Before the
National Institute of Standards and Technology
Department of Commerce
Washington, DC

In re Information on Current and Future States of Cybersecurity in the Digital Economy	Docket No. 160725650-6650-01

COMMENTS OF
COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION

Pursuant to the Request for Information[1] (RFI) issued by the National Institute of Standards and Technology (NIST) on behalf of the Commission on Enhancing National Cybersecurity (CENC or "the Commission") and published in the Federal Register at 81 Fed. Reg. 52,827, the Computer & Communications Industry Association (CCIA) submits the following comments on current and future states of cybersecurity in the digital economy.

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. Our members employ more than 750,000 workers and generate annual revenues in excess of $540 billion.[2]

Given the breadth of the Commission's Request for Information, CCIA has chosen to focus on several specific areas of interest to its members. In these areas, CCIA sees challenges, but also opportunities for collaboration between government and the private sector to deliver solutions through existing or future partnerships and policy proposals.

[1] Notice, Request for information, *Information on Current and Future States of Cybersecurity in the Digital Economy,* 81 Fed. Reg. 52,827 (August 10, 2016), *available at* https://www.federalregister.gov/articles/2016/08/10/2016-18948/information-on-current-and-future-states-of-cybersecurity-in-the-digital-economy [hereinafter "Request for Information"].

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

User Trust and Security

One of the earliest government reports on the viability of the Internet 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] That assessment is no less true today. Tools and procedures that facilitate continued user trust in the digital ecosystem should to be a top priority for the Commission in preparing its recommendations.

Encryption

Ubiquitous strong encryption is essential to ensuring user confidence in the Internet as a platform for expression and commerce. It is increasingly deployed in every facet the digital world, from basic website delivery and communications protocols to online banking and payment processing services. To the extent the Commission is able, its findings and recommendations should recognize and emphasize the ever-growing importance of the unfettered availability of encryption in consumer-facing devices and services. As recognized by security experts and technologists, derogating these protections, for whatever reason, is neither technically feasible nor wise.[4]

Identity and Access Management

NIST has led the development of technical standards for secure digital identity authentication for the federal government. These standards are regularly used to guide implementations in the private sector. Currently, NIST is in the process of updating its guidelines for digital identity authentication,[5] and is receiving broad input on the potential deprecation of SMS as an out-of-band authenticator for multi-factor authentication systems. SMS as a factor can be prone to security weaknesses with respect to a phone number's direct link to a physical device. However, it is still a more secure option than no second factor, especially for users without smartphones or other physical tokens.

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

[4] *See e.g.* Harold Abelson, et. al., *Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications*, MIT CSAIL (July 2015), http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf.

[5] Paul A. Grassi & James L. Fenton, *Digital Authentication Guideline*, Draft NIST Special Publication 800-63-3 (2016), https://pages.nist.gov/800-63-3/sp800-63-3.html.

For the Commission's purposes, the input NIST has received in that process should be an instructive example in encouraging the developers, users, and regulators of data security systems to ensure that the perfect not be the enemy of the good. Where a security technique provides a net gain to users, particularly where the more effective option might be cost-prohibitive for system administrators or users, its use should not be discouraged.

Vulnerabilities Disclosure

Private security researchers and the government regularly discover, encounter, or acquire vulnerabilities and exploits in digital systems in the course of their research and operations. Ecosystem security is contingent on software and service vendors being appropriately notified of such vulnerabilities in order to patch systems and prevent harmful breaches or other negative outcomes. No widely adopted system of vulnerability disclosure exists for private security researchers, and the federal government's disclosure process lacks transparency and rigor. However, with the federal government's facilitation, there are possible paths forward to address both sides of the disclosure problem.

With respect to vulnerabilities research and disclosure by private security researchers, the National Telecommunications and Information Administration (NTIA) recently convened a multistakeholder process to increase awareness and adoption of existing best practices for disclosure, develop best practices for circumstances not previously addressed, and generally improve stakeholders' understanding of the incentives that researchers and vendors must balance when considering how and when to disclose vulnerabilities.[6] Stakeholders in the process are currently developing several outcome documents to address each of those goals. The Commission should encourage that future researchers and vendors take advantage of the final outcome documents of NTIA's process.

With respect to government to private sector disclosure, as the Commission is aware, the existing Vulnerabilities Equities Process (VEP) has raised considerable controversy. The VEP is the method currently used to determine whether a government entity will disclose information about security vulnerabilities to relevant private sector entities or withhold this information for its own purposes, which may include law enforcement, intelligence collection, and offensive

[6] Nat'l Telecomm. & Info. Admin., *Multistakeholder Process: Cybersecurity Vulnerabilities* (Apr. 2016), *available at* https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities.

uses. The VEP is run by the National Security Council and administered by the NSA, but little public information about the process, the equities at stake, and the rates of vulnerability disclosure is available.

