Before the
National Telecommunications and Information Administration
Washington, DC

In re	
Stakeholder Engagement on Cybersecurity in the Digital Ecosystem	Docket No. 1503122523-5253-01

COMMENTS OF
COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION

Pursuant to the request for comments[1] issued by the National Telecommunications Industry Association (NTIA) regarding the identification of substantive cybersecurity issues affecting the digital ecosystem that would benefit from multistakeholder engagement and coordinated action, the Computer & Communications Industry Association (CCIA) submits the following comments.

CCIA represents large, medium and small companies in the high technology products and services sectors, including computer hardware and software, electronic commerce, telecommunications and Internet products and services. CCIA members employ more than 600,000 workers and generate annual revenues in excess of $465 billion.[2]

I. Introduction

CCIA appreciates the opportunity to file in this proceeding, and commends NTIA and the

[1] *Request for Public Comment*, Docket No. 150312253-5253-01, *available at* https://www.federalregister.gov/articles/2015/03/19/2015-06344/stakeholder-engagement-on-cybersecurity-in-the-digital-ecosystem.

[2] A list of CCIA members is available at http://www.ccianet.org/members.

Internet Policy Task Force for turning their expertise to encouraging stakeholder engagement on cybersecurity in the digital ecosystem. As NTIA is aware, certain topics and problems in data management and cybersecurity better lend themselves to a multistakeholder process than others. It is important to focus on those areas where NTIA's expertise as a convening organization can be best leveraged.

In particular, CCIA believes a focus on issues where a collective action problem is currently preventing the wide-adoption of existing solutions, or where broadly accepted best practices have not penetrated or been implemented by small and medium enterprises, would be most effective. Increasing the overall level of knowledge across the stakeholder group is also important. Only by first understanding the state of current threats to the digital ecosystem can stakeholders identify potential policy gaps in this ongoing effort, and then develop best practices to meet the needs of the rapidly evolving threat landscape.

II. Particular topics of interest to a future multistakeholder cybersecurity process

Identity Theft and Secure Identities

The success of the digital economy is dependent in large part on the ability of Internet companies to keep their users' personal information secure in cyberspace. One of the earliest government reports on the viability of the Internet as a platform for commerce said, in 1997, "[i]f Internet users do not have confidence that their communications and data are safe from unauthorized access or modification, they will be unlikely to use the Internet on a routine basis for commerce."[3]

Web security is essential to ensure that consumers have trust in the Internet services they choose to use. Cyber attacks have left the personal data of American citizens vulnerable to

[3] White House, *A Framework for Global Electronic Commerce*, *available at* http://clinton4.nara.gov/WH/New/Commerce/read.html.

hackers and cyber-criminals, exposing them to the very real threats of identity theft, account takeover and cyber fraud, in many cases leading to real financial harm, and creating a potential disincentive to widespread adoption of Internet business models.

A Commerce-led multistakeholder process focusing on secure identities and identity theft mitigation would be an effective forum for increasing the understanding and utilization of multi-factor authentication tools. NTIA should focus such efforts in part on building consensus around a set of guidelines for stronger authentication protocols and other means to combat identity theft. A strong starting point for such an initiative could be the work done by the FIDO Alliance, which has developed technical specifications designed to authenticate users with a reduced reliance on passwords.[4]

Botnet and Malware Mitigation

Consumers continue to be subject to a range of cybersecurity issues that they are not able to effectively protect against solely through their own actions. Malware can be delivered to an increasing range of personal devices through a variety of means, thereby undermining confidence in the digital economy and results in significant costs to consumers and digital industry. Given the array of attack vectors and increasingly large potential attack surface, mitigating concerns related to malware and botnets will require collective action, including efforts from ISPs, security software providers, cloud hosting providers, consumers and others. A multistakeholder process that allows for the perspectives of each of these vulnerable but necessary participants in the digital commerce ecosystem is a natural venue to discuss methods to mitigate threats.

[4] FIDO Alliance, *About the Fido Alliance*, *available at* https://fidoalliance.org/about/overview/.

