The Software Alliance

BSA

July 28, 2017

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

Dear Ms. Remaley,

RE: Promoting Stakeholder Action Against Botnets and Other Automated Threats [Docket No. 170602536–7536–01]

BSA | The Software Alliance (BSA)[1] is grateful for the opportunity to provide comments to the National Telecommunications and Information Administration (NTIA) on promoting stakeholder action against botnets and other automated threats. BSA welcomes the NTIA's multi-stakeholder process to address this complex, cross-sector challenge, as well as similar previous multi-stakeholder processes[2], and believes this broad-based, inclusive approach is most likely to be effective in forging common, actionable solutions in this arena.

BSA is the leading trade association representing the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, developing cutting-edge solutions in use across the range of information technology (IT) platforms, from enterprise cloud services to the Internet of Things (IoT). As such, BSA and its member companies have a strong interest in collaborative action against malicious cyber threats such as botnets.

I. Principles for Collaborative Action

Botnets and other automated threats pose a direct and growing challenge to nearly all aspects of IT use, from personal computing by private individuals to cloud-enabled enterprise management on a global scale by multi-national corporations. Such threats

[1] BSA's members include: Adobe, ANSYS, Apple, Autodesk, Bentley Systems, CA Technologies, CNC/Mastercam, DataStax, Docusign, IBM, Microsoft, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, Trimble Solutions Corporation, The MathWorks, Trend Micro, and Workday.

[2] See NTIA, *Multi-Stakeholder Process: Cybersecurity Vulnerabilities.* https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities.

invade privacy, undermine trust, disrupt commerce, and threaten security. These threats have existed for some time, but new technologies are exacerbating the problem by expanding the scope and ease of botnet and related attacks. For example, as IoT-enabled devices, many of which are not developed with security as a priority, increasingly connect to the internet ecosystem, they can be easily coopted into botnets without the knowledge of the devices' owners. As such technologies fuel the expansion of the botnet threat, concerted action will be necessary to keep consumers, businesses, governments, and critical infrastructure safe.

BSA believes that an approach to action against botnets and related threats should be shaped according to the following principles:

- **Embrace public-private collaboration.** Neither the government nor the private sector alone can tackle the global and multi-dimensional challenge of automated cyber threats effectively; success will depend upon true collaboration built around agile and targeted information-sharing, coordinated action, and stakeholder-informed consensus around standards for security and privacy.

- **Adopt a holistic approach.** While there is a tendency to focus on specific points of intervention – internet service providers (ISPs) or device manufacturers, for instance – an effective approach to combatting botnets and related threats calls for broadly shared responsibility throughout the internet ecosystem and must engage all stakeholders, from product development (hardware and software) to infrastructure and edge providers and ultimately individual consumers.

- **Protect user privacy.** Consumers are a powerful ally in the fight against botnets, and their trust must be maintained through approaches that conscientiously balance security and privacy.

- **Take a global view.** Just as botnets are a global problem, solutions must be developed with a global mentality, relying upon international standards, engaging international stakeholders, and ultimately driving toward international collaboration and harmonization.

- **Remain flexible, adaptable, and outcome-focused.** Both technologies and threats evolve constantly; an effective approach to combatting botnets and related threats will avoid adopting rigid regulations or specifications that cannot keep pace with this evolution. Instead, solutions should harness the innovative power of the market to drive increasing security and ensure rapid adaptation to new threats.

In putting these principles into practice, the US Government should consider: (1) working with industry to develop flexible security standards for the IoT market; (2) promoting market incentives for adoption of these flexible security standards; (3) facilitating coordinated public-private action against botnets and related threats; and (4) engaging with international partners to facilitate global action against botnets and related threats.

II. Flexible Security Standards

BSA supports voluntary consensus-based, industry-led standards setting processes to develop and refine standards relevant to enhancing security against botnets and related threats, particularly with regard to cybersecurity standards for the IoT market. BSA and its members have strongly supported this approach in relation to security critical infrastructure through the National Institute of Standards and Technology's development of the *Framework for Improving Critical Infrastructure Cybersecurity.*[3] Adapting this approach to the IoT market is particularly appropriate, given the diversity of platforms, functionalities, and industries involved in the IoT market.

