Before the
DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration
Washington, D.C.

Notice and Request for Comment	)
	)
A Report to the President on	)
Enhancing the Resilience of the	)
Internet and Communications	)
Ecosystem Against Botnets and Other	)
Automated, Distributed Threats	)
(Draft)	

COMMENTS OF CTIA

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

John A. Marinho
Vice President, Technology and Cybersecurity

Melanie K. Tiano
Director, Cybersecurity and Privacy

CTIA
1400 16th Street, NW, Suite 600
Washington, DC 20036
202-736-3200
www.ctia.org

February 12, 2018

TABLE OF CONTENTS

I. INTRODUCTION AND SUMMARY

CTIA[1] members are pleased to provide feedback on the Department of Commerce's and National Telecommunications and Information Administration's ("NTIA's") Notice and Request for Public Comment ("Request")[2] on the Department of Commerce's and Department of Homeland Security's ("DHS's") (together, "Departments'") Draft Report to the President on "Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats" ("Report").[3] The Request implements Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,"[4] and seeks feedback on the Report's "characterization of risks and the state of the ecosystem, the goals laid out, and the actions to further these goals."

Cybersecurity is a top priority for the wireless and Internet industries, which have been actively responding to botnets and other risks for years. Companies have partnered with DHS in venues like the National Cybersecurity and Communications Integration Center ("NCCIC") and U.S. Computer Emergency Readiness Team ("US-CERT") for decades. Industry has also actively engaged with NIST in developing its "Framework for Improving Critical Infrastructure

---

1 CTIA® (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st century connected life. The association's members include wireless carriers, device manufacturers, suppliers as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. The association also coordinates the industry's voluntary best practices, hosts educational events that promote the wireless industry and co-produces the industry's leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

2 *Request for Public Comment on Promoting Stakeholder Action Against Botnets and Other Automated Threats*, 83 Fed. Reg. 1342 (Jan. 11, 2008), https://www.ntia.doc.gov/files/ntia/publications/fr-botnet_report_rfc_01112018.pdf

3 The Secretary of Commerce and The Secretary of Homeland Security, *A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats*, Draft for Public Comment (Jan. 5, 2018) ("*Report*") , https://www.ntia.doc.gov/files/ntia/publications/eo_13800_botnet_report_for_public_comment.pdf

4 Exec. Order No. 13800, 82 Fed. Reg. 22391 (May 11, 2017).

for Cybersecurity" ("CFS" or "Framework").[5] Our members use sophisticated filtering and other techniques to thwart attacks, and are building new architectures and software-defined networks to support security in Fifth Generation ("5G") networks.

The Departments have a tremendous opportunity to advise the President on botnets and other automated distributed attacks. CTIA offers a number of suggestions[6] that will assist the Departments in developing a roadmap. In the Report to the President, the Departments should:

- Closely align the Report's findings with the NSTAC Report;
- Describe ongoing security efforts led by the private sector;
- Promote industry innovation and avoid suggesting mandates;
- Examine barriers like liability risks and regulatory uncertainty;
- Avoid singling out the network layer, even if unintentionally;
- Support IoT management services and other innovations; and
- Acknowledge the complexities of information sharing and coalitions.

CTIA and its members look forward to helping the Administration and the federal government address botnets and other distributed automated attacks.

II. THE DRAFT RIGHTLY FOCUSES ON INTERNATIONAL EFFORTS AND ENTERPRISE ENVIRONMENTS.

The Report analyzes the global nature of DDoS and other automated distributed attacks, noting that most compromised devices in recent botnet attacks have been located outside of the United States.[7] The Report is correct that "[n]o single stakeholder community can address the problem in isolation."[8] And the Departments should continue to emphasize international

---

5 National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 Draft 2* (Dec. 5, 2017) ("*CSF Version 1.1 Draft 2*"), https://www.nist.gov/sites/default/files/documents/2017/12/05/draft-2_framework-v1-1_without-markup.pdf

6 CTIA comments on all Goals and Actions except for Actions 3.1, 3.3, 4.2, 4.4, 5.3, and 5.4

7 *Report* at 7.

8 *Id.* at 3.

engagement and the need for harmonized and aggressive international work on these issues, with the U.S. taking the lead on pressuring countries that aid and abet malicious actors.

The Report also rightly focuses on enterprise networks, finding that "[m]any at-risk enterprises are unaware of the potential impacts of DDoS attacks on their operations," and that many enterprises may not understand their Internet service contracts or use available DDoS mitigations.[9] It calls for more widespread use of the NIST CSF, as well as for increased consumer education.[10] CTIA supports these goals and is ready to help advance them.

III. THE REPORT CAN HELP THE PRESIDENT BY CLOSELY ALIGNING WITH THE NSTAC REPORT AND FULLY DESCRIBING THE LANDSCAPE.

A. Close aligment with the NSTAC Report will help the Departments offer a comprehensive and actionable plan.

The Departments sought extensive input for this Report through its workshop, request for comment, and through the President's NSTAC.[11] The NSTAC's "Report to the President on Internet and Communications Resilience" ("NSTAC Report") contains thorough assessments and recommendations.[12] While the Departments refer to the NSTAC Report, CTIA believes that the NSTAC's expertise should be more fully incorporated into this Report to the President.

The NSTAC examined how the private sector and government can collaborate to enhance the resilience of the Internet and communications ecosystem from automated distributed attacks. The NSTAC Report was informed by nearly forty subject-matter experts from government,

---

9 *Id.* at 12.

10 *Id.* at 13.

11 *Id.* at 3.

12 National Security Telecommunications Advisory Committee (NSTAC), *Report to the President on Internet and Communications Resilience*, Draft (2017) ("*NSTAC Report*"), https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20ICR%20FINAL%20DRAFT%20-%20508%20compliant.pdf

industry, and academia.[13] NSTAC reviewed federal cybersecurity policies; research and best practices; and guidance from NIST and NTIA.[14]

Based on these inputs, NSTAC's Report to the President offers guidance for mitigating threats posed by botnets and other DDoS attacks. It provides a detailed description of the global Internet ecosystem and the threats it presents. It identifies challenges and mitigation efforts for networks, consumers/the edge/devices, enterprises, and software/applications/operating systems, and internationally. It offers actionable short- and long-term recommendations, as well as a proposed "moonshot" to examine Internet security. Finally, it identifies opportunities for government to further collaborate with industry. The NSTAC's expertise and thoughtful suggestions should be fully incorporated in this Report to the President.

