U.S. CHAMBER OF COMMERCE

Ann M. Beauchesne
Senior Vice President
National Security and Emergency Preparedness

1615 H Street, NW
Washington, DC 20062
202-463-3100

February 12, 2018

Via 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: Promoting Stakeholder Action Against Botnets and Other Automated Threats

Dear Ms. Remaley:

The U.S. Chamber of Commerce welcomes the opportunity to respond to the National Telecommunications and Information Administration's (NTIA's) request for comments on the draft publication—*A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats* (the Report)—which was released by the Department of Commerce (DOC) and Department of Homeland Security (DHS) on January 5.[1]

Last July, the Chamber provided its initial views to NTIA concerning the path ahead on mitigating botnets, which can be used to launch malicious activities such as spam, phishing, and distributed denial of service (DDoS) attacks. The Report—notwithstanding some significant differences of opinion regarding regulation and liability—is mostly in keeping with the Chamber's outlook on cybersecurity.

The Report calls for stakeholders to pursue five "complementary and mutually supportive" goals to minimize the threat of botnets and strengthen the resilience of the cyber ecosystem, which, at a high level, are worth pursuing. However, underpinning the goals are 23 action items, which range in complexity and value to industry, including the time, attention, and resources required of organizations to accomplish them. The Chamber believes that some of these initiatives are best handled by industry; others, by government. And some aspects of the Report, particularly ones that call for government-directed mandates and liability regimes, ought to be jettisoned.

The Report fits well with the Chamber's leading 2018 cybersecurity policy goal. The Chamber wants to build on the positive rapport between DOC and industry in developing the Framework for Improving Critical Infrastructure Cybersecurity (the Framework) to strengthen the protection and resilience of the Internet of Things (IoT). The Chamber urges policymakers to

support DOC in convening a framework-like effort on IoT security, which would go hand in hand with easing threats associated with botnets. A flexible, nonregulatory framework could be widely used around the world by both industry and government stakeholders.

Such a framework would also help inform the benefits and drawbacks of setting minimum security standards for IoT devices through the federal procurement process, among other key topics.[2] The Report urges private entities to build and deploy IoT devices that have security features and practices that are rooted in voluntary, global, and industry-led standards, which is a helpful message.[3] The Chamber urges secure practices for the sake of the business community, consumers, and the long-term viability of device makers.

The Chamber wants leading sectors and companies to drive the solutions to help prevent and lessen the impact of botnets. Businesses have an incredible amount to gain from an internet ecosystem that is increasingly free of botnets and other automated hazards. The Chamber wants to help public and private stakeholders build bridges between organizations that employ relatively sophisticated cyber practices and those that seek to build a program and improve it over time.

***

In the Report, DOC and DHS conclude that the public-private challenges associated with substantially reducing botnets can be packaged into six themes, which the Chamber captures here for the purposes of commenting:

- **Botnets and other automated, distributed attacks are a stakeholder-wide challenge.** The Chamber appreciates the Report writers' acknowledgement that no single stakeholder community can address botnets in isolation. The Chamber, which has members operating throughout the entire internet and communications landscape, urges organizations to mitigate risks so that hazards to businesses' cybersecurity do not pool at any given point. Unmitigated risks and threats could create perils not only for companies and sectors but for cyberspace at large. There is a tendency for stakeholders to focus on distinct groups for intervention against botnets, but a diverse array of participants, including consumer educators, need to take responsibility for doing their parts.

- **Many countries need to tackle botnets, with the U.S. in the lead.** The Report says that the majority of the compromised devices in recent botnets are located outside the U.S. Thus, increasing the resilience of the internet and communications ecosystem against these threats requires coordinated action with international partners.

  First, the Chamber agrees that the U.S. should take the lead on blunting botnets. Stakeholders, especially the U.S. government, need to put additional pressure on foreign countries that aid and abet malicious actors that leverage botnets or look the other way at such illicit activity. Pushback on foreign powers or their subordinates is the special province of governments.

