February 12, 2018

VIA EMAIL: counter_botnet@list.commerce.gov

Evelyn L. Remaley
Deputy Associate Administrator
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW, Room 4725
Washington, DC 20230

Subject: ITI Comment on Draft Report to the President on Promoting Stakeholder Action Against Botnets and Other Automated Threats

Dear Ms. Remaley,

The Information Technology Industry Council (ITI) welcomes the opportunity to respond to the National Telecommunications and Information Administration's (NTIA) Request for Public Comments (RFC), on the Draft Report to the President on Enhancing the Resilience of the Internet and Communications Technology (ICT) Ecosystem Against Botnets and Other Automated, Distributed Threats, jointly transmitted by the Secretaries of Commerce and Homeland Security on January 5, 2018 (the "Report").

ITI is the premier advocate and thought leader in the United States and around the world for the global information and communications technology (ICT) industry. ITI's members comprise leading technology and innovation companies from all corners of the ICT sector, including hardware, software, digital services, semiconductor, network equipment, cybersecurity, and Internet companies. Cybersecurity is rightly a priority for governments and our member companies, and we share a common goal of improving cybersecurity. Facilitating the protection of our customers (including governments, businesses, and consumers), and securing and protecting the privacy of individuals' data are core drivers for our companies. ITI has long advocated for the importance of public-private partnerships, multistakeholder, and public notice and comment processes to develop sound cybersecurity policy, and we would like to commend the Department of Commerce – specifically, both NTIA and NIST – as well as the Department of Homeland Security for their leadership and efforts in producing the Report.

ITI appreciates and supports the government's goals of minimizing the threat of botnets and other automated threats, and strengthening the resilience of the cyber ecosystem more broadly, and we look forward to continuing our collaboration in this regard.

As a preliminary matter, we were pleased to see the themes articulated in the Report reflect several of the recommendations ITI focused on in our comments to NTIA's initial RFI on this topic.[1] In particular,

[1] *See* ITI /ITAPS Comments in Response to NTIA's Request for Public Comment - "Promoting Stakeholder Action Against Botnets and Other Automated Threats" *(Docket No. 170602536–7536–01; RIN 0660–XC035),* filed July 28, 2017, available at https://www.itic.org/dotAsset/ba2359f4-3349-4d0f-93e4-cb49bc5f14d1.pdf.

our previous public comments highlighted the global nature of the botnet problem (corresponding to Theme 1 in the Report) as well as the need to address the problem on an ecosystem wide basis (Theme 6). Our prior comments also stressed the need to find ways to increase the use of available tools by cyberspace's stakeholders (Theme 2), to drive education and awareness across the ecosystem participants (Theme 4) and advocated for greater uptake of security by design approaches including secure development lifecycles (Theme 3). We interpret the fact that many of our high-level suggestions were included in the Report as a promising sign that there is broad consensus across the stakeholder community regarding these themes, lending hope that there is a greater chance that we may realize the unity of effort that will be needed to both seize the opportunities and meet the challenges lying ahead.

Ultimately, realizing progress on many of the action items identified in the report will require close coordination and collaboration amongst and between various stakeholders and stakeholder groups, including across NTIA, NIST, DHS and other US government stakeholders, across the private sector, including not only multiple sectors but also involving small, medium and large sized business enterprises, and also internationally, with government and private sector partners alike.

Below, we provide additional feedback to the Report, focusing our comments on a few strategic recommendations as well as some of the key action items we have identified that may hold early promise, or may be worthy of refinement:

1. Leveraging public-private partnerships and building on existing initiatives and resources.
We appreciated that NTIA took on board our comments relating to the complexity and diversity across the Internet of Things (IoT) landscape, which makes it difficult to envision a set of one-size fits-all rules that could ensure security while keeping pace with the rate of change spurred by both technology innovation and the dynamic nature of the threat environment. We recommend that, in addition to the sector specific regulatory agencies mentioned in the Report, the government make full use of the expertise of all stakeholders, including the private sector, other federal agencies and departments (e.g., the Federal Trade Commission and the Department of Defense), and sector coordinating councils (SCCs). We continue to support replicating approaches that have been successful elsewhere, such as leveraging the Framework for Improving Critical Infrastructure Cybersecurity (Framework) approach wherever possible, which in addition to signifying what a highly effective public private partnership can achieve, is recognized in the Report as a key component to widely and successfully securing enterprise networks via voluntary risk-management approaches grounded in international standards and best practices.

2. Cybersecurity labels/certifications.
Action 5.1 states that the private sector should establish and administer voluntary informational tools for home IoT devices, supported by a scalable and cost-effective assessment process, that consumers will intuitively trust and understand. The following action item asks the private sector to establish voluntary labeling schemes for industrial IoT applications, supported by a scalable and cost-effective assessment process, to offer sufficient assurance for critical infrastructure applications of IoT. As we explained in our submission to NTIA's RFC, to create a trusted digital environment, the federal

government should seek to encourage companies to tailor security measures and tools to address the risks related to their specific business model. Rapid response is critical as the cybersecurity landscape evolves. Static regulatory frameworks can give consumers a false sense of security. Time consuming and expensive labels may be warranted in some contexts related to critical infrastructure protection but should not apply to consumer products with short life spans and multiple use contexts. Additionally, to enable the market to drive demand and incentivize companies to differentiate their products, certifications should not be mandatory. Further, certifications and labels may represent a market barrier especially for small and medium-sized enterprises (SMEs) and start-ups.

