Before the
National Telecommunications and Information Administration
DEPARTMENT OF COMMERCE
Washington, D.C. 20230

In the Matter of	)	
	)	
Stakeholder Engagement on Cybersecurity	)	Docket No. 150312253-5253-01
In the Digital Ecosystem	)	

COMMENTS OF THE NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION

The National Cable & Telecommunications Association ("NCTA")[1] hereby submits its comments in response to the Request for Public Comment ("RFC")[2] issued by the Department of Commerce Internet Policy Task Force (IPTF) on substantive cybersecurity issues in the digital economy that may be addressed through broad, consensus-driven multistakeholder processes. The IPTF plans to focus the multistakeholder effort on "discrete security challenges in the digital ecosystem where collaborative voluntary action between diverse actors can substantially improve security for everyone."[3] Potential outcomes could include "voluntary policy guidelines, procedures, or best practices."[4]

The IPTF sets forth a variety of important cybersecurity issues affecting companies across the Internet ecosystem covering the areas of network and infrastructure security, web security, and business processes and investment. It asks respondents to identify "security challenges [that] could be best addressed by bringing together the relevant participants in an

---

1 NCTA is the principal trade association for the U.S. cable industry, representing cable operators serving more than 80 percent of the nation's cable television households and more than 200 cable program networks. The cable industry is the nation's largest provider of broadband service after investing over $230 billion since 1996 to build two-way interactive networks with fiber optic technology. Cable companies also provide state-of-the-art competitive voice service to more than 28 million customers.

2 *See In re Stakeholder Engagement on Cybersecurity in the Digital Ecosystem,* Request for Public Comment, 80 Fed. Reg. 14360 (Mar. 19, 2015) ("RFC").

3 *Id.* at 14361.

4 *Id.*

open, neutral forum."[5] NCTA's member companies support broader engagement from a cross-section of entities that operate on the Internet toward the goal of strengthening cybersecurity in the digital economy. Such collective efforts can take advantage of a broad spectrum of experts spanning multiple sectors in the development of principles, guidelines and best practices. And in light of ongoing work in this field, we are pleased that the IPTF envisions processes that "complement, rather than duplicate existing initiatives, both inside and outside the government."[6] We also appreciate IPTF's continued recognition that "the pace of innovation in the highly dynamic digital ecosystem makes traditional regulation and compliance difficult and inefficient."[7]

Cable operators have engaged extensively in public-private partnerships with federal agencies to identify and mitigate cybersecurity threats and vulnerabilities, notably through the Communications Sector Coordinating Council ("CSCC") (under the auspices of the Department of Homeland Security), the Communications Security Reliability and Interoperability Council ("CSRIC") (an advisory committee of the Federal Communications Commission)[8] and the National Institute of Standards and Technology (NIST) Cybersecurity Framework multistakeholder process pursuant to the President's Executive Order on Improving Critical Infrastructure Cybersecurity.[9] In particular, the NIST Cybersecurity Framework sets forth a voluntary, business-driven set of industry standards and best practices to help organizations

---

5 RFC at 14361.

6 *Id.*

7 *Id*. at 14360, citing U.S. Department of Commerce, Internet Policy Task Force, Cybersecurity, Innovation, and the Internet Economy (June 2011) ("Green Paper").

8 *See Communications Security, Reliability and Interoperability Council IV*, at https://www.fcc.gov/encyclopedia/communications-security-reliability-and-interoperability-council-iv (last visited May 22, 2015) (describing the members, charter, and working groups of CSRIC IV).

8 *See* Executive Order 13636 – Improving Critical Infrastructure Cybersecurity, rel. Feb. 12, 2013 ("Executive Order").

manage cyber risks. Following this multi-sector effort, the communications sector developed a ground-breaking report on Cybersecurity Risk Management and Best Practices under the auspices of CSRIC that builds on the NIST framework.[10]

NCTA member companies are also actively engaged in various private sector forums and initiatives addressing cybersecurity, including the Internet Engineering Task Force ("IETF") and the Messaging Malware Mobile Anti-Abuse Working Group ("M^{3}AAWG").[11] The collaborative multistakeholder approach embraced by the communications and information technology industries in these and other organizations has led to the development of a wide variety of best practices that cable companies have been able to adapt and implement while maintaining the flexibility to innovate based on their individual profile.

