From: **Julie Kearney**
Date: Mon, Apr 10, 2017 at 4:07 PM
Subject: CTA Comments on Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity
To: "cyberframework@nist.gov" <cyberframework@nist.gov>
Cc: Julie Kearney

Dear NIST Colleagues:

Attached please find CTA's Comments on Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity.

Please feel free to contact me with any questions.
Best regards,

Julie

Julie Kearney
Vice President, Regulatory Affairs
Consumer Technology Association (CTA)
1919 South Eads St.
Arlington, VA 22202

[Attachment Copied Below]

Before the
DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Gaithersburg, MD 20899

In the Matter of	)
	)
Proposed Update to the Framework for	)
Improving Critical Infrastructure Cybersecurity	)

COMMENTS OF THE CONSUMER TECHNOLOGY ASSOCIATION

The Consumer Technology Association ("CTA")[1] is pleased to submit these comments on Draft Version 1.1 of the Framework for Improving Critical Infrastructure Cybersecurity ("Framework").[2] The significant increase in the market for smart, connected devices, combined with media coverage of major data breaches, has thrust the technology industry into a national conversation about the privacy and security of its products. CTA works with its members to manage this complex policy environment using a comprehensive strategy of member education, outreach to regulators, thoughtful responses to legislative initiatives, and promotion of effective industry self-regulatory frameworks. Accordingly, CTA appreciates the opportunity provided by NIST for industry to continue driving the development of the Framework in a manner that protects

---

[1] The Consumer Technology Association ("CTA")™ is the trade association representing the $292 billion U.S. consumer technology industry, which supports more than 15 million U.S. jobs. More than 2,200 companies – 80 percent are small businesses and startups; others are among the world's best known brands – enjoy the benefits of CTA membership including policy advocacy, market research, technical education, industry promotion, standards development and the fostering of business and strategic relationships. CTA also owns and produces CES® – the world's gathering place for all who thrive on the business of consumer technologies. Profits from CES are reinvested into CTA's industry services.

[2] Department of Commerce, National Institute for Standards and Technology, *Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity*, Request for Comments, 82 Fed. Reg. 8408 (Jan. 25, 2017) ("RFC").

American citizens and infrastructure by promoting business and entrepreneurial flexibility to deploy new technologies and risk management solutions tailored to companies' individual cybersecurity needs.

INTRODUCTION

CTA stands for innovators, including manufacturers occupying various parts of the supply chain and service providers relying on multiple technologies, and ranging from large household names to entrepreneurial startups. As a result of this diverse membership, CTA has witnessed first-hand the benefits of the Framework's common language and non-regulatory, flexible approach to cyber risk management, which its members continue to adapt and utilize in response to an ever-evolving threat environment.

CTA's members understand that digital security is a core business imperative and applaud NIST for recognizing that the nation's infrastructure, supply chains, and connected services and devices will be more securely protected when government serves as a nimble convener and educator, rather than a static regulator. Rapidly changing technologies require flexibility and constant industry adaptation that cannot be achieved through compliance with prescriptive rules.[3] Indeed, locking in specific requirements would be counterproductive, potentially delaying or even derailing the launch of new security approaches. The freedom to innovate unquestionably has benefitted consumers and the industry that CTA represents – it has generated more than $290 billion in revenue,

---

[3] Gary Shapiro, *How the Heavy Hand of Government Stifles the On Demand Economy*, TechDirt (Aug. 25, 2015) ("*The Heavy Hand of Government*"), https://www.techdirt.com/articles/20150824/11370432049/how-heavy-hand-government-stifles-demand-economy.shtml.

supports more than 15 million U.S. jobs, and serves as a catalyst for technological revolutions such as the Internet of Things ("IoT"). Provided that the industry is not hampered by top-down security mandates, it will continue to deliver these benefits and be responsive to evolving security challenges. In short, as CTA has previously described, the Framework is emblematic of the sort of innovation-friendly policies that can help the U.S. unleash economic growth and maintain its global leadership role in technology.[4]

In a relatively short period of time, the Framework has become an indispensable tool for cybersecurity risk management. CTA commends NIST for its commitment to updating and honing the Framework to reflect this ongoing experience. CTA likewise welcomes NIST's ongoing interest in soliciting industry feedback on its experience implementing the Framework. Such dialogue can only enhance trust and strengthen the public-private partnership that the Framework represents, and CTA hopes that NIST will continue to promote that exchange of ideas going forward.[5]

Many of CTA's member companies participated in earlier rounds of comments on the Framework, including the one that preceded NIST's proposal of the recent updates. More broadly, both CTA and many of its individual members have been active in working

---

[4] *See, e.g.*, Comments of the Consumer Technology Association, *The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things*, Docket No. 170105023-7023-01, at 10 (filed Mar. 13, 2017) ("CTA IoT Green Paper Comments"); Comments of the Consumer Technology Association f/k/a the Consumer Electronics Association, *The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things*, Docket No. 1603311306-6306-01, at 25-26 (filed June 2, 2016).

[5] Consumer Technology Association, *Internet of Things: A Framework for the Next Administration*, at 8 (Nov. 2016), http://www.cta.tech/cta/media/policyImages/policyPDFs/CTA-Internet-of-Things-A-Framework-for-the-Next-Administration.pdf ("CTA IoT White Paper").

with different government agencies to exchange ideas about the best path for developing forward-looking solutions to the nation's security challenges while also preserving an environment that promotes innovation – particularly as the IoT develops.

