February 12, 2018

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. 180103005–8005–01]

BSA | The Software Alliance (BSA)[1] is grateful for the opportunity to provide comments to the National Telecommunications and Information Administration (NTIA) on the draft interagency report to the President on "Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats." BSA welcomes the Administration's leadership in addressing this growing threat, as well as its broad-based, inclusive approach to 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.

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 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.

---

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

20 F Street, NW, Suite 800
Washington, DC 20001

P 202-872-5500
W bsa.org

As the draft report rightly emphasizes, "automated, distributed attacks are an ecosystem-wide challenge." A solution requires all stakeholders working collaboratively and proactively. The software industry is an important stakeholder in this effort; our members are strong advocates for strengthening security in the development and deployment of software, and welcome the opportunity to lead industry efforts to address vulnerabilities and gaps that botnets and other automated attacks seek to exploit.

BSA appreciates the report's emphasis on software security, and its far-reaching recommendations for mitigating software vulnerabilities and risks. Below, we offer a number of observations on the report, as well as several recommendations for refining the report to ensure it can most effectively drive security improvements across a complex, diverse, constantly evolving ecosystem.

I. The Importance of Integrating Security into Software Development

BSA particularly welcomes the report's emphasis on integrating security into software development processes. We agree that "security must become a primary design goal" and support recommended Action 1.2, which states that "Software development tools and processes to significantly reduce the incidence of security vulnerabilities in commercial-off-the-shelf software must be more widely adopted by industry." BSA has advocated for the broader adoption of security-focused development approaches and, more broadly, for improving IoT cybersecurity through the adoption of proven software security best practices.

BSA's members are industry leaders in the development and adoption of security-by-design principles and secure software development lifecycle processes. These approaches are essential to help organizations effectively integrate security considerations into their development lifecycles and minimize vulnerabilities in software. BSA members have also led efforts to develop internationally recognized standards, such as the ISO 27034 standard currently under development, to encourage adoption of secure software development lifecycle approaches by software developers globally.

Expanding the adoption of secure software development tools and processes will require a multi-faceted approach. Industry must lead, and BSA members are committed to continuing efforts to promote secure software development. The government also can take a number of actions to encourage progress, including by more directly addressing secure software development in core cybersecurity guidance such as NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, by considering secure software development processes in federal government procurements, by continuing to encourage the development and use of international technical standards for secure software development lifecycle approaches, and by encouraging the inclusion of secure software development concepts in computer science and cybersecurity-related education, certification, and training programs (as recommended in Action 5.3).

II. Other Observations

Beyond the report's emphasis on secure software development tools and processes, BSA commends several other aspects of the approach NTIA and other involved agencies have taken regarding software security and the broader ecosystem approach to combatting automated cybersecurity threats.

20 F Street, NW, Suite 800
Washington, DC 20001

P 202-872-5500
W bsa.org

First, BSA applauds the report's support for flexible, voluntary approaches to improving cybersecurity that are rooted in international standards. In our industry, technologies evolve constantly, and innovation is the crux of competitive success. Policies and regulations that become ossified over time, failing to account for or even stifling such innovation, can hamstring an industry that is central to the United States' unrivaled economic success. Flexible approaches can generate competition and innovation toward ever-higher security standards without stifling development of new technologies and products. Keeping such approaches rooted in international standards and efforts to promote international interoperability likewise help foster innovation, collaboration, and economic growth, while urging global industry stakeholders toward shared, meaningful standards for security. NIST's *Framework for Improving Critical Infrastructure Cybersecurity* has demonstrated the value of such approaches to cybersecurity, and should be considered a model as we seek to address IoT cybersecurity and automated threats.