B. The Report should provide additional detail on current efforts, such as network management and information sharing.

The wireless and Internet industries are leading on cybersecurity. Incentives for the communications sector to manage risk are aligned because the ecosystem wants to protect its users and prevent the enormous costs imposed by cybercrime.[15] For example, due to the Mirai botnet attack, Dyn lost an estimated 8% of its business,[16] and the impact on Mirai-affected sites is estimated to have averaged $22,000 per minute of downtime.[17] Attacks have real costs.

---

[13] *See NSTAC Report*, Exhibit A. Topics included botnet and DDoS attacks; network and web-based product development and management; internet measuring and attack modeling; distributed systems and algorithms; developments in telecommunications and IoT technologies; emerging security challenges; the NIST CSF; cyber behavior analytics; law enforcement and botnet takedowns; and cybersecurity practices abroad, among others.

[14] *Id.* at § 1.2.

[15] NIST, *Impacts: Cybersecurity* (explaining that cyberattacks cost businesses $400B per year), https://www.nist.gov/industry-impacts/cybersecurity

[16] Sam Varghese, *DDoS attack on Dyn costly for company: claim*, iTWire, (Feb. 6, 2017), https://www.itwire.com/security/76717-ddos-attack-on-dyn-costly-for-company-claim.html

[17] Ponemon Institute & Radware, *Cyber Security on the Offense: A Study of IT Security Experts*, at 1 (Nov. 2012),

Industry commitment is evident in numerous efforts and confirmed in the NSTAC Report. Industry receives and provides agency input in, for example, the FCC's Communications Security, Reliability, and Interoperability Council (CSRIC)[18] and Technological Advisory Council (TAC); works with domestic and international standards bodies; [19] and engages in myriad efforts coordinated by DHS, the sector specific agency for communication. Industry works through groups like CTIA's Cybersecurity Working Group ("CSWG")—an industry-led group created in 2012 and comprised of over 30 companies, including operators, network suppliers, device suppliers, and security companies—to address issues like automated indicator sharing, authentication, and distributed attacks. Related work abounds.[20] The Report should ensure that the President can fully consider these efforts so that they are properly leveraged in any future federal policy.

C. The Report should address barriers like liability and regulatory uncertainty.

The Report does not address barriers to implementing many of the Actions it calls for. Information sharing, certification regimes, and labeling involve some risk related to public disclosure of sensitive information, responsibility, and liability. The Report briefly notes some commenters' concerns,[21] but the Report should explicitly consider barriers.

---

https://security.radware.com/uploadedfiles/resources_and_content/attack_tools/cybersecurityontheoffense.pdf

[18] Communications Security Reliability and Interoperability Council (CSRIC) III, U.S. AntiBot Code of Conduct (ABCs) for Internet Service Providers (ISPs), Final Report, WG 7 (Mar. 2012), https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-FinalReportFinal.pdf.

[19] Examples include work with 3rd Generation Partnership Project (3GPP), Institute of Electrical and Electronics Engineers, Inc. (IEEE), oneM2M Partners (oneM2M), Alliance for Telecommunications Industry Solutions (ATIS), and GSM Association (GSMA).

[20] For example, the CSRIC Anti-Phishing Working Group focused on eliminating fraud and identity theft; the Anti-Spyware Coalition was dedicated to building a consensus on definitions and best practices around spyware; and the International Botnet Taskforce brought together public and private sector computer security specialists to share best practices, tools, and training to combat botnets.

[21] *Report* at 23.

DHS has already acknowledged these barriers and the power of incentives. In a 2016 report on "Strategic Principles for Securing the Internet of Things (IoT)," the agency recognized that "[p]olicymakers, legislators, and stakeholders need to consider ways to better incentivize efforts to enhance the security of IoT" by looking at "how tort liability, cyber insurance, legislation, regulation, voluntary certification management, standard-setting initiatives, voluntary industry-level initiatives, and other mechanisms could improve security" while encouraging economic activity and "groundbreaking innovation."[22] The Report should align with this prior work.

CTIA appreciates the Departments' recognition that the Report should not promote regulatory solutions. Assistant Secretary Redl recently affirmed this point, stating that the government "cannot solve [botnets] through government regulation."[23] However, perhaps unintentionally, certain parts suggest that regulation could be a solution.[24] In the Final Report, the Departments should consider deemphasizing the potential role of regulation.

D. The Report suggests a market failure, but it is premature to draw conclusions about IoT.

The Report is right that "[p]ersonal computers and mobile devices are more secure than in years past."[25] While the mobile phone ecosystem is quite advanced, there is more to do, particularly on edge devices that make up the diverse IoT. Instead of focusing disproportionately

---

[22] U.S. Department of Homeland Security, *Strategic Principles for Securing the Internet of Things (IoT)*, Version 1.0, at 13 (Nov. 15, 2016), https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

[23] News Release, *Washington: Remarks of Assistant Secretary Redl at State of the Net 2018* (Jan. 29, 2018), https://www.ntia.doc.gov/speechtestimony/2018/remarks-assistant-secretary-redl-state-net-2018

[24] *See, e.g.*, *Report* at Actions 2.3, 4.1, and 4.3.

[25] *Id.* at 14.

on weak security approaches, however, the Report should spotlight businesses that find new and innovative ways to build security into their products. Despite variations in the development and visibility of these devices, network operators and others are innovating to expand security in an evolving array of devices. For example, wireless industry certification regimes—which are critical for validating security functions, like over-the-air software updates and patches—help secure managed-IoT environments and set the foundation for 5G and next generation wireless services.[26] The wireless industry is evaluating options for certifying that key security capabilities are implemented in devices being attached to networks to help mitigate risks to devices, networks, and end-user applications.