In its role as convener, the IPTF can build on these efforts by choosing topics that cut across the sectors that comprise the Internet and by promoting innovation, experimentation, and collaboration in a complex, inter-connected digital ecosystem. Successful efforts to prevent or limit the impact of many of the major cyber attacks requires the participation of all participants in an inter-dependent Internet ecosystem – Internet Service Providers (ISPs), operating system

---

[10] *Cybersecurity Risk Management and Best Practices: Working Group 4: Final Report* (Mar. 2015), available at https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf. ("CSRIC IV Working Group 4 Report").

[11] These organizations have worked on botnet remediation, domain name security and Internet routing protection, as part of their broader cybersecurity activities. IETF, for example, produced a memorandum addressing bot remediation issues for ISPs. *See* Jason Livingood, Nirmal Mody, and Michael O'Reirdan, *Recommendations for the Remediation of Bots in ISP Networks*, (Oct. 26, 2011), *available at* http://tools.ietf.org/html/draft-oreirdan-mody-bot-remediation-18. M^{3}AAWG has been particularly active in developing voluntary practices that could serve as a framework for botnet remediation, drawing from technical experts, researchers, and policy specialists from a broad base of ISPs, software companies, network equipment vendors and other key technology providers, academia and organizations. *See, e.g.* Nirmal Mody, Michael O'Reirdan, Sam Masiello, and Jason Zebek, *Common Best Practices for Mitigating Large Scale Bot Infections in Residential Networks*, Messaging Malware Mobile Anti-Abuse Working Group (July 2009) ("*Best Practices Report*"), *available at* http://www.maawg.org/system/files/news/MAAWG_Bot_Mitigation_BP_2009-07.pdf; M^{3}AAWG Comments on "Cybersecurity, Innovation and the Internet Economy June 2011," (July 2011), *available at* http://www.maawg.org/sites/maawg/files/news/MAAWG_DoC_Internet_Task_Force-2011-08.pdf. *See also* M^{3}AAWG, *MAAWG Published Documents, at* http://www.maawg.org/published-documents (last visited Sept. 26, 2014).

vendors, security companies, website operators, e-commerce platforms, application and service providers and device manufacturers. The recent CSRIC IV, Working Group 4 initiative on cybersecurity risk management specifically addressed the broader Internet ecosystem, finding that "cyber attacks have been observed and mapped to every layer of the Transmission Control Protocol/Internet Protocol (TCP/IP) communication model" and against every category of identified participants in the ecosystem.[12] This work demonstrates that reducing cybersecurity risks calls for the involvement of the multiple categories of ecosystem participants.

With that background in mind, NCTA's member companies have identified three topics that would benefit from broader engagement from stakeholders: botnet/malware mitigation, securing the Internet of Things, and improving web security.

1. Botnet and Malware Mitigation:

ISPs have long worked together to mitigate the impact of malware and botnets on the Internet ecosystem. Through the FCC's CSRIC III Working Group 7, cable ISPs helped develop and implement the Anti-Bot Code of Conduct, a voluntary, industry-driven effort to reduce malware activity.[13] The Anti-Bot Code of Conduct calls on ISPs to take action in five areas: education, detection, notification, remediation, and collaboration.[14] As NCTA has discussed previously, cable operators have taken steps in all five areas: educating customers through support resources, detecting malware via DNS monitoring, notifying users via email, and providing tools for remediation.[15] However, broad cooperation and participation across the

---

[12] CSRIC IV Working Group 4 Report at 26; *see also* Cyber Ecosystem and Dependencies subgroup report at 321.