  NTIA's January 11 notice asks about the utility of metrics. The Chamber holds that metrics could be used to better pinpoint the geographic origins of botnet attacks. While

attribution is a challenge, it is far from impossible.[4] Prominent cyber authorities agree that certain foreign powers or their proxies represent high-end threats against the business community and the U.S.[5] Among the goals worth pursing include reducing the number of safe havens (e.g., parts of Eastern Europe and Asia) from which bad actors launch cyberattacks against American interests with impunity.[6]

Second, the Chamber welcomes recommendations contained in the November 2017 *National Security Telecommunications Advisory Committee Report to the President on Internet and Communications Resilience* (the NSTAC report), which deserve closer attention and support. The NSTAC report says that the U.S. government has unique authorities and duties to protect citizens, enforce the law, and defend the country from external threats. Through these powers, the government can help the private sector stop or deter harmful activities (e.g., botnets).[7]

Third, U.S. officials, led by the Commerce and State departments, should facilitate collaboration on a global scale to urge allied countries to share cyber threat data and use industry-led best practices to identify and remediate botnets. These efforts, which are already underway yet limited, should be expanded and can markedly reduce the number and severity of automated attacks.[8]

- **Effective tools should be more widely employed, benefiting customers and providers.** According to the Report, several botnet-mitigation tools, processes, and practices are available and routinely applied in some market segments. However, they are not commonly used in some areas of the economy for a host of reasons (e.g., the lack of awareness, cost concerns, and insufficient technical expertise).

  First, the Chamber is a strong proponent of the Framework, which enjoys wide support among businesses.[9] It is being used by a significant number of large organizations and, increasingly, by their small and midsize business (SMB) supply chain partners. Company leaders across industry tell the Chamber that the Framework is the cornerstone for how they think about and execute their cyber policies and practices. This should come as no surprise to Report writers—no organization sets out to be less secure or resilient in its operations.

  Second, the Report points out that internet service providers (ISPs) and other infrastructure companies offer commercial botnet-mitigation services, such as ingress and egress filtering. But not all enterprise customers purchase them because of the "expense and the complexity of integrating those services into the other components of the enterprise's network." The Chamber is excited about businesses budgeting specifically for cyber products and services. Public policy, however, has not caught up to the fact that implementing a strong cybersecurity plan can be costly and difficult for organizations.

  The NSTAC report points out that filtering is one of many security techniques that network providers can implement on behalf of their customers. Where feasible, the Chamber wants to help facilitate the broader use of sound cyber practices. Such practices should not be regulated, which is contrary to good security and resource management. The Chamber's goal is for the "ubiquitous adoption of filtering"—to borrow one example

from the Report—to be economically advantageous to enterprise buyers and ISPs—a win-win relationship in other words.[10]

Third, the Chamber wants to foster constructive business-to-business relationships by knocking down barriers to their development and expansion. Policymakers should ensure that existing laws do not limit industry's information sharing or appropriate cyber defensive activities. Industry and government should look for novel ways to limit liability for private entities that employ defensive measures in good faith. The NSTAC report sheds light on barriers that can create hurdles to forward-leaning cybersecurity practices.[11] The Chamber urges policymakers to commit to taking steps with the NSTAC community to weaken obstacles to enhancing botnet-mitigation efforts.

- **Secure device makers deserve recognition and market share.** The Report recognizes that many leading technology companies employ secure development life cycles and security by design techniques (e.g., incorporating security throughout the product development phase). In addition, some companies participate in global, industry-led efforts (e.g., SAFECode) to identify and promote best practices for developing and delivering more secure and reliable software, hardware, and services.

  The Report devotes considerable space to observing that vulnerable IoT devices (e.g., they lack the means to patch vulnerabilities or remain in service after vendor support ends) can unintentionally contribute to botnet attacks. However, instead of seemingly focusing disproportionately on weak approaches to security, the Chamber wants stakeholders to spotlight businesses that are using state-of-the-art ways to build security into their products.

  There are multiple ways to better secure the internet ecosystem, including the adoption of edge systems like IoT gateways, which can help guard infrastructure through the lifetime of IoT devices. What's more, advances in hardware are making security features stronger. There's clearly a consensus that security should be integrated into both hardware and software from the outset of design and construction. Companies do not have to be forced into investing heavily in security, owing to the fact that their organizations' reputation and success depend on protecting customers and earning their trust.[12]

  The Report essentially argues that the vast majority of devices should be able to "resist attacks throughout their deployment life cycles."[13] It goes on to say that broad advances in product security call for flexible, industry-driven, and globally accepted standards and practices to be robust. The Chamber concurs with the thinking that cyber standards and best practices are optimally led by the private sector and adopted on a voluntary basis. They are most effective when developed and recognized internationally. Such an approach avoids burdening multinational enterprises and technology adopters with the requirements of numerous, and often conflicting, jurisdictions.