A voluntary, consensus-based, industry-led standards-setting process to establish cybersecurity standards for the IoT market should focus on the following core concerns at minimum:

(1) Identity management. Standards should be informed by best practices for identity management and authentication, including by addressing the use of hard-coded and default passwords, superuser credentials, common administrator credentials, and similar vulnerabilities.

(2) Security-informed code. Standards should be informed by best practices for building security into software code development, including practices to minimize the inclusion of known and potential vulnerabilities in code.

(3) Patchability. Standards should be informed by best practices for software security updates, including ensuring that firmware or software is able to accept authentic security updates from its developers.

(4) Consumer notifications. Standards should ensure that IoT devices are capable of notifying their owners or operators of security information, such as when security issues are detected and how to apply security updates.

One important factor behind the success of the *Framework for Improving Critical Infrastructure Cybersecurity* has been its reliance upon international standards wherever possible; this approach should be repeated in any voluntary standards-setting framework for IoT cybersecurity.

As industry and the government collaborate to strengthen IoT security to prevent botnet attacks, it is important to acknowledge the critical role encryption plays in securing Internet-connected devices. Any policy that would undermine industry's ability to use encryption, such as proposals to mandate backdoor access to encrypted devices, would be tremendously damaging to efforts to combat botnets and cybersecurity threats writ large. As cybersecurity expert Bruce Schneier recently testified before Congress, "Attempts to weaken encryption will make these attacks easier and more damaging, and will harm our society far more than their benefit."[4]

[3] National Institute for Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0. https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[4] Schneier, Bruce, *Testimony Before the United States House of Representatives Committee on Energy and Commerce Subcommittee on Communications and Technology and Subcommittee on Commerce, Manufacturing, and Trade*, November 16, 2016. http://docs.house.gov/meetings/IF/IF17/20161116/105418/HHRG-114-IF17-Wstate-SchneierB-20161116.pdf.

Finally, it is worth noting that securing IoT devices is only part of the equation when it comes to battling botnets and related threats; continued attention to securing other IT platforms and networks is equally important. Just as the *Framework for Improving Critical Infrastructure Cybersecurity* might be adapted to the IoT market, it also offers a useful starting point to inform security frameworks for IT platforms and networks beyond critical infrastructure. Other concepts discussed in this comment, including market incentives for standards adoption and public-private collaborative action, also apply equally to these platforms and networks as to the IoT market.

III. Market Incentives for Standards Adoption

In relying upon a voluntary, consensus-based, industry-led standards-setting process, developing security standards is only half the battle: such an approach will not be effective unless the standards are adopted on a wide scale. Government and industry should collaborate to develop incentives for adopting such standards, and a range of proposals for incentivizing adoption of standards have been advocated.

Several proposals relate to incentivizing adoption of security standards by increasing transparency to consumers around security features in some form. The *Commission on Enhancing National Cybersecurity* proposed the development of "the equivalent of a cybersecurity 'nutritional label' for technology products and services – ideally linked to a rating system of understandable, impartial, third-party assessment that consumers will intuitively trust and understand."[5] Similarly, the European Commission is considering "a 'Trusted IoT label', aimed at consumers, giving transparent information about different levels of privacy and security, and where relevant, demonstrating compliance with the EU's Network and Information Security Directive."[6] Organizations such as the Underwriters' Laboratory[7] and ISCA Labs[8] have worked to develop IoT security certifications, awarded upon completion of third-party security testing and assessment.

These initiatives are promising, provided they are developed smartly and with the input of all impacted stakeholders. First, they must be truly market-driven, establishing cybersecurity as a market differentiator that increases competition among providers to achieve an ever-rising bar for cybersecurity. In this vein, such incentives must be developed with robust leadership by and input from industry and other stakeholders. Second, assessments and/or certifications should be flexible and outcomes oriented, allowing for different technology solutions and approaches to achieve these outcomes. Third, there must be alignment among approaches – a proliferation of differing certifications and/or labels will serve to confuse rather than inform consumers, and will fail to drive the

[5] Commission on Enhancing National Cybersecurity, *Report on Securing and Growing the Digital Economy*, December 1, 2016. https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf.