Given the serious exploits that the government likely encounters, the VEP should be more robust and transparent than the existing process. At minimum, the VEP's structure should be enshrined in law; have broad participation from agency stakeholders including the FTC and Departments of Commerce, Homeland Security, State, and Energy; and be administered by a civilian agency with cybersecurity expertise, like DHS. The process of assessing vulnerabilities should have clear, standardized criteria; a set timeline for making determinations; regular reporting to Congress and the public; and oversight by independent bodies like the Privacy and Civil Liberties Oversight Board and relevant Inspectors General.

Public-Private Partnerships

The private sector and federal and state governments are all increasingly subject to attacks from bad actors, from nation states to criminal cartels. Collaboration among and between levels of government and the private sector is essential to the overall health of critical infrastructure and the digital ecosystem.

Information Sharing

Sharing of cyber threat data, when done effectively in a privacy-protective manner, can increase the cost of attacks and abusive behavior to attackers. Companies already share cyber threat information with both the government and other entities, both directly and through Information Sharing and Analysis Centers (ISACs); however, information sharing is often too slow and encumbered by overclassification and sector or government-specific siloing.

Information sharing about cyber threats needs to be faster and easier. Sharing should be done in real-time and machine-to-machine, enabling automated processes to address threats as they're discovered. Private entities need assurance that they are not violating laws and regulations by sharing cyber threat information, and individuals need confidence that cyber threat information sharing does not infringe on expectations of privacy. Finally, processes should be established to expedite security clearances so critical infrastructure employees can receive classified government cyber threat information.

Progress has been made in sharing of cyber threat information in part because of the passage of the Cybersecurity Act of 2015, which provided private sector liability protection for sharing and directed DHS to produce privacy rules for the collection and dissemination of threat data.[7] Whether the final privacy rules provide sufficient protection for users remains to be seen, and the Commission should consider their efficacy as it makes future recommendations regarding private-sector-to-government information sharing.

The issuance of Executive Order 13691 has encouraged the development of Information Analysis and Sharing Organizations (ISAOs), which will enable the effective sector-specific information sharing capabilities of ISACs to be used across industries, regions, and threat-types.[8] The Commission should further encourage the work of the ISAO Standards Organization currently developing the model practices and procedures for such organizations.[9] Peer-led information sharing is a vital tool in addressing a fast-evolving threat environment. The Facebook-led ThreatExchange platform is an effective model of a free, automated sharing platform that works through the participation of 250 trusted partner companies,[10] which the Commission should look to as an example for other ISACs and ISAOs.

Federal Government's Ability to Convene

One of the federal government's most effective tools to improve cybersecurity outcomes is its ability to bring together the private sector, consumer groups, and government experts to develop collaborative solutions to complex problems. This is regularly employed at the federal level by NTIA, as discussed with respect to the multistakeholder process on cybersecurity vulnerabilities. However, the government must also convene groups to address the numerous data security threats that cut across sectors and levels of government, where there are gaps in levels of expertise and understandings of risk.

The Commission should recognize that collaboration between different levels of government and the private sector has already lead to demonstrable results with respect to online tax fraud. Convened in 2015, the IRS Security Summit brought together the IRS, private sector companies, and State Departments of Revenue to develop security upgrades during the 2016 tax

[7] 18 U.S.C. § 1501.
[8] Exec. Order No. 13,691 § 2, 3 C.F.R. 271 (2015).
[9] About, ISAO STANDARDS ORGANIZATION, https://www.isao.org/about/.
[10] New Features and Integrations, THREATEXCHANGE, https://www.facebook.com/notes/threatexchange/new-features-and-integrations/1694983804048278.

preparation season.[11] The security upgrades include: a new password requirement for DIY filers, secure information sharing between tax software providers and the IRS to discover suspicious activity, and collaborative security reviews with reporting to the IRS and states.

Based on the IRS's own data, these newly implemented security techniques led to significant reductions in identity theft and fraudulent activity. Together, these techniques contributed to over $1.1 billion in prevented fraudulent returns and a 48% drop in identity theft reports to the IRS's Identity Theft Assistance Service.

September 9, 2016

Respectfully submitted,

Bijan Madhani
Public Policy & Regulatory Counsel
Computer & Communications Industry Association
900 17th Street NW, 11th Floor
Washington, D.C. 20006
(202) 783-0070

[11] 2015 Security Summit Report: Protecting Taxpayers from Identity Theft Tax Refund Fraud, IRS, https://www.irs.gov/PUP/newsroom/2015%20Security%20Summit%20Report.pdf.