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 2 of Version 1.1 of the Framework for Improving Critical Infrastructure Cybersecurity ("Framework"), which the National Institute of Standards and Technology ("NIST") released for public comment in December of last year.[2] CTA commends NIST for how it has addressed certain stakeholder concerns about the initial draft of Version 1.1, both for the broad-based collaborative process it has conducted since the release of the first draft and for the substance of the revisions that resulted from it. CTA supports Draft 2 of Version 1.1 and believes that it will preserve the Framework's "flexible, voluntary, and cost-effective nature," thus achieving NIST's

[1] Consumer Technology Association (CTA)™ is the trade association representing the $351 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] *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 Draft 2, at iii (rel. Dec. 5, 2017), *available at* www.nist.gov/cybersecurity-framework. ("Framework Draft 2").

goals in pursuing this update in the first place.[3] In these comments, CTA addresses the updates on three critical issues – cybersecurity measurement, supply chain risk management, and coordinated vulnerability disclosure.

## INTRODUCTION

Just last week, CTA concluded CES 2018, the global stage for innovation and proving ground for innovators and breakthrough technologies for fifty years.[4] As it does each year, this experience showcased the dynamic nature of technology today and the consumer benefits that are possible when companies are allowed to innovate freely – as was demonstrated by the proliferation of smart, connected devices that were on display. It also enabled business leaders and pioneering thinkers in both industry and government to continue the national conversation about digital security in an ever-evolving threat environment. To that end, CES 2018 featured a number of panels focused on cybersecurity issues.[5] Moreover, various companies (including CTA members) demonstrated their security solutions, illustrating the shared understanding of CTA members that cybersecurity is a core business imperative.

Against this backdrop, NIST's latest revisions to Version 1.1 of the Framework are a welcome development. As CTA emphasized in its comments on the previous iteration of

---

[3] 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, 8409 (Jan. 25, 2017).

[4] More information is available at https://www.ces.tech/.

[5] *See, e.g.*, Cybersecurity in a Connected World, https://www.ces.tech/Conference/ConferenceProgram/Conference-Tracks/Connect2Car/Cybersecurity-in-a-Connected-World; Cybersecurity and the Auto Industry, https://www.ces.tech/Conference/ConferenceProgram/Conference-Tracks/Vehicle-Technology/Cybersecurity-and-the-Auto-Industry.aspx.

Version 1.1,[6] rapidly changing technologies such as those in evidence at CES 2018 require flexibility and constant industry adaptation that cannot be achieved through compliance with prescriptive rules.[7] Indeed, locking in specific requirements would be counterproductive, potentially delaying or even derailing the launch of new security approaches. CTA thus explained that policymakers can best promote innovation by favoring market-driven solutions based on open industry standards and avoiding prescriptive regulations, technology mandates, and barriers to trade.[8] Accordingly, CTA and many of its individual members continue to be active in working 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.[9]

The Framework has been 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, and

---

[6] Comments of the Consumer Technology Association, *Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity* (filed Apr. 10, 2017) ("CTA Comments").

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

[8] CTA Comments at 5; *see also, 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); 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).

[9] *See, e.g.*, CTA Comments at 3-4; Consumer Technology Association, *Internet of Things: A Framework for the Next Administration*, at 8-10 (Nov. 2016), http://www.cta.tech/cta/media/policyImages/policyPDFs/CTA-Internet-of-Things-A-Framework-for-the-Next-Administration.pdf.

an indispensable tool for cybersecurity risk management. Although some parties initially expressed unease about aspects of Version 1.1 that signaled the prospect of a more prescriptive compliance regime, Draft 2 includes several corrections that, in CTA's view, should assuage these concerns. CTA discusses these updates below.

## DISCUSSION

### 1. Cybersecurity Measurement

In its comments on the first draft of Version 1.1, CTA argued that 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.[10] CTA also asserted that the Framework should recognize the fluidity of cybersecurity measurement and the need for ongoing collaboration, as opposed to pursuing any sort of consensus on metrics within a fixed timeframe.[11]

Draft 2 aligns with these recommendations. Clarifying the intent of Version 1.1's provisions on cybersecurity measurement, the section is now named "Self-Assessing Cybersecurity Risk with the Framework."[12] In contrast to the original title for this section ("Measuring and Demonstrating Cybersecurity"), this new title embodies an important theme with respect to the Framework's approach to measurement: that individual companies can, should, and must engage in a meaningful self-assessment of their cybersecurity risk profiles that takes account of their particular circumstances and business objectives, rather than having that

[10] CTA Comments at 6.

[11] *Id.*

[12] Framework Draft 2 at 21.

role be determined or prescribed by third parties. Moreover, while Draft 2 does not purport to dictate how companies should conduct such self-assessments, it does set useful parameters, cautioning them to "avoid[] reliance on artificial indicators" and urging them instead to "be thoughtful, creative, and careful" about how they employ metrics.[13] This guidance is not only the best approach in its own right, it also is more faithful to the Framework's core tenets than was the previous draft.