It thus seems premature to state that "[p]erceived market incentives do not align with the goal of dramatically reducing threats perpetrated by automated and distributed attacks."[27] There have been some devices that lack strong security, but the Report should not generalize that "[m]arket incentives motivate product developers, manufacturers, and vendors to minimize cost and time to market, rather than to build in security or offer efficient security updates."[28] In fact, there are certainly incentives to motivate many industry players to do the right things.[29] Market incentives in the IoT and connected-device-service space are complex and changing. The Report should advise the President that manufacturers and standards bodies are addressing security, including through certification programs and new services, which should be encouraged.

---

[26] CTIA, *Protecting America's Wireless Networks* (April 2017), https://www.ctia.org/docs/default-source/default-document-library/protecting-americas-wireless-networks.pdf

[27] *Report* at 8 (internal quotation marks omitted).

[28] *Id.*

[29] *See* III(B), *supra*.

E. The Departments should specify who in government is responsible for Actions and focus on what the government can do today.

CTIA applauds the Departments for seeking guidance on steps they can take now to help mitigate threats. One such step involves accountability. The Report does not make clear who in the government is accountable for goals and identified action items.[30] To help ensure that ideas do not languish, the Departments should identify who in the government is responsible for specific Actions.

The Departments also should prioritize specific things the government can do *now*, such as implementing mobile device management in agencies and across the government, raising awareness of basic cyber hygiene, and emphasizing secure device design in appropriate procurement settings. Ample tools are available to help government IT and security officials manage risk while broader issues and incentives are addressed. The private sector uses multiple tools, including forms of two-factor authentication, device management, and encryption of appropriate data and users' communications in transit and at rest. An increased focus on employee and user behavior and training could go a long way, as we have seen dramatic changes in behavior after dedicated messaging about security. More broadly, the government can support continued private sector innovation with targeted funding and guidance on use of the NIST Framework for small businesses and technology companies. Having a practical focus on actionable federal government steps will help the President act with more immediate results.

[30] Most Actions refer to "the federal government" evaluating or implementing certain measures.

IV. THE REPORT SHOULD USE ONGOING WORK TO PROMOTE THE ADAPTABLE, SUSTAINABLE, AND SECURE MARKETPLACE ENVISIONED IN GOAL ONE.

In Goal One, the Departments aim to "[i]dentify a pathway toward an adaptable, sustainable, and secure technology marketplace," and "present a comprehensive portfolio of mutually supportive actions and options that, if implemented, would improve the resilience of the ecosystem."[31] Many tools exist and the ecosystem is quite resilient. To drive improvement, the Departments should promote existing tools and best practices across the global ecosystem. The President's emphasis on restrained and responsible regulation should inform the Report: the Departments should be mindful of the potential for duplicative efforts, as more organizations are looking to address IoT security.

A. Baseline security profiles for IoT devices, proposed in Action 1.1, should focus on government, and international efforts to promote security should involve industry.

The Report calls for the government to "augment the existing [NIST] suite of standards and practices… with baseline security profiles for IoT devices in U.S. government environments," which "can establish the practicality and efficacy of profiles and create a starting point" for future efforts.[32] Action 1.1 should clarify that the profiles are to focus on federal IoT issues and are not intended for IoT generally. Federal profiles should be risk-based and allow for flexibility based on the use case and agency mission.

Action 1.1 also calls for NIST to take a lead role coordinating federal engagement on standards and exploring a federal strategy for international standards to address automated distributed threats.[33] If NIST fills this role, it should seek the active engagement of industry

---

[31] *Report* at 23.

[32] *Id.* at 23-24.

[33] *Id.* at 25.

experts. This is particularly crucial because a federal strategy to address these threats must consider a variety of actors with different needs and interests. The Departments should also leverage the NIST CSF and explore doing the same for IoT in collaboration with industry.

B. Security in commercial-off-the-shelf software, Action 1.2, should be addressed in a non-prescriptive way.

The Report states that "NTIA should engage diverse stakeholders in examining the role of transparency tools and practices in improving manufacturers[']and purchasers[']understanding of what goes into IoT products, such as by documenting off-the-shelf software and firmware included in a product or device."[34] And it urges software developers to "begin transitioning to these tools [*e.g.*, SANS list of dangerous software errors; SWAMP] immediately."

CTIA welcomes the opportunity to work with NTIA on an effort to discuss the software ecosystem, which is highly dynamic, complex, and diverse. But, while NTIA should consider promoting the use of these tools, neither the Report nor NTIA should promote any particular software tool. Tools are constantly changing, so the Report (and any future NTIA work) should promote *processes* that can promote secure development, with a focus on flexibility.[35] Approaches to software security vary. Veracode states that "Security Development Lifecycle (SDL) is a software development security assurance process consisting of security practices grouped by six phases: training, requirements & design, construction, testing, release, and

---

[34] *Id.* at 25-26. The Report refers to a "secure update mechanism in Action 1.1," but there is no such reference in Action 1.1.

[35] For example, Carnegie Mellon University's Software Engineering Institute (SEI) promotes agile and lean principles software-reliant systems in government. *See* Carnegie Mellon University, Software Engineering Institute (last visited Jan. 23, 2018), https://www.sei.cmu.edu/process/index.cfm

response."[36] Another company's SDL has seven "focus areas."[37] Whether a future NTIA effort addresses federal government settings (as it should) or also tries to reach the private sector, it should emphasize that organizations must determine what software development processes align with their needs.

This Action also discusses transparency. It is not clear that IoT products or software inputs need to carry "assurances" for commercial buyers or government purchasers. The government should think hard about the benefits and risks of disclosures or lists of vulnerabilities. Any government effort in this direction should build on existing obligations, such as in prior National Defense Authorization Acts that addressed computer software assurance in the federal government. Governments efforts to mandate changes to software security expectations—whether through lifecycle management or requiring assurances about testing and vulnerabilities—should focus on software *developed* under a contract with the government and should not attempt to insert the government into the development of commercial software products that are simply *purchased* by the government. Increasing obligations on commercial products purchased by the government should be considered with caution.