  The Chamber especially welcomes DOC's engagement with overseas audiences and its commitment to "advocate against attempts by governments to impose top-down, technology-specific 'solutions' to IoT standardization needs."[14]

- **More dialogue is needed concerning so-called market incentives; regulation would stunt security and innovation, including the deployment of IoT.** The Report contends that current market incentives—a mix of carrots and sticks—do not align with the goal of reducing threats emanating from botnets. The Report adds, somewhat simplistically, that market incentives motivate product developers, manufacturers, and vendors to minimize cost and time to market, rather than build in security or offer efficient security updates. There needs to be a "better balance between security and convenience" when developing products, the Report concludes.[15] Industry shares this goal of striking a better balance between security, speed, and functionality. Companies want to connect the building of stronger devices with increasing sales and profitability, which is easier said than done.

  Nevertheless, several parts of the Report call for closer scrutiny, including baseline security profiles, labeling mechanisms, transparency tools and practices, and product certification regimes.[16] The Chamber urges DOC and DHS to cultivate more discussions with industry and stakeholders to better pinpoint the practical expectations of vendors and customers. The upcoming workshop from February 28 to March 1 offers a good opportunity to exchange perspectives.

  Market forces can play a constructive role in improving device security. The Chamber is interested in establishing commercial settings where product makers and buyers voluntarily opt-in to mutually beneficial security arrangements. But policymakers and agency officials would set back U.S. and international cybersecurity efforts dramatically if they pursue the regulation of edge devices as well as infrastructure organizations and enterprise networks.

  The Chamber believes that the private sector should lead the establishment of truly voluntary assessment and labeling mechanisms for IoT products that are embedded in flexible, industry-driven standards.[17] BSA | The Software Alliance explained in detail the positives and negatives associated with labeling schemes in its July 2017 comments to the NTIA on botnets.[18] The Chamber holds that governments—whether U.S. or foreign—should not mandate the use of label/certification/ratings programs, which would impede the vigorous competition needed for enabling stronger cybersecurity.[19]

- **The Chamber is increasing awareness about botnets and related threats through its cyber education campaign.** The Report cautions that "knowledge gaps" among home and enterprise customers, product developers, manufacturers, and infrastructure operators can hamper the deployment of the tools and practices that make the internet ecosystem more resilient.

  The Chamber, its members, and government agencies (e.g., NIST, DHS, and the FBI) are allies in advancing cybersecurity awareness in the business community. NIST, in particular, is batting 100% when it comes to participating in the Chamber's national cybersecurity education campaign. Agency principals have attended all 16 of the Chamber's regional events since 2014. NIST also joined the Chamber in Brussels last December to advocate for international alignment with the Framework among government and corporate officials representing the EU, Japan, and Israel. More private organizations should support the Chamber's cyber education campaign.

The Chamber agrees with the Report's view that increased education can help SMBs identify IoT products that are designed with security in mind. Small firms would be better equipped to buy products that track closely with their unique security concerns and obligations. Ideally, business professionals would be aware of the various risks related to unsecure IoT devices and could select devices that are more secure.[20]

A key point is that sound private sector-led IoT risk management initiatives can create a virtuous cycle of security in which consumers seek out secure devices and services, and industry stakeholders prioritize security in the design, production, and improvement phases of their offerings. Different sets of flexible cybersecurity best practices would be relevant for different IoT audiences, from producers to network operators to users.

***

The Chamber appreciates the opportunity to offer its views to the NTIA on the path ahead on mitigating botnets. If you have any questions or need more information, please do not hesitate to contact me (abeauchesne@uschamber.com, 202-463-3100) or my colleague Matthew J. Eggers (meggers@uschamber.com, 202-463-5619).

Sincerely,

Ann M. Beauchesne
Senior Vice President

Matthew J. Eggers
Executive Director, Cybersecurity Policy

Endnotes

[1] Promoting Stakeholder Action Against Botnets and Other Automated Threats, *Federal Register*, January 11, 2018. www.federalregister.gov/documents/2018/01/11/2018-00322/promoting-stakeholder-action-against-botnets-and-other-automated-threats

[2] www.uschamber.com/sites/default/files/final_uscc_feedback_s1691_federal_cyber_iot_bill_nov_13_2.pdf

[3] *A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats* (the Report). Draft dated January 5, 2018, pgs. 5–6, 34. www.ntia.doc.gov/files/ntia/publications/eo_13800_botnet_report_for_public_comment.pdf

[4] www.lawfareblog.com/attribution-malicious-cyber-incidents-soup-nuts

[5] www.armed-services.senate.gov/imo/media/doc/DSB%20CD%20Report%202017-02-27-17_v18_Final-Cleared%20Security%20Review.pdf