[13] *See* CSRIC III Working Group 7 Final Report, *U.S. Anti-Bot Code of Conduct for Internet Service Providers (ISPs), available at* http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-ReportFinal.pdf.

[14] *Id.* at 14.

Internet ecosystem remains the cornerstone to achieve a significantly higher level of malware mitigation.

Even the most successful remediation efforts show the need for intense collaboration among Internet stakeholders. In 2011, the FBI seized the command and control servers of a class of malware called DNS Changer infecting nearly 500,000 computers in the U.S. ISPs worked hard to notify their infected customers via emails, phone calls, in browser notifications and DNS redirects.[16] Despite knowing the IP addresses of infected devices and extensive outreach by cable operators and law enforcement, over 70,000 devices remained infected a year later. Contacting customers with infected devices and encouraging them to install anti-malware software remains very difficult.[17] Customers often ignore malware notifications or fail to correctly install the remediation tools.[18]

Programming networks also have a strong interest in this issue. These companies often host websites and microsites tied to programming that permit users to post content, making it critical to protect websites that host user-generated content from cross-site scripting or malware vulnerabilities.

While botnets and malware remediation have long been addressed through M[3]AAWG and other private sector groups, the FCC's CSRIC process provided an opportunity to solidify an

---

[15] NCTA Comments at 7-18 (Sept. 26, 2014) filed in response to *FCC's Public Safety and Homeland Security Bureau Requests Comment on Implementation of CSRIC III Cybersecurity Best Practices*, Public Notice, DA 14-1066, (July 25, 2014).

[16] *See DNS Changer Working Group: About*, at http://www.dcwg.org/aboutcontact/ (last visited May 22, 2015) (listing AT&T, CenturyLink, Comcast, Cox, Time Warner Cable, and Verizon as ISPs explicitly working with the DNS Changer Working Group on cleaning up DNS Changer. Other ISPs undertook independent measures to combat the botnet.).

[17] *See* Wei Meng, Ruian Duan, Wenke Lee, *DNS Changer Remediation Study*, M[3]AAWG at 68, (noting that telephone calls to customers are the most effective method of notifying them of a malware infection), *available at* https://www.maawg.org/sites/maawg/files/news/GeorgiaTech_DNSChanger_Study-2013-02-19.pdf.

[18] *See id.* at 59.

anti-botnet code of conduct for communications network operators. But this was a more sector-specific forum.[19] An IPTF botnet and malware multistakeholder process could bring hosting providers, software vendors, network operators and others to the table in an open, voluntary, and transparent forum to discuss techniques to improve customer malware notifications and other measures for remediation. By facilitating a forum for new perspectives and cooperation among the spectrum of Internet participants, IPTF could help industry find greater success in tackling a growing and increasingly sophisticated cybersecurity challenge.

2. Securing the Internet of Things

NCTA members are at the forefront of developing new products to leverage ubiquitous computing and low power sensors. Many cable operators offer Internet-powered security and home monitoring systems to their customers.[20] The "Internet of Things" promises to add millions of devices to the Internet, from connected thermostats and fitness devices to Wi-Fi enabled light-bulbs.[21] However, the immense benefits of Internet-connected devices could easily be undermined by security concerns.

Unlike desktops and mobile devices, individual Internet connected devices may have no screen or user interface at all and remain untouched by the consumer for months if not years at a time. Despite the lack of consumer interaction, these devices often run complex operating systems and rely upon Internet connectivity to function, thus facing the same threats and

---

[19] *See generally* CSRIC III Working Group 7 Final Report, *U.S. Anti-Bot Code of Conduct for Internet Service Providers (ISPs), available at* http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-ReportFinal.pdf.