C. Work is underway to mitigate distributed threats, as called for in Action 1.3.

The Report identifies promising strategies to prevent and mitigate distributed threats (*e.g.*, hardware roots of trust, network tools like the Manufacturer's Usage Description (MUD)),

---

[36] Veracode, *Secure Software Development Practices*, https://www.veracode.com/security/secure-development

[37] *See e.g.*, Symantec, *Symantec Software Security Process* (Oct. 26, 2016) (the focus areas are: threat modeling, security code review, security tools, vulnerability management, penetration testing, cryptography review, and third party software) https://www.symantec.com/content/dam/symantec/docs/about/symantec-software-security-process-en.pdf

but says that "commercialization and adoption… is notoriously challenging."[38] It also highlights threats like ransomware, claiming that new innovations are needed. Fortunately, industry has mitigation tools, long recognized by NIST and others.[39] The private sector is constantly working on approaches to mitigate new threats. No doubt, there can be challenges to full adoption by all actors, but the Report overstates the issue. Network operators and innovators are adopting practices suited to their needs and abilities.

D. Action 1.4, on collaboration to ensure adoption of IoT best practices, is duplicative of Action 1.3 and already underway.

The Report suggests that prior efforts to promote best practices were unsuccessful. It calls for the federal government to "engag[e] the community to review prior activities" and "identify paths for driving change in organizations."[40] The Report understates current efforts on best practices and guideline adoption. Best practices are being identified, and consensus approaches are emerging. The Report should lean more heavily on the NSTAC Report and related documents, which identify and encourage the promotion of flexible standards.[41]

Action 1.4 also focuses on transparency, stating that "NTIA should engage stakeholders from both the vendor and enterprise customer communities to promote greater awareness and use of transparency tools and practices."[42] Transparency is not necessarily the solution. Poor programming and testing are major factors behind the failure of best practices. It will be very difficult to offer the "assurances" the Report envisions, which may be less important than

---

38 *Report* at 26-27.

39 NIST has numerous publications addressing hardware roots of trust, MUD and other approaches. *See NIST Initiatives in IoT*, https://www.nist.gov/itl/applied-cybersecurity/nist-initiatives-iot

40 *Report* at 28.

41 *NSTAC Report* at Executive Summary.

42 *Report* at 28.

commitments to communicate and patch when needed. This area needs further study before the Departments recommend that the President promote transparency and security assurances.

V. GOAL TWO PUTS TOO MUCH EMPHASIS ON THE NETWORK LAYER AND SHOULD NOTE CURRENT INFRASTRUCTURE COORDINATION EFFORTS.

Goal Two is to "Promote innovation in the infrastructure for dynamic adaptation to evolving threats." The Report states that to "establish a more resilient Internet and communications ecosystem, standards and practices that deter, prevent, and/or mitigate botnets and distributed threats should be continuously implemented and upgraded in all domains in response to and anticipation of the evolving threat."[43]

CTIA supports this goal. Industry is collaborating and sharing information daily, including detection, notification, and mitigation methods. Industry is also aggressively working on automated processing and response to support collaboration, as well as mitigating bad traffic. The Report should be careful not to suggest that mandates are necessary in this area and do more to describe current network innovation for the President.

A. Collaboration called for in Action 2.1 occurs now and is expanding.

The Report states "[c]ollaboration between ISPs and their peering partners should include sharing of detection, notification, and planned or utilized mitigation methods within the network."[44] It claims that "[i]ndustry should lead efforts to expand the scope and utility of information sharing" and "work collaboratively with government to improve coordinated responses to actionable information and lead the development, refinement, and standardization of information sharing protocols."

---

[43] *Id.*

[44] *Id.*

The Report should give the President a more accurate picture. It should not suggest that sharing presently is "not comprehensive."[45] It can identify organizations, venues, and reports that lead and refine current sharing,[46] which increased after the Cybersecurity Information Sharing Act of 2015. For example, CTIA's CSWG brings together the wireless communications sector (carriers, manufacturers, and others) to engage in cross-sector collaboration.[47] Industry also participates in automated indicator sharing at DHS and has expanded its work at the NCCIC and NCC-ISAC. The Report should applaud the expansion of these existing sharing efforts.

The Report calls out peering arrangements and suggests that they can be used to change the landscape. ISPs need not be prodded to address sharing and response coordination in peering and transit agreements. Sharing occurs and continues to evolve. The government should drive participation by providing value to the private sector and helping overcome international obstacles. If it believes more sharing is needed, it should examine barriers and incentives, such as the difficulties smaller organizations have participating.

B. A cybersecurity framework profile for enterprise DDoS prevention and mitigation (Action 2.2) is promising and would need to be carefully scoped.

The Report suggests that stakeholders, in consultation with NIST, should develop a CFS Profile for enterprise DDoS prevention and mitigation.[48] The Report expects that the Profile

---

45 *Id.*

46 *See, e.g.*, National Cybersecurity and Communications Integration Center (NCCIC) ("The NCCIC serves as a central location where a diverse set of partners involved in cybersecurity and communications protection coordinate and synchronize their efforts"), https://www.us-cert.gov/nccic; The National Coordinating Center for Communications (NCC) ("The NCC-Communications ISAC facilitates the exchange of vulnerability, threat, intrusion, and anomaly information amongst government and industry telecommunications participants"), https://www.us-cert.gov/nccic/ncc-watch

47 CTIA, *Cyber Security Working Group*, https://ctia.org/about/benefits/cybersecurity-working-group

48 *Report* at 29. CSF Profiles are compilations of guidance and best practices around particular threats that follow the CSF model.

would "help enterprises identify opportunities to improve DDoS threat mitigation and aid in cybersecurity prioritization by comparing their current state with the desired target state." It suggests that the Profile should be mandated for federal agencies when complete, but does not provide much guidance on the intended audience and scoping.