[6] www.uschamber.com/sites/default/files/u.s._chamber_letter_nist-wh_cyber_commission_rfi_sept._9_final_v2.1.pdf

[7] *National Security Telecommunications Advisory Committee Report to the President on Internet and Communications Resilience* (the NSTAC report), November 16, 2017.

www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20ICR%20FINAL%20%2810-12-17%29%20%281%29-%20508%20compliant_0.pdf

The Chamber generally agrees with the NSTAC report's recommendations to strengthen botnet takedown efforts:

- Department of Justice (DOJ) policies should support active U.S. government intervention. DOJ may need additional resources in order to increase these efforts, which are dependent on collaboration with both the private sector and international partners.
- The national security implications of botnets justify a focus by DOJ on prevention and disruption of botnet attacks, not just prosecution.
- The budget for cybercrime at the federal level should reflect the importance of prevention and should not necessarily be tied to prosecution and convictions (pg. 34).

Also, in the 114th Congress, the Chamber supported S. 2931, the Botnet Prevention Act of 2016.
www.uschamber.com/sites/default/files/documents/files/160519_s2931_botnetpreventionact_graham_whitehouse.pdf

[8] The NSTAC report, pgs. 31–32.

[9] The Chamber supports further consideration of the Cybersecurity Framework distributed denial of service (DDoS) profile that the Coalition for Cybersecurity Policy and Law put forward in its July 27, 2017, letter to the National Telecommunications and Information Administration (NTIA) on Promoting Stakeholder Action Against Botnets and Other Automated Threats.
www.ntia.doc.gov/files/ntia/publications/coalition_for_cybersecurity_policy_law_comment_rfc_botnets.pdf

[10] The Report, pgs. 10–13.

[11] According to the NSTAC report, the Cybersecurity Information Sharing Act of 2015 (P.L. 114–113), or CISA, authorizes businesses to monitor information on an information system for cybersecurity purposes and provides liability protections for such activities and other defensive measures. Statutes like CISA allow industry to protect their networks and support government botnet takedown efforts. If more is expected from the private sector, additional protections should be considered. Enhanced cybersecurity will require mutually beneficial partnership between industry and government (pgs. 15, 34).

[12] Joint Information Technology Industry Council (ITI) and IT Alliance for Public Sector (ITAPS) letter to the NTIA on Promoting Stakeholder Action Against Botnets and Other Automated Threats (July 28, 2017), pg. 6.
www.ntia.doc.gov/files/ntia/publications/iti_response_to_ntia_rfc_re_botnets_automated_threats_final_docket_no._170602536-7536-01.pdf

[13] The Report, pgs. 16–17.

[14] NTIA's January 2017 *Green Paper: Fostering the Advancement of the Internet of Things* is a significant policy paper regarding the development of the IoT. Some parties argue that strict definitions or labels could inadvertently narrow the scope of the IoT's potential applications (pgs. 5, 13).
www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf

[15] The Report, pg. 3.

[16] The Report, see, for example, pgs. 23–27 and 34–36.

[17] See, for example, the UL Cybersecurity Assurance Program.
https://services.ul.com/service/ul-cybersecurity-assurance-program-ul-cap/?ind=Cybersecurity

[18] BSA letter to NTIA on Promoting Stakeholder Action Against Botnets and Other Automated Threats (July 28, 2017), pgs. 4–5.
www.ntia.doc.gov/files/ntia/publications/bsa_botnets_comments_072817.pdf

[19] The Chamber's Global Information Security Working Group (GISWG) pushes our organization's views to international audiences, including calling on countries and regions to align their cybersecurity governance programs with the Framework. Last summer, the GISWG and six European organizations sent a letter to the European Commission regarding "measures on cybersecurity standards, certification and labelling to make ICT-based systems, including connected objects." The industry groups argued that Europe, like the U.S., can expect to benefit from economic growth brought about by the expanding IoT as long as policymakers cultivate a digital environment that avoids misguided regulations and supports pioneering businesses.

See August 16, 2017, letter to the European Commission from the American Chamber of Commerce to the European Union (AmCham EU), the Confederation of Danish Enterprise, the Confederation of Danish Industry, the Confederation of Industry of the Czech Republic, EurElectric, the International Chamber of Commerce in Belgium, and the U.S. Chamber of Commerce.
www.uschamber.com/sites/default/files/iot.cybersecurity.coalition._ec.letter.pdf

[20] The Report, pgs. 18–19 and 35–36.