, or systems throughout each stage of the product lifecycle.

The report should clearly reflect the holistic definition of the infrastructure ecosystem described Section II. Section II of the Draft Report defines "infrastructure" as including "the technology and organizations that enable connectivity, interoperability, and stability, going beyond the physical wires, wireless transmitters and receivers, and satellite links to include the hardware, software, tools, standards, and practices on which the ecosystem depends – for example, routers, switches, Internet service providers, DNS providers, content delivery networks, hosting and cloud-service providers."[10] It critically recognizes that given "the complexity of modern infrastructure, with key tools and players interspersed through the ecosystem, no single tool can secure the infrastructure."[11] In later portions of the report, however, that view seems to simplify, focusing primarily on the role of ISPs and their relationships with enterprise networks. The next workshop should include a session focusing on

[8] Draft Report at 3.
[9] Draft Report at 15 (acknowledging that "[t]here are many legacy servers, desktops, laptops, and mobile phones in use today, and this will be the case for the foreseeable future").
[10] Draft Report at 9-10.
[11] *Id*. at 10.

determining the roles and describing the activities of additional participants in the infrastructure domain so that the final report reflects actionable steps for all elements of infrastructure.

b. Foster incentives to innovate forward rather than comply back ward.

The Draft Report recognizes the vital role of industry-developed standards and best practices. To that end, any approach to security assurance or certification should be industry-driven and geared toward harnessing market drivers for security, and should take care to avoid creating a false sense of security or calcifying into static compliance checklists that require companies to comply backward rather than innovate forward. Important challenges with respect to cybersecurity assurance or certification have been detailed at various stages in this process and others. Many industry organizations across sectors and internationally are working to develop assurance or certification programs, and we recommend that the final report promote activity to advance these initiatives.

c. Any approach toward securing federal IoT should be developed in an open collaboration with industry, should be based on risk management principles and technology neutral, should maintain a mechanism for refreshing guidelines to keep apace of emerging technologies and security innovation, and should make clear that specific requirements should not be hardcoded into statute.

By prioritizing security of the government's federal networks and directing agencies to collaborate with industry on the development of federal procurement guidelines and profiles, the Draft Report identifies an important step in deterring automated, distributed threats. By transitioning off of legacy network technology, adopting a flexible process-based approach to risk management, and using industry-driven best practices, the government can provide leadership in the development of those practices and drive demand for security in the broader marketplace.

However, the Final Report must make clear that these efforts should follow core principles. In short, any approach to securing Federal IoT:

- Should be developed in an open collaboration with industry,
- Should be based on risk management principles and technology neutral,
- Should maintain a mechanism for refreshing guidelines to keep apace of emerging technologies and security innovation, and
- Should make clear that specific requirements should not be hardcoded into statute.

II. AS A CRITICAL OVERARCHING ACTIONABLE PRIORITY THE FINAL REPORT SHOULD DIRECT FOLLOW ON COLLABORATIVE PROCESSES BETWEEN GOVERNMENT AND INDUSTRY TO ADDRESS KEY ISSUES.

The final report should identify actionable areas to build on current momentum with follow on work between federal agencies and industry to develop targeted recommendations for key issue areas. An initial step would be to prioritize which issues are most pressing and in need of addressing, but follow on work streams might convene stakeholders to tackle any number of identified issues (for example, the notion of "shared responsibility," related legal obligations and responsibilities; how to improve international and cross-border and cross-sector collaboration in real world operational settings; etc.).

Follow on work should build on the example of this process, with a clear interagency playbook of roles and responsibilities (e.g. which agency would convene stakeholders, what expertise or outreach other agencies would contribute) so that the agencies play to their strengths and the processes are navigable for organizations with limited resources. As the Draft Report notes in discussion of Governance, Policy, and Coordination, "lack of clarity around roles and responsibilities has impeded collective action, resulting in security failures."[12] As this process has demonstrated, stakeholders are ready to participate in policy problem-solving, but we need to have an organized, targeted way to do so. Many organizations, even billion-dollar enterprises with an international footprint have only a few or even one person tasked with engaging in Washington, D.C. Stakeholders of all backgrounds need to be able to know where to engage or where to direct the attention of subject matter experts to meaningfully participate.

The process that NTIA, NIST, and DHS have undertaken thus far in this initiative has been a model of coordination, efficiency, and promotion of private sector expertise and experience. We recommend that any and all follow up actions follow a similar model.

III. CONCLUSION

TIA thanks the Departments of Commerce and Homeland Security for the depth of their work on these issues and their partnership in developing this report. TIA and its members look forward to continued collaboration in the months ahead.

Respectfully submitted,

TELECOMMUNICATIONS INDUSTRY ASSOCIATION

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

February 12, 2018

[12] Draft Report at 20.