CTIA supports NIST frameworks that provide guidance for risk management.[49] The Report should emphasize that, if NIST embarks on this task, it should pursue the characteristics that made the CSF a success: according to NIST Director Charles Romine, the Framework's "voluntary, risk-based prioritized, flexible, repeatable, and cost-effective approach" is critical.[50]

The Report should also clarify several aspects of the proposal. First, it is unclear how an effort on enterprise DDoS prevention and mitigation would fit with NIST's efforts, already underway, on IoT generally. NIST is engaged in other work related to IoT, including the NIST Cybersecurity for IoT Program.[51] The Report should clarify deliverables and responsibility, and explain how a new CSF Profile would fit into current NIST workflows.

---

[49] Comments of CTIA, *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 Draft 2*, at 1 (filed Jan. 19, 2018), https://www.nist.gov/sites/default/files/documents/2018/01/31/2018-01-19_-_ctia.pdf; Comments of CTIA, *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 Draft 1*, at 1 (filed Apr. 10, 2017), https://www.nist.gov/sites/default/files/documents/2017/04/21/2017-04-10_-_ctia.pdf

[50] Testimony of Charles H. Romine, Ph.D., Director, Information Technology Laboratory, NIST, before the United States House of Representatives, Committee on Science, Space, and Technology, Subcommittee on Research and Technology (Feb. 14, 2017). NIST has discussed the Framework's voluntary nature in presentations, press releases, and Q&A. *See* NIST, Press Release, *NIST Releases Update to the Cybersecurity Framework* (Jan. 10, 2017) ("This update is fully compatible with the original framework, and the framework remains voluntary and flexible to adaption."); Barrett, Matt, *A Framework for Protecting Our Critical Infrastructure* (Nov. 1, 2017), https://www.nist.gov/blogs/taking-measure/framework-protecting-our-critical-infrastructure; and NIST, Cybersecurity Framework FAQs, Framework Basics, FAQ 1 and 2 (updated Aug. 25, 2016), https://www.nist.gov/cyberframework/cybersecurity-framework-faqs-framework-basics

[51] NIST, *Cybersecurity for IoT Program*, https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program

Second, the Departments should clarify the intended audience of a profile for enterprise DDoS prevention and mitigation. A "framework" for use by the federal government will differ significantly from one for the private sector, so having "multiple levels to support industry sectors with difference resilience requirements"[52] may not be appropriate. The Report should explain to the President how a CSF Profile could complement the existing Framework.

C. Action 2.3 should focus on tools to improve federal cybersecurity so that the government can lead by example.

The Report suggests that IoT profiles created in Action 1.1 be included in federal procurement compliance guidelines.[53] It also suggests using the CSF Profile for DDoS prevention and mitigation created in Action 2.2 to implement basic DDoS prevention and mitigation measures for federal networks.

CTIA is generally wary of using procurement to try to drive global technological change given the relatively small buying power of the federal government and the danger of multiple national standards balkanizing markets.[54] Nonetheless, the federal government needs to improve its approach and should lead by example. If IoT guidelines created in Action 1.1 are focused on federal environments, it would make sense to rely on them in procurement to improve federal security. IoT profiles should be limited to government uses so that they can be actionable for procurement. The government also must abide longstanding federal procurement law and policy, including the National Technology Transfer and Advancement Act,[55] requiring the use of open standards, and foregoing U.S.-specific requirements when possible.

---

[52] *Report* at 29-30.

[53] *Id.* at 29.

[54] With over 180 countries and several distinct regions, each could take its own approach.

[55] National Technology Transfer and Advancement Act of 1995, P.L. 104-113, https://www.nist.gov/standardsgov/national-technology-transfer-and-advancement-act-1995

The Report calls for the government to consider "effective ways to mandate the use of software development tools and processes that significantly reduce the incidence of security vulnerabilities in all federal software procurements, such as through certification requirements."[56] This includes "regulations" that favor or require "commercial-off-the-shelf software developed using such processes, when available."[57] It is desirable for the federal government to consider security in procurement. But the Report should emphasize risk management and avoid mandates or one-size-fits-all solutions. The Report should not tout particular solutions because technology can rapidly become obsolete. Mandates can be blunt, overlooking risk management and discouraging flexible, use-specific solutions. Rigid procurement demands and certification requirements can disrupt the commercial-off-the-shelf acquisition regime and increase risks to contractors, such as frivolous False Claims Act suits.[58]

D. Robust industry and government collaboration on information sharing protocols, in Action 2.4, is underway.

The Report encourages collaboration to address distributed automated threats, including through the creation of information sharing protocols.[59] The Report states that "industry should lead efforts, in collaboration with the federal government and other stakeholders, to enhance information-sharing protocols to meet stakeholder needs and establish international standards to facilitate global coordination."

---

56 *Report* at 30.

57 *Id.*

58 *See, e.g.*, U.S. Chamber Institute for Legal Reform, *Lawsuit Ecosystem II*, at 48 (Dec. 2014) (noting the "explosion" in FCA claims over the past decade), http://www.instituteforlegalreform.com/uploads/sites/1/evolving.pdf; U.S. Chamber Institute for Legal Reform, *Fixing the False Claims Act: The Case for Compliance-Focused Reforms*, at 30-31 (highlighting use of the FCA in cases of minor technical violations), http://www.instituteforlegalreform.com/uploads/sites/1/Fixing_The_FCA_Pages_Web.pdf

59 *Report* at 30.

Industry is working on automated processing and response. DHS has been leading the AIS program, and industry ISACs are working on innovations. The communications sector has actively shared information for years; is working on customizing sharing protocols for its needs; and regularly shares information with government. As the NSTAC Report recognizes, network providers collaborate, "developing capabilities at the network layer leveraging big data analytics and machine learning to detect and mitigate IoT based attacks and are likely to continue to introduce new capabilities and services to help better manage IoT devices."[60] The Report should align with the NSTAC Report so that the President does not overlook ongoing innovation in sharing platforms.

E. Action 2.5 focuses on network functions but overlooks key complexities.

The Report encourages the federal government to increase efforts to mitigate bad traffic, because "[w]hile network providers cannot be expected to serve as traffic cops and identify all bad packets, both common and newer tools and practices can help filter out some types of bad traffic."[61] Industry is working on these issues, but the Report does not convey enough of that to the President. The NSTAC Report notes that "ISPs and network operators invest heavily in capabilities to manage traffic," including "port blocking, machine learning and AI to help detect bots, destination black hole filtering and sinkholing of malicious IP addresses."[62] The Report should provide the President with a more accurate picture of what the ecosystem is doing.