BSA also commends the report for acknowledging the harms caused by use of unlicensed software. The use of unlicensed software exposes enterprises and government agencies alike to heightened risks of malware infections and other security vulnerabilities. Because unlicensed software is less likely to receive critical security updates that would otherwise mitigate the risks associated with malware exposure, its use heightens the risk of harmful cybersecurity incidents. Unfortunately, as the report notes, the use of software that is not properly licensed, including by government agencies and contractors, is still a significant problem globally. Many enterprises and government agencies do not have adequate policies for managing software licenses. Transparent and verifiable software asset management (SAM) practices identify situations where entities are using unlicensed software, as well as situations where the licenses they have far exceed the number of users. Under-licensing creates legal liability and security risks, while over licensing creates inefficiencies and unnecessary costs. Enterprise and government stakeholders should adopt SAM practices based on international standards for their own procurement and software asset management, improving cybersecurity and reducing costs by ensuring that they only use properly licensed software.

The report also usefully highlights the security benefits migration to cloud services can bring. It rightly identifies several challenges many enterprises face – including insufficient cybersecurity expertise, inadequate cybersecurity risk analysis, and difficulty working with network providers when under attack – that security-focused cloud services can help address. Given the increasing use of software solutions in industries of all types, the growing unmet demands for cybersecurity professionals, and the rising sophistication in cyber defenses and attacks, the report may benefit from expanding its analysis of the benefits of cloud services and managed security services for enterprises and small businesses. In that vein, BSA also appreciates the reports acknowledgement that cloud providers are developing unique cybersecurity solutions that can buttress device- and gateway-focused solutions, helping strengthen layered defense approaches and better secure the IoT ecosystem. When security is prioritized, cloud services can offer enterprises tremendous benefits in terms of security and efficiency, and will be a critical part of security the IoT.

20 F Street, NW, Suite 800
Washington, DC 20001

P 202-872-5500
W bsa.org

Finally, BSA agrees with the report's emphasis on educating consumers regarding cybersecurity and the cybersecurity features of consumer products. BSA has advocated for the development of tools to inform consumers of product cybersecurity characteristics, including in our comments to NTIA on Promoting Stakeholder Action Against Botnets and Other Automated Threats last year. Too often, potential consumers lack the ability to make informed decisions that differentiate between products based on security, in part because there are too few tools to enable consumers to obtain and compare critical product security information.

The draft report proposes a number of ideas for educating consumers that are worthy of further consideration: "voluntary informational tools for home IoT devices" (Action 5.1), "voluntary labeling schemes for industrial IoT applications" (Action 5.2), associated assessment and certification mechanisms for these schemes, and transparency tools to document software components (Action 1.2).

It is important to ensure such tools are developed in a way that is voluntary, industry-led, meaningful, cost-effective, and sufficiently nuanced to capture the broad array of security considerations and diversity of devices. These ideas hold promise, 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. Second, assessments and/or certifications associated with these tools 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 broader industry toward higher cybersecurity standards. Fourth, 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. Finally, these tools must be sufficiently flexible and nuanced to meaningfully capture security considerations across software products that vary dramatically according to function, intended use, risk, and sophistication. One-size-fits-all approaches are unlikely to be helpful in informing consumer decisions across the diverse spectrum of software products and IoT devices.

Specifically with regard to the report's proposed development of software transparency mechanisms, we recommend that any such effort be approached with caution. Such mechanisms should be considered, along with other potential solutions, through multi-stakeholder collaborative processes, and should avoid any approach that provides non-actionable information to customers, provides misleading information about potential vulnerabilities when software products may include successful mitigations, or treats all vulnerabilities equally, given the wide spectrum of risk associated with coding flaws. These pitfalls risk diverting resources from more pressing cybersecurity challenges, undermining the effective risk management strategies encouraged by the *Framework for Improving Critical Infrastructure Cybersecurity* and other effective cybersecurity best practices. We look forward to working with NTIA and other stakeholders to achieve the report's goals in this area while avoiding unintended consequences.

BSA is eager to partner government and industry stakeholders in developing tools to better inform consumers according to the above considerations. Ultimately, smartly designed policy tools that leverage market forces to shape consumer behavior are most likely to achieve far-reaching impact in elevating cybersecurity across the ecosystem.