[6] Meanwhile, CTA has provided technical security guidance for a number of audiences, including a technical report (CTA TR-12) titled *Securing Connected Devices for Consumers in the Home*,[7] security best practices and an online checklist for connected home dealers and professionals,[8] and has issued consumer PSAs in radio markets reading 2.2 million people. Likewise, some CTA members are members of industry groups that have developed cybersecurity resources for consumers and best practices for home security,[9] and some have collaborated with NIST on programs like its Cyber-Physical Systems Program and Cybersecurity for IoT Program.

---

[6] *See, e.g., id.* at 9-10 (describing participation of CTA and its members in various ongoing efforts to address IoT issues); IoT Green Paper Comments at 1-4 (describing CTA response to the Commerce Department's "Green Paper" on fostering the advancement of the IoT).

[7] CTA Technical Report: Securing Connected Devices for Consumers in the Home, CTA-TR-12 (Nov. 2015), https://standards.cta.tech/kwspub/published_docs/CTA-TR-12-Final.pdf.

[8] CTA, Welcome to the Connected Home Security Checklist Tool, https://www.cta.tech/Membership/Divisions-Councils/TechHome-Division/Device-Security-Checklist.aspx; TechHome (a Division of Consumer Technology Association), Recommended Best Practices for Securing Home Systems (Dec. 2015), https://www.cta.tech/cta/media/Membership/PDFs/Recommended-Best-Practices-for-Securing-Home-Systems-v16.pdf.

[9] CTA IoT White Paper at 8 n.100 (noting resources developed by the National Cyber Security Alliance and the WiFi Alliance, both of which share some members with CTA).

RESPONSES TO SPECIFIC QUESTIONS

Consistent with its previous advocacy and ongoing activities, CTA offers the following observations in connection with two of the specific questions identified in Framework Version 1.1.

How do the changes made in the draft Version 1.1 impact the cybersecurity ecosystem?

As a general matter, CTA is hopeful that the changes in draft Version 1.1, if adopted, can have a positive impact on the cybersecurity ecosystem by addressing two increasingly important issues – metrics and supply chain risk management ("SCRM") – so long as these changes are implemented in a manner that does not create barriers to trade or otherwise depart from the core principles underlying the Framework. In particular, CTA continues to believe that policymakers can best promote innovation by favoring market-driven solutions based on open industry standards and avoiding over prescriptive regulations, technology mandates, and barriers to trade.[10] In this respect, CTA applauds the intention underlying the proposed update to allow the Framework to "retain[] its flexible, voluntary, and cost-effective nature."[11] Any proposed updates concerning metrics and SCRM should endeavor to reflect this guiding principle, and should seek to avoid setting in motion a process by which further steps on these issues could calcify into inflexible standards to which industry participants are expected to adhere.

---

[10] *See, e.g.*, *id.* at 8-9; *see also* Shapiro, *The Heavy Hand of Government*. The National Technology Transfer and Advancement Act (NTTAA), Public Law 104-113, directs federal agencies to adopt voluntary consensus standards wherever possible.

[11] RFC, 82 Fed. Reg. at 8409.

Continued flexibility is particularly important with respect to metrics. Identifying appropriate metrics for assessing cyber preparedness is a challenging exercise, and acceptable answers have been and will continue to be elusive. As Thomas Bossert, Assistant to the President for Homeland Security and Counterterrorism and the Deputy National Security Advisor, recently described the pursuit of cybersecurity metrics: "I'll know it when I see it."[12] Thus, the Framework should eschew the pursuit of uniform metrics that would apply across sectors or industries, in order to allow individual companies to develop measurement methodologies that take their unique circumstances into account and to let this aspect of Framework implementation stabilize. Moreover, rather than seeking any sort of consensus on metrics within a fixed timeframe, the Framework should note that the matter is fluid and requires ongoing collaboration.

Is there a better label than "version 1.1" for this update?

CTA believes that the proposed title "Version 1.1" is appropriate. This is not merely a matter of aesthetics. In contrast to NIST's original aspiration toward a "Framework Version 2.0," the proposed title conveys an intent to make changes incrementally as experience with the Framework matures, rather than undertaking a more radical overhaul of an approach to cybersecurity risk management that is being increasingly embraced both domestically and globally.

---

[12] Thomas Bossert, *Cyber Disrupt 2017 Keynote: Next Steps for Cybersecurity After a Decade of Lessons Learned* (Mar. 15, 2017), https://www.csis.org/analysis/cyber-disrupt-2017-keynote-next-steps-cybersecurity-after-decade-lessons-learned.

CONCLUSION

CTA looks forward to working with NIST and other stakeholders on the continued evolution of the Framework.

Respectfully submitted,
CONSUMER TECHNOLOGY ASSOCIATION

By: */s/ Julie M. Kearney*

Julie M. Kearney
Vice President,
Regulatory Affairs
Brian Markwalter
Senior Vice President,
Research and Standards
Michael Bergman
Senior Director,
Technology and Standards
Consumer Technology Association
1919 S. Eads Street
Arlington, VA 22202

April 10, 2017