This core theme carries through the text that follows, culminating with the proposition that "[o]rganizations are encouraged to innovate and customize how they incorporate measurements into their application of the Framework with a full appreciation of their usefulness and limitations."[14] This vote of confidence for industry sets precisely the right tone as NIST prepares to "initiat[e] a cybersecurity measurement program focusing on aligning technical measures to determine effect on high-level organizational objectives, as well as to support decision making by senior executives and oversight by boards of directors," which according to the "Roadmap" document that accompanies Version 1.1 "will involve consultation with the business, research, and government sectors."[15] CTA welcomes this express commitment to continued collaboration and looks forward to working with NIST in connection with the development of a cybersecurity measurement program.

---

[13] Framework Draft 2 at 21.

[14] Framework Draft 2 at 22.

[15] Draft NIST Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1, at 14-15 (Dec. 5, 2017), *available at* https://www.nist.gov/sites/default/files/documents/2017/12/05/draft_roadmap-version-1-1.pdf.

### 2. Supply Chain Risk Management

The revisions to the Framework's section on supply chain risk management ("SCRM") – entitled "Communicating Cybersecurity Requirements with Stakeholders" – likewise provide comfort that the Framework is not endorsing a prescriptive approach. Although SCRM may appear to some regulators as ripe for some sort of rules, Draft 2 (like the draft before it) avoids any such temptation. In addition, Draft 2 includes additional text that highlights the challenges of SCRM as experienced by CTA members. For instance, it correctly observes: "Supply chains are a complex, globally distributed, and interconnected set of resources and processes between multiple levels of organizations. Supply chains begin with the sourcing of products and services and extend from the design, development, manufacturing, processing, handling, and delivery of products and services to the end user. Given these complex and interconnected relationships, [SCRM] is a critical organizational function."[16] Such an addition ensures that the Framework is premised on the real-world experiences of industry participants today, facilitating and promoting its continued voluntary use.

### 3. Coordinated Vulnerability Disclosure

Finally, regarding coordinated vulnerability disclosure ("CVD"), Draft 2 adds a new, fifth subcategory under the "Respond" Function and the "Analysis" Category: "Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from

[16] Framework Draft 2 at 16.

internal and external sources (e.g. internal testing, security bulletins, or security researchers)."[17] CTA sees potential advantages and disadvantages to this addition.

On one hand, this subcategory strikes CTA as a common-sense addition, in that it prompts companies to think through how they should learn about and analyze vulnerabilities – an exercise that industry should encourage. It also does not directly raise the same concerns about regulatory requirements prompted by the CVD provision in the pending Warner-Gardner bill – namely, that the Department of Homeland Security's National Protection and Programs Directorate would issue guidelines for agencies to impose on contractors regarding the disclosure of vulnerabilities, and that these guidelines would be related in some way to new statutory liability protections for researchers under the Computer Fraud and Abuse Act and the Digital Millennium Copyright Act. In that setting, there has been some concern that the new liability protections and disclosure guidelines might prompt a veritable free-for-all among researchers (including those hired by contractors' competitors) hacking devices for nefarious or competitive purposes in order to hurt contractors' prospects in procurement processes or otherwise damage a contractor's reputation.

On the other hand, however, this addition may, even if inadvertently, gloss over the inherent challenges associated with CVD. As highlighted by the new text relating to SCRM discussed above, CVD involves numerous entities with different roles, and sharing information among them is not straightforward. Yet by setting forth more specific guidance as compared to

[17] The first four subcategories remain unchanged from the original draft of Version 1.1: "(1) Notifications from detection systems are investigated; (2) The impact of the incident is understood; (3) Forensics are performed; and (4) Incidents are categorized consistent with response plans." Framework Draft 2 at 43.

the more brief and more general descriptions in the other four subcategories in this category – for instance, the third subcategory is simply, "Forensics are performed" – this addition arguably suggests an incrementally more prescriptive approach to CVD than is the case with other parts of the Framework's guidance in the "Analysis" category. While CTA believes that discovering and addressing vulnerabilities are important elements of cybersecurity risk management, we caution that the specificity of this new subcategory relative to the other subcategories under "Analysis" may be somewhat premature, particularly given the ongoing multifaceted processes underway between government and industry that are pertinent to the issues of vulnerabilities and patching.[18] Accordingly, we recommend that NIST consider changes that generalize the guidance, thereby lessening the potential for the more prescriptive interpretation. For instance: "Processes are established to discover and address vulnerabilities."

[18] See, *e.g.*, U.S. Department of Commerce, National Telecommunications & Information Administration, *Multistakeholder Process: Cybersecurity Vulnerabilities*, https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities; and *Multistakeholder Process:Internet of Things (IoT) Security Upgradability and Patching*, https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security; U.S. Department of Commerce, National Institute of Standards and Technology (NIST), Cybersecurity for IoT Program, https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program; and National Telecommunications & Information Administration, *Request for Comment on Promoting Stakeholder Action Against Botnets and Automated Threats*, https://www.ntia.doc.gov/federal-register-notice/2018/rfc-promoting-stakeholder-action-against-botnets-other-automated-threats.

## 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
(703) 907-7644

January 19, 2018