[20] *See, e.g.* Comcast, *Xfinity Home*, at http://www.xfinity.com/home-security; Cox, *Cox Homelife*, at http://www.cox.com/residential/homelife.cox; Time Warner Cable, *Time Warner Cable IntelligentHome Gears Up for "Internet of Things" with Smart Door Locks and Smart Lighting Available at BestBuy.com*, at http://www.timewarnercable.com/en/about-us/press/twc-ih-gears-up-for-internet-of-things.html;

[21] *Internet of Things will Deliver $1.9 Trillion Boost To Supply Chain and Logistics Operations*, Cisco.com, Apr. 15, 2015, at http://newsroom.cisco.com/release/1621819/Internet-Of-Things-Will-Deliver-1-9-Trillion-Boost-To-Supply-Chain-And-Logistics-Operations (last visited May 22, 2015) (estimating that more than 50 billion devices will be connected to the Internet by 2020 compared to 15 billion today).

vulnerabilities of larger devices.[22] Preventing malware authors from infecting these devices and using them as a launching point is key to avoiding persistent threats like DNS amplification attacks. Despite years of work, over 28 million open DNS resolvers remain unsecured, amplifying DDoS attacks launched from hijacked devices.[23] Without proper security techniques and continued software updates, connected light-bulbs, toaster ovens, and other IoT devices could become the next persistent launching point for DDoS attacks.[24]

To secure these devices, a much more proactive approach is needed. As millions of new devices are purchased by consumers and attached to the network, ISPs will not be able to handle this problem alone. Even if malware activity is discovered by an ISP, asking a customer to install an anti-malware tool years on their Internet-connected lightbulb years after purchase is simply not an option. Security must be incorporated into these devices by design and as vulnerabilities are discovered, they must be resolved, regardless of how long the device has been in field. Working together, device manufacturers, software developers, edge providers, and Internet service providers should ensure that these new devices do not become a host for malware and a launching point for DDoS attacks. While NCTA is aware that NIST is in the process of developing a framework for cyber-physical systems, the Internet of Things is only one

---

[22] *See Internet of Things: Privacy & Security in a Connected World: FTC Staff Report*, at 10, *available at* https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf (Jan. 2015); See also *KCodes NetUSB: How a Small Taiwanese Software Company Can Impact the Security of Millions of Devices Worldwide*, SEC Consult Vulnerability Lab, May 19, 2015, at http://blog.sec-consult.com/2015/05/kcodes-netusb-how-small-taiwanese.html (last visited May 22, 2015) (describing a common security vulnerability in millions of routers and other connected devices).

[23] *Open Resolver Project, at* http://openresolverproject.org/ (last visited May 22, 2015).

[24] *The Internet of Things: New Threats Emerge in a Connected World*, Symantec Official Blog, Jan. 20, 2014 at http://www.symantec.com/connect/blogs/internet-things-new-threats-emerge-connected-world (last visited May 22, 2015).

aspect of that working group's focus.[25] IPTF's multistakeholder process would provide an additional forum for productive discussion and progress in this area.

3. Improving Web Security

NCTA's members include the largest Internet service providers and the leading programming networks. Our companies are committed to doing their part to achieve greater security for their services and applications on the Web. Absent consumer confidence in the security of their personal information on the Web, broadband customers will be reluctant to adopt the array of innovative new Internet services that cable operators and programmers offer. While ISPs play a major role as operators of the underlying network, every web host, browser vendor, and app developer plays a role in ensuring that their users' data is protected.

Over the past year, it has become apparent that many web sites and services depend on a core group of open-source technologies. In early 2014, a vulnerability was discovered in the popular OpenSSL library, which provides encryption for many web services, desktop applications, and mobile apps.[26] Despite its use in the web servers powering almost two-thirds of the web, OpenSSL was surprisingly vulnerable to exploitation.[27] OpenSSL is far from the only piece of software that has proven vulnerable. On May 20, 2015, a new flaw was found in the transport-layer security used to establish encrypted connections between end users and websites that would allow an attacker to intercept those communications in real time.[28]

---

[25] *See* Cyber Physical Systems, available at www.nist.gov/cps/ (last visited May 25, 2015).