[6] European Commission, *Fact Sheet: Digital Single Market – Digitising European Industry Questions & Answers*, April 19, 2016. http://europa.eu/rapid/press-release_MEMO-16-1409_en.htm.

[7] Underwriter's Laboratory website. http://industries.ul.com/product-security-services/product-testing-and-validation.

[8] ISCA Labs website. https://www.icsalabs.com/technology-program/iot-testing.

broader industry toward higher cybersecurity standards. It is in working toward a common, aligned approach that the government can play a particularly important role. Finally, processes involving the assessment and/or certification of products must be transparent; standards, methodologies, and findings must be consistent and readily available to both product developers and consumers.

BSA believes that market-driven incentives for adopting consensus-based standards are far preferable to other alternatives. Other proposals commonly discussed as incentives to widespread adoption of standards include requiring standards adoption through regulation, shaping the market through government acquisition, and using standards adoption (potentially in conjunction with certification or labeling regimes) to shape insurance markets and legal liability.

BSA opposes the adoption of inflexible and overly burdensome regulatory models, which risk stifling innovation, failing to keep pace with the rapid evolution of technology, and failing to create true competition toward greater cybersecurity. Shaping the market through government acquisition may be worth exploring, but carries two concerns. First, efforts to leverage government acquisition in the past have often resulted in establishing regulatory frameworks that disprivilege many industry stakeholders and hinder the government from keeping up with technological innovation. Second, because of the fairly limited scale of government purchases further diffused by the diverse range of technological platforms used by the government, many unique to individual agencies or organizations, efforts to leverage government acquisition may have limited impact in shaping the market. Any efforts to leverage government acquisition to drive higher cybersecurity standards should address these concerns, avoiding increasing regulatory burdens and focusing on technologies procured on a large scale.

Finally, proposals to shape insurance markets and legal liability according to demonstrated compliance with cybersecurity standards hold promise, but must be approached with great caution. Particularly with IoT devices, the array of stakeholders involved – including device manufacturers, network operators, software developers, and security providers – is so broad and entangled as to impede accurate and fair judgments about liability and risk. More work is needed to develop frameworks for clarifying responsibilities of different stakeholders, as well as to increase and improve data contributing to a better understanding of cyber risk.

IV. Setting the Stage for Coordinated Action

In addition to promoting cybersecurity in the development of products, action is needed to identify and dismantle active automated cyber threats. BSA member companies have been global leaders in combatting botnets, playing key roles – in partnership with the US Government and other stakeholders – in taking down some of the most expansive and damaging botnets to date.[9] However, due to the global, cross-sector, and criminal nature of the threat, industry cannot act alone. Such action requires collaboration between a wide array of stakeholders, including industry, academic researchers, law enforcement agencies, and governments worldwide.

[9] *See, e.g.,* Testimony of Cheri McGuire (Symantec) and Richard Boscovich (Microsoft) before the Senate Judiciary Committee, July 15, 2014. Available at https://www.judiciary.senate.gov/imo/media/doc/07-15-14McGuireTestimony.pdf and https://www.judiciary.senate.gov/imo/media/doc/07-15-14BoscovichTestimony.pdf

The US Government can play critically important roles in facilitating and sustaining collaborative action against botnets and related threats. Such roles should include:

- *Facilitating timely, targeted information-sharing.* Robust information-sharing is a cornerstone for effective public-private collaboration against cyber threats. Yet, while current information-sharing architectures are useful, these mechanisms would benefit from continued improvement. Information shared through existing authorities must become more *timely* and *targeted* – the right information must reach the right stakeholders at the right time – to maximize impact in addressing cyber threats such as botnets.