This section of the Report also does not address the complexities of network filtering and scanning, including the effects of increased encryption use. Like the NSTAC Report, the Report

---

60 *NSTAC Report* at § 3.0.

61 *Report* at 30.

62 *NSTAC Report* at § 3.1.

should focus on challenges and complexities that ISPs face, including that ISPs are unlikely to have the broad payload visibility that may be required for aggressive blocking.[63]

VI. GOAL THREE SHOULD FOCUS ON IOT MANAGEMENT INNOVATIONS AND RECOGNIZE THE LIMITATIONS OF IPV6.[64]

Goal Three seeks to "[p]romote innovation at the edge of the network to prevent, detect, and mitigate bad behavior."[65] The Report calls for "increased detection and mitigation of compromised devices in home or enterprise networks, and where those networks connect to the internet." CTIA agrees that the edge of the network is key. The Report should acknowledge the complexities that edge providers face, the potential that emerging solutions will assist management of security challenges, and the limitations of some proposed solutions.

A. The Report should tout emerging managed services for home and small businesses, discussed in Action 3.2.

The Report states that "[r]ather than expect homeowners to become security experts, the IT and IoT industries should prioritize simple and straightforward deployment and configuration processes for devices marketed to home and small businesses."[66] Basic consumer cyber hygiene is important, and consumers will benefit from ongoing refinement in product configuration and management tools. Industry continues to work on emerging managed home IoT. Companies are experimenting with management platforms that may overtake much individual consumer control.[67] The NSTAC Report emphasizes that "[t]he government should support industry

---

63 *Id.*

64 CTIA does not comment on Actions 3.1 or 3.3.

65 *Report* at 31.

66 *Id.*

67 Google, Amazon, IBM, Verizon and AT&T are among many offering IoT management platforms. *See* https://cloud.google.com/solutions/iot/; https://cloud.google.com/solutions/iot/; https://aws.amazon.com/iot/ http://www.verizonenterprise.com/products/internet-of-things/; https://www.ibm.com/internet-of-things/spotlight/watson-iot-platform; https://www.business.att.com/solutions/Portfolio/internet-of-

investment in home management services, which would oversee operations of connected devices within the home" and "could be offered in routers or as a separate device within the home."[68] The Report should emphasize these and other solutions.

B. IPv6 offers benefits but Action 3.4 needs refinement to align with the NSTAC Report.

The Report expects that "as we transition to IPv6, consumer ISPs may be better positioned to observe device-specific misbehavior when IPv6 addresses are not subjected to NAT. This information can, in turn, map to other edge-focused solutions."[69] But IPv6 is not a panacea. People are unlikely to immediately update their networks upon IPv6 availability, and thus it is not a solution to the problem. Even as U.S. operators transition to IPv6, global partners may lag. And, because IPv6 may raise its own security challenges, we need to move in a coordinated way.[70] As the NSTAC Report recognizes:

> Operators running IPv6-enabled networks require tools for security, detection, and monitoring. Due to the unique security challenges that IPv6 introduces, the ecosystem must mature security support for IPv6, improve asset discovery and detection tools to identify rogue IPv6 devices, and ensure network monitoring supports both IP Version 4 and IPv6 network assets.[71]

The Report should more closely align with the NSTAC Report and consider complexities beyond the network layer to ensure that it does not create unreasonable expectations.

---

things/?WT.srch=1&source=ECPS0000000PSM00P&wtpdsrchprg=AT%26T%20ABS&wtpdsrchgp=ABS_SEARCH&wtPaidSearchTerm=iot&wtpdsrchpcmt=iot&kid=kwd-391320683&cid=783759108&schParam=1622&LNS=PS_IT_IOT_UNB_1117. Innovations like BitDefender specifically target home settings. https://www.bitdefender.com/box/

68 *NSTAC Report* at § 3.2.

69 *Report* at 32.

70 *See* Comments of CTIA, *In the Matter of Promoting Stakeholder Action Against Botnets and Other Automated Threats*, at 9-10 (filed Jul. 28, 2017), https://www.ntia.doc.gov/files/ntia/publications/ctia_botnet_comments.pdf

71 *NSTAC Report* at § 3.1.

VII. THE COMPLEXITIES OF INDUSTRY-GOVERNMENT COALITIONS SHOULD BE FULLY ADDRESSED IN GOAL FOUR.[72]

A. CTIA supports collaboration with law enforcement as appropriate on efforts like botnet takedowns, but Action 4.1 should recognize the challenges in working with government.

The Report calls for "[l]aw enforcement [to] proactively lay out what kinds of data will help them investigate and prosecute bad actors, and work with infrastructure providers to make it cheaper and easier to share this information while protecting user privacy."[73] It also calls on "ISPs and larger enterprises" to increase information sharing.

The Report should encourage sharing beyond the ISP level and suggest steps that will make cooperation with the government easier and less risky. The NSTAC Report focuses on broad, ecosystem-wide sharing[74] and increased resources, effort, and work by federal law enforcement to promote coordination.[75] It also recognizes that cooperation can subject companies to scrutiny and push the bounds of permissible network activity. That is why the NSTAC explicitly calls for a policy framework for increased collaboration between government and ISPs. This Report is silent on these aspects of the challenge and should emphasize NSTAC recommendations that can be acted on now, including those related to DOJ resources and incentives.[76] It could also refer to models of cooperation in other countries, such as the United Kingdom, in which government offers value to industry and protects shared information.[77]

---

[72] CTIA does not comment on Actions 4.2 or 4.4.

[73] *Report* at 33.

[74] *NSTAC Report* at § 3.1.

[75] *Id.* at § 2.3.

[76] *Report* at 33.