However, as NTIA is of course aware, NTIA previously convened a multistakeholder process to address how labels might be productively used to help improve transparency for consumers regarding the ability of IoT devices to receive security updates.[2] That effort was based on input from diverse private sector stakeholders, with flexible recommendations to adapt to the wide variety of IoT deployments. The document achieved consensus from the convened multistakeholder body. However, NTIA has not organized the final outputs of the multistakeholder process, nor has it used its convening role to work with the private sector on facilitating awareness of the outputs. Yet several reports, including this draft botnet report, suggest the need for additional work on an IoT security transparency framework – work that industry already began via the multistakeholder process. Stakeholders should seek to build on this existing effort to advance meaningful progress in this area.

ITI commends the federal government's decision to resist developing a compulsory far-reaching and prescriptive cybersecurity labelling or certification regime in the United States**.** We would advise the federal government to facilitate an industry-led, collaborative work stream to identify whether and in what contexts the voluntary scheme developed in the multistakeholder process should apply to products, components, or processes.

3. Transparency solutions.

We agree with the Report that software development tools and processes to reduce the incidence of security vulnerabilities in commercial-off-the-shelf software must be more widely adopted by industry, and that the federal government should collaborate with industry to encourage further enhancement and application of these practices to improve marketplace adoption and accountability. However, we have some concerns with the draft Report's suggestions included in Action 1.2 regarding the "role of transparency tools and practices in improving manufacturers and purchasers understanding of what goes into IoT products, such as by documenting the off-the-shelf software and firmware included in a product or device."

[2] *See* Communicating IoT Device Security Update Capability to Improve Transparency for Consumers, NTIA Multistakeholder Process on Internet of Things Security Upgradability and Patching, Jul. 14, 2017, available at https://www.ntia.doc.gov/files/ntia/publications/draft_communicating_iot_security_update_capability_-_jul_14_2017_-_ntia_multistakeholder_process.pdf.

ITI agrees with the problem statement this action item endeavors to solve. However, we are concerned that the Report preordains full disclosure of third party software components to customers as the best means of addressing these challenges. There are risks that this approach may lead to prioritization of efforts which are not necessarily the most effective in reducing cybersecurity risks. For instance, the presence of a vulnerable library in a software product does not mean it is exploitable in that product – often it in fact is not. In other cases, customer pressure may prioritize a patch to a vulnerability with a low CVSS score over a vulnerability with a higher CVSS score.

NTIA has discussed separately its intent to convene a multi-stakeholder process to explore this issue, and potential solutions, in greater depth, including further developing and promoting best practices that relate to vendors' internal processes, practices and policies governing their use, and vulnerability management, of such libraries. We support an open, multistakeholder process that examines a full range of solutions and recognizes that software component transparency is only one consideration in a holistic software security process to drive better outcomes.

4. Awareness-raising initiatives.

Cyberspace's stakeholders – consumers, businesses, governments, and infrastructure owners and operators – need to know how to reduce risks to their property, reputations, and operations. The Report appropriately aims to prioritize this work and ITI and our companies stand ready to offer our support in this regard. We support Actions 5.3 and 5.4 to encourage the academic and training sectors to fully integrate cybersecurity into pre-existing disciplines. As we mentioned in our comments to NTIA's initial RFC, the consumer awareness side of the ecosystem is an equally important part of the equation, and the government has an important role to play. Action 5.5 to establish a public awareness campaign to support recognition and adoption of the home IoT device security profile and branding is a positive step in this direction.

5. Continue international efforts and prioritize international cybersecurity standardization.

The Report emphasizes the importance of a coordinated international approach to secure cyberspace against botnets and automated threats, and in fact identifies in its first principal theme that "automated distributed attacks are a global problem." Given that many of the compromised devices in recent botnets have been geographically located outside the United States, we agree that increasing the resilience of the Internet and communications ecosystem against these threats will require coordinated action with international partners. For this reason, we are pleased to see the Report reflects our earlier recommendation urging the federal government to promote international adoption of best practices and relevant tools through bilateral and multilateral international engagement efforts in Action 4.2. We further suggest the federal government make the preservation and promotion of a global market a primary goal in setting any product assurance requirements.

In our view the U.S. needs a proactive and adequately resourced national strategy involving both industry and government working together to develop and further international cybersecurity standards. The U.S. has already made some progress in this area, including the Interagency Report on

Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity (the "International Standardization Strategy") published by NIST in 2016. We recommend that the current administration prioritize furthering this strategy to improve the U.S. government's participation in the development and use of international standards for cybersecurity. Doing so will require a unity of effort with industry, as well as adequate resources and political support.

6. Information sharing.

While we appreciate the importance of increasing the effectiveness of private sector information sharing with law enforcement laid out in Action 4.1, "ISPs and large enterprises should increase information sharing with law enforcement to provide more timely and actionable information regarding automated, distributed threats", we would like to reiterate the importance of making sure any efforts intended to spur additional sharing of cyber threat information among and between businesses and government entities to improve cybersecurity remain voluntary.

Conclusion

ITI would like to thank NTIA for its commitment to partnering with the private sector to advance our shared cybersecurity goals, and for the opportunity to share our perspectives on the Report. ITI and our member companies stand ready to work with the Department of Commerce – including both NTIA and NIST – the Department of Homeland Security, and other federal government stakeholders to further discuss how to effectively operationalize the goals and actions set forth in the Report. Realizing progress on many of the action items will require close coordination and collaboration amongst and between various stakeholders and stakeholder groups across the private and public sectors, the ecosystem and the globe, but it will also require the continued leadership of the Departments of Commerce and Homeland Security, as well as private sector stakeholders. We are available at any time to elaborate on the foregoing comments and our suggestions. Please continue to consider ITI as a resource on cybersecurity issues, and do not hesitate to contact us with any questions regarding this submission.

Best Regards,

John Miller
Vice President, Global Policy and Law
Information Technology Industry Council