[26] *How Heartbleed transformed HTTPS security into the stuff of absurdist theater*, Ars Technica, Apr. 21, 2014, *at* http://arstechnica.com/security/2014/04/how-heartbleed-transformed-https-security-into-the-stuff-of-absurdist-theater/.

[27] *The Heartbleed Bug*, heartbleed.com, *at* http://heartbleed.com/ (last visited May 22, 2015).

[28] *HTTPS-crippling attack threatens tens of thousands of Web and mail servers*, Ars Technica, May 22, 20, 2015, *at* http://arstechnica.com/security/2015/05/https-crippling-attack-threatens-tens-of-thousands-of-web-and-mail-servers/.

Despite their importance, these core technologies are not always well funded, staffed, or consistently developed. Past industry efforts have been made to increase funding and devote more development resources to technologies like OpenSSL. For example, in 2014, a new fund was established at the Linux Foundation to provide monetary support to essential software, including OpenSSL.[29] The IPTF should build on these past industry efforts to secure the web by convening a broader group of Internet stakeholders, including network operators, software vendors, and web hosting companies to identify essential software, coordinate action to rapidly fix known vulnerabilities, and discuss ways to better support these shared and essential pieces of software in the future.

But even secure software will not inspire consumer confidence if it remains ambiguous to consumers whether their communications are secure. The "green lock" indicating a secure HTTPS connection has long been a key element in ensuring that consumers trust the websites they communicate with. However, as new security features have been implemented and old, insecure ones deprecated, it has become much more difficult for consumers to identify which websites are secure.[30] The Internet community must ensure that consumers are clearly and conspicuously provided with reliable information about the security of their communications. The IPTF process could facilitate a broad discussion of common techniques for reassuring consumers that their information is secure.

---

[29] *Tech giants, chastened by Heartbleed, finally agree to fund OpenSSL*, Ars Technica, Apr. 24, 2014, *at* http://arstechnica.com/information-technology/2014/04/tech-giants-chastened-by-heartbleed-finally-agree-to-fund-openssl/.

[30] *See, e.g.* Steve Schultz, *Firefox Changes its HTTPS User Interface…Again*, Freedom to Tinker, Jul. 24, 2012, *at* https://freedom-to-tinker.com/blog/sjs/firefox-changes-its-https-user-interface-again/ (describing changes to the Mozilla Firefox browser's user interface for displaying HTTPS security information); *Google to display warnings on sites that use SHA-1 certificates*, GlobalSign Blog, Sept. 4, 2014, *at* https://www.globalsign.com/en/blog/google-to-display-warnings-on-sites-that-use-sha-1-certificates/ (describing Google's plans to warn users when certain encryption algorithms are used to with HTTPS content).

However, incorporating desktop browser vendors, web services providers, and ISPs into this work is only part of the solution. Today, more than two thirds of Americans own a smartphone.[31] While the "green lock" is present in most mobile browsers, mobile apps have become an increasingly popular means of interacting with online services. Many of these applications use an embedded web browser to display content. Without the browser interface, there is no easily recognizable way for a consumer to know whether the app's connection is secure. The IPTF should encourage mobile app developers and vendors to come to the table and discuss a common, easily identifiable method for informing customers that their information is secure across devices and services.

CONCLUSION

For the foregoing reasons, NCTA recommends that the IPTF consider establishing multistakeholder processes to address botnet and malware mitigation, web security and/or securing the Internet of Things.

Respectfully submitted,

/s/ Rick Chessen

Rick Chessen
Loretta P. Polk
National Cable & Telecommunications Association
25 Massachusetts Avenue, N.W. – Suite 100
Washington, D.C. 20001-1431
(202) 222-2445

Matthew J. Tooley
Vice President, Broadband Technology
Science & Technology

Galen Pospisil
Research Assistant

May 27, 2015

[31] *U.S. Smartphone Use in 2015*, Pew Research Center, *at* http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/ (last visited May 22, 2015).