[77] The United Kingdom's Cyber Security Information Sharing Partnership (CiSP) offers a model of how to engage industry. The benefits of joining CiSP include obtaining early warning of cyber threats; learning from the experiences, mistakes, and successes of other users without fear of exposing

The Report offers the President a view on the government's approach to companies victimized by cybercrime: "law enforcement treats companies that have suffered an intrusion or distributed attack as victims of a crime, and conducts their investigations of such reported crimes with discretion to avoid the unwarranted release of information concerning the incident, whenever possible."[78] To help the President understand the challenges companies face, it would be helpful if the Report acknowledged that companies experiencing an attack or vulnerability often face more risk than "the unwarranted release of information concerning the incident."[79] They face litigation complexities, regulatory oversight, Congressional scrutiny, and other collateral consequences that harm reputation and consume resources. The President may want to consider more protections for companies and encourage federal agencies and others to refrain from revictimizing companies that suffer an attack or an unexpected vulnerability.

In a similar vein, the Departments should candidly advise the President on the impact of global privacy and security approaches on sharing and collaboration. The Report calls for governments to "work with private-sector entities responsible for compliance with data privacy protection regulations, as well as those entities involved in botnet investigatory work, to ensure that both equities are preserved (compliance and botnet investigations)."[80] This is not enough. Global privacy and security regimes may impede information sharing and the cooperation needed to engage in botnet mitigation. Commentators have observed that "[m]any factors can affect an organization's legal ability to engage in global business-to-business sharing of cyber

---

organizational sensitivities; and additional services and tools. *See* National Cyber Security Centre, Cyber Security Information Sharing Partnership (CiSP), https://www.ncsc.gov.uk/cisp

78 *Report* at 33.

79 *Id.*

80 *Id.*

threat information," including "whether IP addresses can be lawfully shared between organizations as cyber threat intelligence."[81] The Report should highlight the need for clear rules about sharing data between the private sector and U.S. and foreign government entities that do not run afoul of EU and other privacy laws.

B. In Action 4.3 the Report appears to open the door to regulation and sector-specific security requirements, creating uncertainty.

The Report discusses actions that sector-specific regulatory agencies can take to "promote ecosystem resilience."[82] It touts Federal Trade Commission ("FTC") enforcement and its unfairness authority under Section 5 of the FTC Act, and suggests that there should be a reexamination of agency efforts, including possible increased regulation or information collection. But the regulation of cybersecurity—whether network or device side—is likely to be counterproductive. Because of its dynamic nature, cybersecurity simply does not lend itself to regulation as an effective model. The Departments should avoid fostering regulatory uncertainty, which will chill collaboration and increase risk.

C. The Report should emphasize voluntary, risk-based collaboration with the operational technology community in Action 4.5.

The Report states that "[t]he incorporation of networking functionality into operational technology has introduced new cybersecurity challenges that can be addressed only through the combined expertise of the cybersecurity and operational technology (OT) communities."[83] To facilitate cooperation, the Report suggests that the government expand "current engagements that

---

81 Tom Spring, *New EU Privacy Laws Will Complicate B2B Data Sharing*, Threat Post (June 26, 2017) (quoting Clare Sullivan, Georgetown University Law Center Professor and Fellow at the Center on National Security and the Law), https://threatpost.com/new-eu-privacy-laws-will-complicate-b2b-data-sharing/126518/

82 *Report* at 34.

83 *Id.* at 35.

bring the cybersecurity and OT communities together to share knowledge and expertise and that promote awareness and accelerate technology transfer from the cybersecurity community." CTIA agrees that collaboration is appropriate, as long as it is on a voluntary, risk-based basis. Like other ecosystems, there is a vast range of appropriate security controls and measures within the OT environment. The suitability of a particular control or measure depends on the nature and sensitivities of the operations. By emphasizing voluntary, risk-based collaboration, the Report would promote flexibility and allow for targeted collaborations that address individualized risks.

VIII. AWARENESS, EDUCATION SOLUTIONS, AND PRIVATE INNOVATION SHOULD BE EXPANDED IN GOAL FIVE.[84]

Goal Five claims that to "enhance the resilience of the Internet and communications ecosystem against distributed threats, all stakeholders must recognize and be prepared to execute their roles and responsibilities."[85] Many of the identified Actions promote certifications, disclosures, or labeling. While there is promising work in the private sector on voluntary certifications, it is premature to begin selecting or preferring an approach. CTIA expects the emergence of certifications that are business-to-business, business-to-consumer, and suitable for home use. The Report should acknowledge this coming diversity and ensure that nothing the government does stymies innovations in certifications.

A. Action 5.1 should recognize complexities of consumer disclosures and informational tools for home IoT devices.

The Report finds that "[i]n an ideal world, consumers would prefer IoT products that also protect their security and privacy, but security-conscious consumers cannot easily identify IoT products that were designed to be secure."[86] It envisions the use of "consumer-oriented testing

---

[84] CTIA does not offer comment on Actions 5.3 or 5.4.

[85] *Report* at 35.

[86] *Id.*

organizations" as part of its goal that the private sector "devise an efficient and effective assessment and labeling approach for IoT devices."

This focuses too much on consumer disclosures, the merits of which remain uncertain. Consumer disclosures can be complex, and conveying nuance is difficult. Too many or complex disclosures result in notice fatigue.[87] The Report should take a cautious approach and not overemphasize their perceived benefits. The Report also does not seem to leave room for the development of managed home services. As previously noted, it should more closely align with the NSTAC Report's recommendation to "promote home management services."[88]

B. The Departments should not promote "labeling schemes for industrial IoT applications" in Action 5.2 because innovation will shape certifications and disclosures.

The Report claims that critical infrastructure and industrial IoT deployment environments present "significantly higher risks to the nation than home applications."[89] It states that "[t]he private sector should establish an efficient but robust evaluation process to ensure that IoT devices for these sectors offer enhanced resilience at an appropriate level of assurance."