20 F Street, NW, Suite 800
Washington, DC 20001

P 202-872-5500
W bsa.org

III. Recommendations

Building on the observations in the previous section, BSA offers the following recommendations for further refining the draft report as it is finalized for presentation to the President:

(1) *Address definitional challenges associated with IoT.* The report rightly identifies security in the Internet of Things as a primary focus in combating botnets and other automated threats. The Internet of Things, still new and evolving, is defined differently by different stakeholders, creating the risk of confusing or counterproductive outcomes for IoT-focused policies. The report should take account of these definitional challenges.

IoT devices and the systems they support come with a broad range of characteristics, including widely varying levels of vulnerability and risk, a diversity of technical architectures and functions, and target markets of different sizes and levels of sophistication. These differences matter greatly for approaching IoT policymaking; effective policy approaches may differ based on whether an IoT device has an operating system, how the device accesses the internet, or whether the device controls life-critical functions. Any approach to IoT policymaking that does not acknowledge and distinguish between this broad diversity of risk, functionality, and market characteristics, or that serves as the basis for one-size-fits-all approaches, will be ineffective and counterproductive. Instead, effective IoT policy requires a definitional framework that facilitates the thoughtful, tailored application of security solutions. The report should either offer a working definitional framework of the Internet of Things that can inform policy discussions moving forward or acknowledge the gap and make recommendations for addressing it.

(2) *Clarify that security baselines should be risk-informed.* Security baselines represent a promising approach to elevating IoT device security; however, as the previous recommendation suggests, such baselines should be calibrated according to the different types, functions, and risks associated with IoT devices, rather than serving as single, across-the-board standards. Action 1.1 should be modified to reflect this nuance, highlighting the need for a risk-based approach.

(3) *Address the pressing challenge of cybersecurity workforce shortfalls.* As the report rightly notes, improving security against botnets and other automated threats requires collaboration and innovation among stakeholders across the Internet ecosystem. Achieving the ambitious vision set out by the report will require that the technology industry and other stakeholders invest in dedicating additional employee resources to addressing the pressing challenges the report identifies. Yet, stakeholders already face a significant shortage of qualified, available cybersecurity and IT professionals, and that shortage is projected to grow far more acute in coming years. Beyond identifying the need for improved cybersecurity education, the report should include a significant discussion of the workforce challenges associated with securing the Internet ecosystem, and concrete recommendations for addressing these challenges. Such recommendations might include government and industry steps to expand investments in STEM education, apprenticeship programs, mid-career retraining programs, and expanding diversity in the technology workforce.

(4) *Advance concrete recommendations on addressing unlicensed software.* The report rightly emphasizes the insecurity created by large-scale use of unlicensed software; studies have shown that the presence of pirated and unlicensed software in an IT environment can

greatly increase security risks. However, it does not include recommendations for combatting the unlicensed use of software. Actions can be taken by a number of stakeholders – including both government and industry – to address these issues; the report should include specific recommendations for tackling this challenge, including the expanded adoption by enterprises of software asset management principles. Moreover, federal agencies should lead by example and require their component agencies, as well as contractors supporting these agencies, to adopt robust software asset management practices. Further guidance from the Office of Management and Budget to federal agencies on improving software asset management practices could help accelerate government leadership in this area.

(5) *Expand consideration of emerging technologies.* Finally, the report contains a few brief mentions of the potential utility of emerging technologies – Artificial Intelligence in particular – in combatting botnets. As AI and other emerging technologies take root, they will bring both greater sophistication in automated threats such as botnets and far greater power to defend networks against these threats. Key stakeholders, including the government, can play important roles in fostering the development of AI and harnessing its power to defend networks. The development and deployment of these technologies may be worth more extensive consideration in the report.

BSA commends NTIA and other agencies involved in the drafting of this report for a thoughtful, holistic examination of the botnet threat and the future of IoT security, and appreciate the commitment expressed throughout the report to work collaboratively with industry stakeholders to build a more stable, secure Internet ecosystem that is resilient in the face of threats from botnets and other automated attacks. BSA and our members are eager to work with you to advance toward that objective.

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

Sincerely,

Tommy Ross
Senior Director, Policy

20 F Street, NW, Suite 800
Washington, DC 20001

P 202-872-5500
W bsa.org