To avoid redundancy, any work done by a multistakeholder process focusing on botnet and malware mitigation should build upon prior work. In this case, the Department of Commerce's Industry Botnet Group (IBG) produced a set of principles aimed at managing the growing botnet problem through collective action, with an aim to educate users and report on lessons learned.[5] The collected knowledge of this effort would be particularly informative to a future multistakeholder process on botnet mitigation, which could help disseminate best practices to end-users, including small enterprises and consumers.

Core Internet Infrastructure, Vulnerability Disclosure

Considerable prior work has been done at within the federal government on the proper implementation of secure Internet infrastructure protocols and vulnerability disclosure. In the former category, the National Institute of Standards and Technology (NIST) has prepared guides for the deployment of the Secure Domain Name System (DNSSEC), improvement of Border Gateway Protocol (BGP) security, and the use of Transport Layer Security (TLS) in networks.[6] Similarly, the National Infrastructure Advisory Council at the Department of Homeland Security developed early recommendations for appropriate vulnerability disclosure protocols.[7] NTIA should consider working to adapt this early work for consumption by less technically sophisticated stakeholders in a future process.

[5] Industry Botnet Group, *Principles for Voluntary Efforts to Reduce the Impact of Botnets in Cyberspace* (Sept. 2013), *available at* http://industrybotnetgroup.org/principles/.

[6] *See e.g.* Ramaswamy Chandramouli and Scott Rose, *Secure Domain Name System (DNS) Deployment Guide*, National Institute of Standards and Technology (Sept. 2013), *available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-81-2.pdf; Rick Kuhn *et al*., *Border Gateway Protocol Security*, National Institute of Standards and Technology (July 2007), *available at* http://www.nist.gov/customcf/get_pdf.cfm?pub_id=51195; and Tim Polk *et al*., *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*, National Institute of Standards and Technology (April 2014), *available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf.

[7] John Chambers *et al*., *Final Report and Recommendations by the Council on Vulnerability Disclosure Framework*, National Infrastructure Advisory Council, *available at* https://www.dhs.gov/xlibrary/assets/vdwgreport.pdf.

Privacy

NTIA currently has a series of multistakeholder processes that address privacy-related issues.[8] Those should continue to be the primary mechanism through which stakeholder input is sought and best practices are developed. Should privacy be implicated in the context of NTIA's cybsecurity-focused process, it should look to prior work addressing privacy in a system security context, such as the NIST Cybersecurity Framework.[9]

III. Prior work by other expert organizations on cybersecurity

NTIA should also be cognizant of and deferential to the extensive ongoing cybersecurity-related work at standards bodies and other international participatory organizations. These include, but are not limited to:

- Internet Engineering Task Force
- Worldwide Web Consortium
- IEEE
- ISO/IEC
- Wi-Fi Alliance
- Bluetooth SIG
- Consumer Electronics Association
- Telecommunications Industry Association
- 3GPP
- FCC Communications, Security, Reliability, and Interoperability Council
- INCITS/ANSI
- Linux Foundation
- Open Web Application Security Project
- PCI Security Standards Council
- RASA Security for Business Innovation Council
- IT Sector Coordinating Council
- IT-ISAC

[8] Nat'l Telecomm. & Info. Admin., *Privacy Multistakeholder Process: Mobile Application Transparency* (Nov. 2013), *available at* http://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency; Nat'l Telecomm. & Info. Admin., *Privacy Multistakeholder Process: Facial Recognition Technology* (April 2015), *available at* http://www.ntia.doc.gov/other-publication/2015/privacy-multistakeholder-process-facial-recognition-technology.

[9] Nat'l Inst. of Standards & Tech., *Framework for Improving Critical Infrastructure Cybersecurity* (Feb. 2014) at 15, *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

- Financial Services Sector Coordinating Council
- FS-ISAC

IV. Conclusion

CCIA commends NTIA's interest in identifying substantive cybersecurity issues affecting digital commerce that might be served by a process to develop broad consensus, coordinated action, and the development of best practices. CCIA encourages NTIA to consider and expand upon the considerable prior work by expert bodies and federal agencies on cybersecurity-related issues as it begins to develop any future multistakeholder process.

May 27, 2015

Respectfully submitted,

Bijan Madhani
Public Policy & Regulatory Counsel
Computer & Communications Industry Association
900 Seventeenth Street NW, 11th Floor
Washington, D.C. 20006
(202) 783-0070