The Report's emphasis on industrial labeling is misguided. It is not clear that industrial IoT needs "labeling" at all. Rather, the industry will continue to see certifications and other assurance mechanisms develop for products, services, and enterprise information-system security personnel. Indeed, they have already begun to emerge. For example, Underwriters Laboratories

---

87 Prepared Statement of the FTC, Hearing on Discussion Draft of H.R.__, Data Security and Breach Notification Act of 2015 Before the Subcomm. on Commerce, Manufacturing, & Trade of the H. Comm. on Energy & Commerce, 114th Cong. (Mar. 18, 2015) ("[A]ny trigger for providing notification should be sufficiently balanced so that consumers can take steps to protect themselves when their data is at risk, while avoiding over-notification, which may confuse consumers or cause them to ignore the notices they receive."), https://www.ftc.gov/system/files/documents/public_statements/630961/150318datasecurity.pdf

88 *NSTAC Report* at § 3.2.

89 *Report* at 36.

(UL) has developed the Cybersecurity Assurance Program (CAP) to certify IoT products.[90] Other programs include the DOD-approved Global Industrial Cyber Security Professional (GICSP),[91] as well as Praetorian, which offers "end-to-end [IoT] penetration testing and security assessment services."[92] The Report should recognize these efforts and promote solutions that allow the private sector to innovate, foster competition, and enable stronger security.

C. The Departments should expand on Action 5.5's call for a public awareness campaign, but not focus on "home IoT" branding.

Action 5.5 states that the "government should increase its strategic engagement and convening power with targeted user communities and civil society to improve security adoption and awareness."[93] Such a discussion should be far broader than disclosures about home IoT or particular approaches, and the government should do more than simply raise public awareness. The U.S. Chamber of Commerce,[94] NSTAC, and others have called for broad-based security awareness campaigns.[95] These campaigns could build on Stop.Think.Connect., but should do more to focus on individual and enterprise users' responsibilities and available security options.

---

90 Rob Enderle, *New IoT security certification aims to make the world safer*, CIO (May 20, 2016), https://www.cio.com/article/3073263/security/new-iot-security-certification-aims-to-make-the-world-safer.html

91 GIAC, *Global Industrial Cyber Security Professional (GICSP)*, https://www.giac.org/certification/global-industrial-cyber-security-professional-gicsp

92 Praetorian, *Gain confidence that your Internet of Things devices and data are secure*, https://www3.praetorian.com/internet-of-things-security-1030?creative=229660642207&keyword=%2Biot%20%2Bsecurity&matchtype=b&network=g&device=c&gclid=EAIaIQobChMI0d7e3Pnc2AIVmYizCh13yg7OEAAYAiAAEgJL0PD_BwE

93 *Report* at 38.

94 *See* U.S. Chamber of Commerce & Wiley Rein LLP, *The IoT Revolution and Our Digital Security: Principles for IoT Security* (Sept. 2017), https://www.wileyrein.com/assets/htmldocuments/FINAL%20REPORT%20-%20The.IoT.Revolution..Our.Digital.Security.Final%20002.pdf

95 *See* Comments of CTIA, *Security and Privacy Controls for Federal Information Systems and Organizations*, DRAFT NIST SP 800-53 (filed Sept. 12, 2017).

Again, the NSTAC Report is instructive. It states that "[t]he Nation needs an informed digital citizenry. Individuals and enterprises must understand how their decisions impact networks, systems, and each other."[96] It further claims that this effort should amplify "[b]est practices to mitigate attacks [with a] focus on user and enterprise education about networking hygiene and vulnerability management. This includes strong authentication, turning off unwanted features, and updating services."[97] The NSTAC Report cites the UK as an example of education collaboration, noting that "[t]he U.K. Government has launched a variety of public awareness campaigns aimed at educating the public about safer practices. It collaborated with large device manufacturers for two-factor authentication accounts… the government also uses its websites to remind users to upgrade their software."[98] Other efforts across Europe have also focused on end-user education for both individual and enterprise users.[99]

To encourage broad adoption, government efforts need to be streamlined. The NSTAC Report notes that "[t]he government has resources in place to educate consumers [but] the

---

96 *NSTAC Report* at Executive Summary, Key Lessons Learned.

97 *Id.* at § 2.2. *See also* Wiley Rein and Chamber White Paper The IoT Revolution, at 28 (citing consumer education and enterprise user education as vital), https://www.wileyrein.com/assets/htmldocuments/FINAL%20REPORT%20-%20The.IoT.Revolution..Our.Digital.Security.Final%20002.pdf; FCC. CSRIC II, Working Group 2A: Final Report. Cyber Security Best Practices, at 91 (Mar. 2011) ("The FCC CSRIC recommendations emphasized the importance of educating end-users on protective measures, such as strong passwords, anti-virus software, firewalls, and accepting updates."), https://transition.fcc.gov/pshs/docs/csric/WG2A-Cyber-Security-Best-Practices-Final-Report.pdf

98 *NSTAC Report* at § 3.6.

99 *See, e.g.*, European Cyber Security Month, *What is ECSM?* available at: https://cybersecuritymonth.eu/about-ecsm/whats-ecsm (ENISA, the European Commission DG CONNECT, and partners are deploying Europeans Cyber Security Month every October.) (*See* page 29); *See also* Raj Samani. McAfee, UK. Briefing to the NSTAC ICR Subcommittee. August 15, 2017. (The NSTAC Report cites the EU "No More Ransom" project, a collaboration between the European Cybercrime Center, Dutch police, and commercial companies including Amazon Web Services).

messages may be lost in the sheer number of tip pages, FBI advisories, and other communications that exist."[100] The Report should echo this emphasis on efficiency.

IX. CONCLUSION

CTIA and its members support the Departments' work to develop the Report. This is an important topic on which the federal government can do much good. We encourage the Departments to advise the President that extensive work on botnets and automated distributed attacks is underway. By encouraging international cooperation, painting a complete picture of the DDoS landscape, and closely aligning with the NSTAC Report, this Report can be a valuable tool to help the President lead the digital future.

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

John A. Marinho
Vice President, Technology and Cybersecurity

Melanie K. Tiano
Director, Cybersecurity and Privacy

CTIA
1400 16th Street, NW, Suite 600
Washington, DC 20036
202-736-3200
www.ctia.org

[100] *NSTAC Report* at § 3.2.