- *Continuing broad cross-industry collaboration initiatives.* Government-facilitated initiatives to bring together broad groups of stakeholders to combat botnets and other cyber threats, such as the Communications Security, Reliability, and Interoperability Council (CSRIC) Botnet Working Group, have demonstrated their effectiveness in achieving consensus on means for collaboration, identifying voluntary best practices, and sharing lessons learned. The government should continue to facilitate such fora.

- *Using its convening power to facilitate collaboration.* Timely information-sharing and broad-cross industry collaboration are important elements of addressing the botnet challenge, but responses to specific botnet threats requires targeted, agile public-private collaboration. The government can play an important role by moving beyond broad-based collaborative initiatives to convene threat-specific targeted working groups that maximize the capabilities of the most relevant public and private sector stakeholders. While private industry stakeholders are often willing to collaborate to address prominent current cyber threats, such cooperation can be accelerated when the government is able to identify and convene relevant stakeholders, leveraging both its convening power and its intelligence-informed understanding of threats. Stakeholders relevant to addressing current threats will often change from incident to incident, so a standing, broad-based working group will be less effective than the convening of targeted, threat-specific groups to confront each specific incident.

- *Ensuring clarity on lawfulness and liability.* Finally, the government can help advance effective industry collaboration to address botnets and related threats by providing greater clarity on the legality of measures taken and potential liability associated with such measures. In particular, greater clarity is needed with regard to potential application of anti-trust laws to collaboration among industry stakeholders to combat cyber threats, liability associated with taking measures to disinfect networks of malware, and both legality and liability in relation to vulnerability research.

V. Setting the Stage for Global Action

Finally, an effective approach to combatting botnets and related threats must consider the global nature of the threats. Botnets often involve networks of infected machines located in multiple countries, with command-and-control nodes often located outside the jurisdiction of U.S. law enforcement. As a result, international collaboration must be part of the solution.

Countries with which U.S. law enforcement may seek to partner around the world must possess both the *political will* to cooperate in confronting cyber threats and the *capability* to do so. Currently, there are significant gaps in capability that must be addressed to enable more effective cross-border collaboration. For instance, the United Nations International

Telecommunications Union's *Global Cybersecurity Index 2017* found that less than 50% of countries worldwide have developed a national cybersecurity strategy, and only around 43% have any sort of cybersecurity training regime for their law enforcement communities.[10] Cybercrime often takes root in countries that lack ability and/or strategy to detect or prosecute cyber criminals. The US Government could thus improve effectiveness of international collaboration through expanding its global cyber capacity-building efforts.

Finally, both the government and industry must increase involvement in international standard-setting organizations. These organizations offer the best means to ensure a basic level of cybersecurity in products across the globe, and US government and business stakeholders have too often neglected the sort of robust, detail-oriented engagement in these bodies necessary to shape standards to address shared security concerns. Industry and government should partner to enhance participation in these organizations and to coordinate advocacy on key security concerns. Additionally, given that many private sector experts who may wish to participate in international standard-setting processes often must do so in their spare time or in volunteer capacity, the government should consider the viability of targeted grants to support standards development efforts.

VI. Conclusion

While there are no silver bullets for mitigating the threat of botnets and other automated threats, true collaboration among private industry stakeholders, and between private industry and the government, can produce meaningful improvements in security against these threats and concrete outcomes in dismantling the most damaging botnets. Several of BSA's members have played leading roles in some of the most successful public-private collaborative efforts to dismantle botnets, such as initiatives against the Gameover Zeus, Rustock, ZeroAcess, and Bamital botnets. What is notable about these efforts, as well as about efforts to drive more effective security in the design of information technology devices, is that no single organization – public or private – can succeed alone. BSA and its members are deeply committed to working with industry stakeholder across sectors, with government agencies, and with law enforcement to disrupt botnets, strengthen security against automated cyber threats, and make ensure a more trusted and secure Internet for everyone.

Thank you for the opportunity to comment on this important matter.

Sincerely,

Tommy Ross
Senior Director, Policy

[10] International Telecommunications Union, *Global Cybersecurity Index 2017*. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf.