Before the Department of Commerce
National Institute of Standards and Technology
Washington, D.C.

Request for Comments	)
	)
Framework for Improving Critical	)
Infrastructure Cybersecurity	)
Version 1.1 (Draft 2)	)

COMMENTS OF CTIA

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

John A. Marinho
Vice President, Technology and Cybersecurity

Melanie K. Tiano
Director, Cybersecurity and Privacy

CTIA
1400 16th Street, NW, Suite 600
Washington, DC 20036
202-736-3200
www.ctia.org

January 19, 2018

TABLE OF CONTENTS

I. Introduction and Executive Summary

CTIA[1] members are pleased to provide feedback on Draft 2 of the Cybersecurity Framework ("CSF" or "Framework"). The communications industry has "enthusiastically embraced" the Framework.[2] In November 2017, NIST pointed to the Communications, Security, Reliability, and Interoperability Council (CSRIC) work mapping the Framework to industry activities as a resource for best practices on cybersecurity risk management.[3]

CTIA appreciates NIST's efforts to incorporate many of our recommendations. While we are pleased to see industry feedback reflected in Draft 2, CTIA urges a few changes to Draft 2 to increase its usability. We explain our suggestions and include an Appendix of specific language recommendations. We look forward to helping NIST with priority Roadmap issues in separate work streams. NIST and other parts of the government can help small and medium businesses. Making progress on measurement and self-assessment will require creativity and broad engagement. And NIST should address federal agency cybersecurity. CTIA looks forward to helping NIST with these issues.

II. NIST Should Emphasize the Characteristics that Made the Framework a Success.

We appreciate NIST's effort to implement feedback provided by commenters on Draft 1 expressing concern about proposed changes on measurement. This includes CTIA's recommendation that Section 4.0, then titled *Measuring and Demonstrating Cybersecurity*, be revised to focus on voluntary self-assessment—not grading compliance.[4] This is a point that others echoed,[5] along with urging more flexibility.[6] While NIST's changes to this section go far to improve the Draft, there are two more things NIST should do to preserve the CSF's utility.

---

1 CTIA® (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st century connected life. The association's members include wireless carriers, device manufacturers, suppliers as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. The association also coordinates the industry's voluntary best practices, hosts educational events that promote the wireless industry and co-produces the industry's leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

2 Letter from Robert Mayer, Chairman, Communications Sector Coordinating Council, *et.al.*, to the Gov't Accountability Office, at 18 (Oct. 31, 2017) ("CSCC GAO Letter"), https://www.ustelecom.org/news/oct-2017-cscc-letter-gao

3 NIST, Matt Barrett, *A Framework for Protecting Our Critical Infrastructure* (Nov. 1, 2017), https://www.nist.gov/blogs/taking-measure/framework-protecting-our-critical-infrastructure.

4 Comments of CTIA, Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity, at 12 (filed April 10, 2017) ("*CTIA Version 1.1 Draft 1 Comments*"), https://www.nist.gov/sites/default/files/documents/2017/04/21/2017-04-10_-_ctia.pdf

5 *See* Comments of The US Telecom Association, Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity, at 4 (filed Apr. 10, 2017).

6 *See* Comments of U.S. Chamber of Commerce, Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity, at 5 (filed Apr. 10, 2017); Comments of Business Roundtable, Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity, at 1 (filed Apr. 10, 2017); Comments of CTA, Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity, at 2 (filed Apr. 10, 2017) ("CTA Comments").

The CSF offers *voluntary* guidelines and best practices. According to NIST Director Charles Romine, the Framework's "voluntary, risk-based prioritized, flexible, repeatable, and cost-effective approach" is critical.[7] NIST has discussed the Framework's voluntary nature in presentations, press releases, and Q&A.[8] Despite NIST's significant past efforts to emphasize the Framework's voluntary nature, Version 1.1 Draft 2 only mentions this critical element in passing. NIST should add language that emphasizes that the Framework developed under EO 13636 continues to evolve, is voluntary for the private sector, is flexible and risk-based, and uses a common language to address cybersecurity risk in a cost-effective way.[9] Expanding on the Framework's voluntary nature is especially important as other countries look to act on cybersecurity.

CTIA supports NIST's elimination of proposed Section 3.7 on federal alignment. The Framework has two sets of users with different obligations. Federal agencies are required by Executive Order 13800 to use the CSF.[10] Agencies have numerous obligations for handling sensitive information, such as classified information and citizens' personal information. But, with the exception of some government contractors, private organizations have different needs. To reduce confusion, NIST should make clear that the Framework addresses different audiences by including language that indicates the document was developed to improve risk management in critical infrastructure, but is now mandatory for federal agencies. By contrast, the Framework is adaptable so that it can be voluntarily used by private organizations of varying sizes and abilities, in any sector or community, and these uses will vary substantially.[11]

III. NIST Has Properly Focused on Self-Assessment, and Can Broadly Explore Measurement in the Roadmap.

A. Section 4.0 can be refined to *encourage* self-assessment.

CTIA applauds NIST's revisions to focus on flexible self-assessment. Renaming Section 4.0 from "Measuring and Demonstrating Cybersecurity" to "Self-Assessing Cybersecurity Risk within the Framework" is consistent with NIST's goal that organizations use internal evaluations to improve decision making. There are a few things NIST can do to encourage self-assessment.

---

7 Testimony of Charles H. Romine, Ph.D., Director, Information Technology Laboratory, NIST, before the United States House of Representatives, Committee on Science, Space, and Technology, Subcommittee on Research and Technology (Feb. 14, 2017).

8 *See* NIST, Press Release, NIST Releases Update to the Cybersecurity Framework (Jan. 10, 2017) ("This update is fully compatible with the original framework, and the framework remains voluntary and flexible to adaption."); Barrett, Matt, *A Framework for Protecting Our Critical Infrastructure* (Nov. 1, 2017), https://www.nist.gov/blogs/taking-measure/framework-protecting-our-critical-infrastructure; and NIST, Cybersecurity Framework FAQs, Framework Basics, FAQ 1 and 2 (updated Aug. 25, 2016), https://www.nist.gov/cyber framework/cybersecurity-framework-faqs-framework-basics

9 *See* Appendix for recommended edits to lines 80-83 on page 1 of Draft 2.

10 Exec. Order No. 13800, 82 FR 22391 (May 11, 2017), https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

11 *See* Appendix for recommended edits to lines 95-96 on page 1 of Draft 2.

NIST should underscore that self-assessments are voluntary. NIST should also acknowledge that organizations' abilities to conduct "thoughtful, creative, and careful" reviews as contemplated will vary based on an organization's resources.[12] Relatedly, the revised Framework rightly recognizes limitations in any self-assessment and warns against reliance on artificial indicators. Draft 2 should clarify that self-assessments are likely to be part of an iterative process, particularly because cybersecurity measurement remains nascent. For example, in line 752, NIST should add "Over time," to the start of the sentence.[13]

Finally, NIST can encourage self-assessments by addressing concerns about the risk of public or third-party disclosure or requests for production of results by regulators. NIST should explicitly acknowledge the competitive and security sensitivity of self-assessment information. It should recognize that organizations conducting self-assessments may prudently protect information from external disclosure. NIST should add language that explicitly notes the process and results of such assessments are likely to be sensitive and proprietary. NIST should further recognize that, depending on the assessment's goal and structure, results may not be useful or understandable outside the organization, and organizations that intend to share results may structure their assessment activities differently than those who expect to use them exclusively for internal use.[14] NIST should acknowledge the sensitivity of this information and explain why it is acceptable to keep the results of such reviews confidential.

B. The Roadmap provides an opportunity to advance the study of measurements and self-assessments.

NIST's Roadmap proposes to launch a Cybersecurity Measurement Program to focus on "aligning technical measures to determine effect on high-level organizational objectives, as well as to support decision making by executives and boards of directors."[15] The initiative will build on existing approaches and include consultation among researchers, business, and government.[16]

NIST should focus on federal agencies, but to the extent it addresses the private sector, NIST's Measurement Program should be guided by industry, which understands the complexity of measurement. With industry, NIST should develop principles to guide the program and catalyze research. Researchers are exploring measurements, but there is no consensus. Business schools are also engaged. For example, the Kogod Cybersecurity Governance Center at American University studies cybersecurity governance.[17] Thoughtful, experiential development

---

[12] NIST, *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 Draft 2*, at 21 (Dec. 5, 2017) ("*Version 1.1 Draft 2*"), https://www.nist.gov/sites/default/files/documents/2017/12/05/draft-2_framework-v1-1_without-markup.pdf

[13] *See* Appendix for recommended edits to line 752 on page 21 of Draft 2.

[14] *See* Appendix for recommended edits to lines 756-758 on page 21 of Draft 2.

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

[16] *Id*.

[17] Kogod Cybersecurity Governance Center, *Cybersecurity Governance: Five Reasons Your Cybersecurity Governance Strategy May be Flawed and How to Fix It* (Mar. 18, 2018), http://www.american.edu/kogod/research/cybergov/upload/cybersecurity-five-reasons.pdf

takes time, and NIST should talk to companies, auditors, cybersecurity consultants, insurers, and others to identify possible approaches.

IV. NIST Should Refine the Discussion of Supply Chain Risk Management.

CTIA appreciates NIST's discussion of complex supply chain risk management ("SCRM"). With a few modest changes, NIST can better reflect supply chain variability and clarify that each organization should tailor supply chain security to their needs.

NIST's definition of supply chain[18] does not capture the breadth of supply chains and inputs. For example, there is a critical human element, as companies use contractors, consultants, in ways that impact the design, offering, and management of products and services. The Draft's definition of cyber SCRM[19] is good, but it appears that NIST is trying to characterize supply chains generically enough to address federal agencies, critical infrastructure, general businesses, as well as innovators and technology providers. This leads to confusion. For example, Figure 3 is not very illuminating about which entities NIST is trying to capture. Similarly, "Buying Decisions" in Section 3.4 is confusing: what "buyers" does NIST have in mind, and how will they use "Target Profiles"? NIST's attempt to include a broad definition is understandable, but the Draft would be more useful if NIST provided clarity about which entities it is referencing.[20]

Some discussions oversimplify challenges. They assume a high degree of sophistication—a willingness and ability to demand and enforce contractual commitments, as opposed to, for example, reliance on indemnifications. This is a difficult area for companies of all sizes, some of whom are just starting to grapple with the diversity, complexity, and age of hundreds or thousands of contracts that might have cybersecurity implications. Draft 2 should acknowledge challenges in applying the SCRM ideals to existing relationships, and it should note that for forward-looking activities, organizations may have limited ability to negotiate.[21]

Given the supply chain's complexity and the myriad relationships it entails, NIST should make clear that parts of the ecosystem will work together in different ways. For example, NIST should clarify that risk assessment discussions between buyers and sellers need to take place within the context of conducting appropriate cost-benefit analyses, tailored to each enterprise's cybersecurity posture.

---

[18] *Version 1.1 Draft 2*, at 16 ("a complex, globally distributed, and interconnected set of resources and processes between multiple levels of organizations [that] . . . . 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.")

[19] *Id.* at 17 ("the set of activities necessary to manage cybersecurity risk associated with external parties[,] . . . address[ing] both the cybersecurity effect an organization has on external parties and the cybersecurity effect external parties have on an organization.")

[20] The Framework also does not clearly define "cybersecurity outcome," which Draft 2 uses frequently. NIST should clearly define it.

[21] NIST should say something like: "Private organizations may have challenges in analyzing and managing risk in existing relationships and contracts, which may be numerous and complex. This may make it prudent to devote resources elsewhere. Likewise, some organizations will have limited ability to make security related demands on suppliers or to actively monitor vendors' activities, and those of the vendors' supply chain."

Verification activities can be resource-intensive, and buyers should be aware of the costs incurred from expanding or complicating suppliers' verification requirements. For many relationships, there may not be a standardized cybersecurity-related audit or certification procedure that a supplier can use to satisfy multiple buyers, so there is a risk of creating inefficient outcomes to the extent different buyers request different types of information from suppliers. Buyers should work with suppliers in choosing verification steps so that suppliers can be efficient and sustain their privacy goals.[22] NIST should clarify, either in ID:SC or in the SCRM section, that buyers and suppliers can create cost savings by agreeing to verification processes, rather than suggesting rigid requirements that could negatively impact supplier privacy and security goals. Suppliers and buyers should make resource efficiency part of their analysis when determining what verification steps are conducted.

In sum, the Draft should clarify a few things: that supply chains include people; that not all contracts and suppliers present the same risks; and that companies prudently should prioritize within SCRM. To accomplish this, NIST should clarify that supply chains begin with the sourcing of products and services and include various inputs, including people like third-party vendors and consultants. They extend from the design, development, manufacturing, processing, handling, and delivery of products and services to the end user. NIST should also emphasize that people are involved at every step of the supply chain and may introduce risk, which should be appropriately considered in the SCRM process. NIST should also add that while cyber SCRM is the set of voluntary activities undertaken to manage cybersecurity risk associated with external parties, not all organizations have the maturity or resources needed to address every aspect of their supply chain.[23] The cost-benefit analysis of smaller firms does not justify investment in a cyber SCRM regime intended for much larger organizations. NIST should recognize that a rigid, one-size-fits-all regime could be counterproductive, and that flexibility is essential.

V. It is Premature to Include Vulnerability Disclosure Programs in the Framework, But They Can Be Addressed in the Roadmap.

Though the topic was not included in the January 2017 draft, NIST proposed at its workshop to add vulnerability disclosure programs to the Framework. Workshop participants expressed uncertainty, but Draft 2 nonetheless adds a subcategory on vulnerability disclosure lifecycle to the Framework Core.[24] Because this topic needs far more consideration, it is premature to include it in the Framework Core.

Though coordinated vulnerability disclosure programs may seem uncontroversial to some in the security community, the programs are relatively new and numerous challenges attend

---

[22] For example, the new ID.SC-5 in Table 2 currently says response and recovery planning and testing "are conducted with suppliers and third parties" but makes no mention of the cost-benefit analysis associated with deciding whether (and if so, how) to conduct such testing with a particular supplier based on the risks and priorities identified in the overall SCRM assessment process. That section should clarify that it does not prescribe particular types or frequency of testing that will apply across the board, nor does it purport to impact relevant contractual relationships between suppliers and buyers.

[23] See Appendix for recommended edits to lines 621-624 on page 16 and lines 625-626 on page 17 of Draft 2.

[24] *Version 1.1 Draft 2*, at 23. The draft's Risk Assessment category now includes "Asset vulnerabilities are identified and documented." *Id.* at 27.

them. Several CTIA members have robust programs that include bounties and third-party engagement, but they know from experience that programs are complex and evolving, and not all companies are prepared to adopt them.

NIST acknowledges that guidelines are still in flux. The Roadmap discusses vulnerability disclosure, noting that "appropriate guidelines and standards need to be defined and then adopted in products to enable organizations of various levels of capability and size to make use of indicators and other related information."[25] The Roadmap cites NIST SP 800-150, ISO/IEC 29147, and ISO/IEC 30111 as examples of work in the area.[26]

Publicly available guidance on developing a vulnerability disclosure program has not fully grappled with the many complexities that exist and add to the challenges. NTIA's sample vulnerability disclosure policy would allow white hat hackers to engage in "reverse engineering or circumventing protective measures,"[27] but companies may not want to waive the protections of copyright law or the Computer Fraud and Abuse Act. The DOJ Cybersecurity Unit's framework for vulnerability disclosure programs raises similar issues.[28] Not all companies are prepared to work with third-party security researchers or third parties who identify and want to disclose claimed vulnerabilities. The research community has varied motives, with some actors abusing disclosures.[29] NIST should consider whether there are adequate protections and incentives to work with third parties in a constructive and confidential manner.

In practical terms, companies must consider several complexities related to handling claimed vulnerabilities. This includes whether they have resources for a program, which will need to include sufficient personnel and expertise. A company must consider obligations it might have to notify and work with other businesses, partners, suppliers, regulators, and the public about reported vulnerabilities.[30] And, consequences create concern. Public disclosures can alarm consumers and expose vulnerabilities for bad actors to exploit. Disclosures also have led to class-action litigation and federal investigations, even if no cyber incident occurred.

---

[25] The Roadmap adds a subsection to the "Cyber-Attack Lifecycle" focusing on coordinated vulnerability disclosure (CVD). *Roadmap*, at 5.

[26] *Id*.

[27] NTIA Safety Working Group, *Coordinated Vulnerability Disclosure "Early Stage" Template and Discussion* (Nov. 4, 2016), https://www.ntia.doc.gov/files/ntia/publications/safetywg_draft_11-04-16_clean.pdf

[28] Department of Justice, Criminal Division, Cybersecurity Unit, *A Framework for a Vulnerability Disclosure Program for Online Systems* (July 2017), https://www.justice.gov/criminal-ccips/page/file/983996/download. Like NTIA, the Cybersecurity Unit encourages companies to waive the protections of the Computer Fraud and Abuse Act. Still, CTIA commends the Cybersecurity Unit for specifying that its framework is voluntary and "does not dictate the form of or objectives for vulnerability disclosure programs" because different organizations have different goals and priorities.

[29] *See, e.g.*, Matthew Goldstein, *Hedge Fun and Cybersecurity Firm Team Up to Short-Sell Device Maker*, New York Times (Sept. 8, 2016) (describing how a cybersecurity researcher and hedge fund joined forces to exploit a claimed vulnerability in a medical device to short its manufacturer's stock).

[30] *See* Megan L. Brown and Matt Gardner, *Considering a Vulnerability Disclosure Program? Recent Push Raises Questions for General Counsel*, CircleID (Feb. 10, 2017), http://www.circleid.com/posts/20170210_considering_a_vulnerability_disclosure_program.

Foundational issues remain murky, making it appropriate to give further consideration before adding to the Framework. For example, it is unclear what constitutes a "vulnerability"[31] as distinguished from configuration issues that create risks. NIST has acknowledged the difficulty in defining "vulnerability," noting that there are many definitions "covering various combinations of concepts, including knowledge, attacks, exploitability, risk, intention, threat, scope and time of introduction."[32] In terms of handling identified vulnerabilities, not all vulnerabilities are the same or have the same impact. Companies (and the ecosystem) need to grapple with varying severity and consider what likelihood of exploitation justifies or requires disclosure and taking corrective action. They must also confront the reality that not all vulnerabilities can or should be patched. As the Verizon Data Breach Investigations Report notes, not all vulnerabilities are able to be fixed, but they can be managed with varying mitigations or compensating controls.[33]

Adding a topic of such novelty and complexity to the Framework Core is premature and may discourage Framework use by less mature organizations. NIST should remove it from the Framework Core and address it in the Roadmap.

VI. NIST Should Address Guidance for IoT in Other Proceedings.

The CSF includes several references to IoT.[34] No doubt, the Framework will be a useful tool for those looking to enhance IoT risk management, but Draft 2 does not differentiate between IoT settings: ***first***, IoT is used by an enterprise and needs to be managed as part of overall cyber risk management; ***second***, IoT is a product or service that is designed, built, and deployed, for which innovators may bring Framework principles to bear. NIST should focus the Framework on enterprise management of IoT and clarify that it is not setting expectations for IoT developers.[35] We look forward to continuing our work with NIST on IoT security issues in other workstreams, in which NIST should be guided by voluntary standards, international efforts, and global best practices, including IoT guidelines that have already been established by global entities.[36]

---

[31] *See, e.g.,* variance of NIST's definition of "vulnerability" (SP 800-53: "weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source;" SP 800-61: "a weakness in a system, application, or network that is subject to exploitation or misuse;" CNSSI-4009: "weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source." Available at: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf. *See also* ISO/IEC 30111 (Nov. 1, 2013) (defining "vulnerability" as "weakness of software, hardware, or online service that can be exploited").

[32] NIST, *Dramatically Reducing Software Vulnerabilities: Report to the White House Office of Science and Technology Policy*, NISTIR 8151 (Nov. 2016), http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8151.pdf

[33] *See* Verizon, 2017 Data Breach Investigations Report (10th Ed.), at 13, http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/.

[34] *See, e.g., Version 1.1 Draft 2*, at 2-3, 17.

[35] *See* Appendix for recommended edits to lines 107-108 on page 2 of Draft 2.

[36] *See* U.S. Chamber of Commerce & Wiley Rein LLP, *The IoT Revolution and Our Digital Security: Principles for IoT Security* (Sept. 2017), https://www.wileyrein.com/assets/htmldocuments/FINAL%20REPORT%20-%20The.IoT.Revolution..Our.Digital.Security.Final%20002.pdf. *See also* Comments of CTIA, Security

VII. The Authentication Discussion Should Emphasize Flexibility for the Private Sector.

CTIA appreciates NIST's edits to support evolving authentication tools. The addition of authentication as a Subcategory, with references to single and multi-factor authentication, within the Identity Management and Access Control Category, raises the profile of these verification systems.[37] NIST also addresses Identity Management in the Roadmap.

CTIA suggests adding the phrase "as appropriate" to Framework subcategory PR.AC-7: "Users, devices, and other assets are authenticated [as appropriate] (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)." Varied approaches to authentication exist, so each organization (particularly in the private sector) should evaluate options and freely determine what makes sense. NIST has been looking at authentication for federal systems and has embraced aspirational goals (such as discouraging certain forms of multifactor authentication, as in SP 800-63). While there may be reason to restrict *federal agencies'* authentication options, NIST should make clear that private organizations are free to use any form of authentication that they deem appropriate.

VIII. NIST Should Emphasize Voluntary Information Sharing and Consider Whether Incentives are Needed To Promote Broader Information Sharing.

NIST should not suggest that information sharing is a prerequisite to mature use of the Framework. Instead, NIST should encourage voluntary sharing efforts to include small and medium enterprises. NIST augments expectations in four Tiers[38] with an increasing degree of sophistication in information sharing. According to NIST, Tier 1 organizations do not collaborate with other entities, nor do they share information.[39] Tier 4 organizations share prioritized information internally and externally in real or near-real time.[40] As the Cybersecurity Information Sharing Act of 2015 (CISA) made clear, information sharing is *voluntary*. NIST should place less emphasis on external sharing to ensure that sharing remains voluntary.

Section 2.2 makes clear that moving between tiers takes place based on the totality of the circumstances, not based on prescriptive requirements about the nature or quantity of information sharing. While Draft 2 appropriately makes information sharing practices one of the factors an organization should consider, it should clarify that there are no baseline requirements on information sharing. Accordingly, Section 2.2's "External Participation" discussions in the "Tier 3" and "Tier 4" sections should make clear that organizations "may" share information, rather than it being a mandate.

---

and Privacy Controls for Federal Information Systems and Organizations, DRAFT NIST SP 800-53 (filed Sept. 12, 2017).

37 *See Version 1.1 Draft 2*, at 30-31.

38 *Id.*, at 9-10.

39 *Id.*, at 10.

40 *Id.*, at 12.

As CTIA members know from experience sharing information,[41] the quality, not quantity, of information shared is what enhances security. Section 4.2 of the Roadmap (Cyber-Attack Lifecycle) highlights the importance of "timely communication" and "actionable information" to counter threats and address vulnerabilities.[42] NIST should encourage *voluntary* sharing of *meaningful* information. In fact, it is worth investigating whether sharing cyber threat indicators and defensive measures is enough. CISA did not address sharing of other information, like cyber risk management practices. Two years after CISA, it may be time to consider whether additional sharing is needed.

One specific area where additional protections could be helpful is in the context of third party interactions (assessments, risk analyses and forensics) and the use of outside assistance. This relates to information sharing as well as self-assessment activity. After an organization begins to use the framework, there should be a 'safe' environment to hire or work with external third parties to help assess weaknesses and improve them. This could include consultants, ISACs and ISAOs, and others who can help companies better address cyber risks and solutions. This would be particularly helpful for small and medium sized organizations who may not have the internal resources to do these activities, but also fear public disclosure, third party discovery or regulatory oversight related to their efforts.[43]

IX. CTIA Looks Forward to Collaborating on Key Roadmap Projects.

The Roadmap lays out twelve areas of future work, some of which are likely to be more important than others in the near term. NIST should prioritize projects in three particularly fruitful areas: small businesses, international engagement, and federal agency alignment. Focusing intently on a few high impact efforts will increase the chance that progress can be made and have an effect.

A. Section 4.12 on Small Business Awareness and Resources has more potential for immediate impact than many other initiatives.

Small and medium sized businesses (SMBs) need help. CSRIC found that special considerations and accommodations may be necessary for SMBs to use the Framework.[44] The National Security Telecommunications Advisory Committee (NSTAC) has recognized that small businesses lack the same resources and access to cyber expertise as larger entities.[45] The Small

---

41 *See CTIA Version 1.1 Draft 1 Comments*, at 3-4.

42 *Roadmap*, at 4.

43 *See, e.g.*, J. Higgins, *Head of auto industry's ISAC cites 'chilling effect' of lawsuit on cyber info-sharing* (Nov. 2017), https://insidecybersecurity.com/daily-news/head-auto-industry%E2%80%99s-isac-cites-%E2%80%98chilling-effect%E2%80%99-lawsuit-cyber-info-sharing

44 Communications Security, Reliability and Interoperability Council, *Cybersecurity Risk Management and Best Practices, Working Group 4: Final Report*, at 27 (Mar. 2015).

45 The President's National Security Telecommunications Advisory Committee, *NSTAC Report to the President on Internet and Communications Resilience* (Nov. 16, 2017), https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20ICR%20FINAL%20DRAFT%20-%20508%20compliant.pdf.

Business Administration (SBA) has cited the need for the Framework to address concerns specific to SMBs, including areas like cost, compliance, and education.[46] After it finalizes the revised Framework, NIST should prioritize developing use cases for smaller enterprises, and helping resource-constrained organizations improve their basic blocking and tackling. It should resist the urge to further tinker with the Framework by adding additional elements. NIST can immediately improve the nation's security by identifying actionable guidance and considering how to raise awareness among smaller enterprises about resources that exist already. This may be more important and impactful than other efforts NIST has underway on specific security and technology issues.

B. International engagement is critical, so NIST should prioritize Section 4.8.

CTIA commends NIST for engaging with the international community to promote the Framework in international standards. Cybersecurity demands an open and predictable development environment rather than regional, closed processes.[47] Given the interconnectedness of the global digital infrastructure, NIST should prioritize work under Section 4.8.

NIST acknowledges that international entities do not yet share a common language for cybersecurity.[48] Worse than the lack of a common lexicon, some countries are developing unique standards and best practices, which threaten interoperability principles that helped the digital economy thrive. For example, China and other countries have pursued top-down, bordered, government-centric approaches.[49] Microsoft,[50] Intel,[51] and J.P. Morgan[52] stress the need for a global harmonized approach on cybersecurity. Specialized, regional cybersecurity requirements balkanize digital infrastructure, increase costs, and impede innovation. This is why companies call for global collaboration. NIST should prioritize global collaboration, partnering with and assisting the Department of Homeland Security (DHS) and others on private sector

---

46 *See* Small Business Administration, *Comments to the National Institute of Standards (NIST) regarding its Preliminary Cybersecurity Framework* (Dec. 16, 2013), https://www.sba.gov/sites/default/files/Advocacy%20Comment%20Letter%20to%20NIST%20on%20Cybersecurity.pdf.

47 Karen McCabe, IEEE Senior Director, Technology Policy and International Affairs, *Global, Open Standards for Cyber-security*, Beyond Standards IEEE Standards Association (Nov. 6, 2014), https://beyondstandards.ieee.org/cybersecurity/global-open-standards-for-cyber-security/

48 *Roadmap*, at 13.

49 *See* Laura DeNardis, Gordon Goldstein, & David A. Gross, *The Rising Geopolitics of Internet Governance: Cyber Sovereignty v. Distributed Governance*, Columbia School of International and Public Affairs (Nov. 30, 2016), https://sipa.columbia.edu/sites/default/files/The%20Rising%20Geopolitics_2016.pdf

50 Microsoft, *Developing a National Cybersecurity Strategy*, at 22 (Oct. 2013), https://blogs.technet.microsoft.com/microsoft_on_the_issues/2013/10/04/microsoft-releases-best-practices-for-developing-a-national-strategy-for-cybersecurity/

51 Jackie Medecki and Riccardo Masucci, *Intel Guides Conversation on Global Approaches and Standardization to Improve Cyber Risk Management at CyberNextDC*, Intel (Nov. 6, 2017), https://blogs.intel.com/policy/2017/11/06/intel-guides-conversation-at-cybernextdc/

52 Reuters Staff, *Regulators need to develop global cyber security standards -JPM's Pinto*, Reuters (Oct. 14, 2017), https://www.reuters.com/article/usa-iif-banks/regulators-need-to-develop-global-cyber-security-standards-jpms-pinto-idUSL4N1MP093

readiness and partnerships with government.[53] Likewise, NIST should help promote open standards and best practices consistent with U.S. economic and security interests.[54]

C. NIST can do a lot of good on federal agency alignment, Section 4.5, which is in its core area of expertise.

NIST is well suited to promote federal agency cybersecurity alignment. NIST has historically advised agencies on cybersecurity, including on how to implement the Framework.[55] NIST has the technical expertise and widespread credibility to ensure that federal agencies align their approaches. Improvement of federal network security is a critical priority for the Executive Branch,[56] and should be for NIST, particularly after years of scrutiny and high-profile incidents.

It is not uncommon for agencies to have their own cybersecurity standards. For example, the Internal Revenue Service (IRS)[57] and Federal Bureau of Investigation (FBI)[58] have their own information safety regulations that do not necessarily align with the Framework. Now that Executive Order 13800 requires all federal civilian agencies to use the CSF, NIST should take a lead role. As part of a federal risk management approach, all agencies should use mobile management; patch and update software and operating systems; educate users on cyber hygiene; and take extra precautions (like encryption) for senior officials. Use of the NIST Framework will help agencies prevent breaches of government systems that hold citizen and company data.[59]

---

[53] Thomas P. Bossert and Jeanette Manfra, *Press Briefing on the Attribution of WannaCry Malware Attack to North Korea*, White House (Dec. 19, 2017) (Manfra: "A company can't single-handedly defend itself against a nation-state attacker. Cybersecurity is a shared responsibility…As identified in the WannaCry incident, cybersecurity defense is a global challenge. As many as 150 countries had systems infected by this ransomware. And it is only through international partnerships that the United States had time to prepare."), https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/

[54] *See* President Donald J. Trump, *2017 National Security Strategy* at 18 (Dec. 2017) ("Departments and agencies will eliminate unnecessary regulations that stifle growth, drive up costs for American businesses, impede research and development, discourage hiring, and incentivize domestic businesses to move overseas. We will balance our reduction in regulations with adequate protections and oversight."), https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

[55] NIST, *The Cybersecurity Framework: Implementation Guidance for Federal Agencies*, Draft NISTIR 8170 (May 2017), https://csrc.nist.gov/csrc/media/publications/nistir/8170/draft/documents/nistir8170-draft.pdf

[56] *See* President Donald J. Trump, *2017 National Security Strategy* at 12-13 (Dec. 2017) ("Federal networks also face threats. These networks allow government agencies to carry out vital functions and provide services to the American people. The government must do a better job of protecting data to safeguard information and the privacy of the American people. Our federal networks must be modernized and updated."), https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

[57] IRS, *Encryption Requirements of IRS Publication 1075* (Aug. 27, 2017), https://www.irs.gov/privacy-disclosure/encryption-requirements-of-irs-publication-1075

[58] FBI, *Criminal Justice Information Services (CJIS)*, https://www.fbi.gov/services/cjis.

[59] *See, e.g.*, U.S. Office of Personnel Management, *Cybersecurity Incidents*, Cybersecurity Resources Center, https://www.opm.gov/cybersecurity/cybersecurity-incidents/; U.S. Securities and Exchange Commission, *Statement on Cybersecurity* (Sept. 20, 2017), https://www.sec.gov/news/public-statement/statement-clayton-2017-09-20.

X. Conclusion

CTIA and its members support NIST's hard work and collaborative spirit to develop the Framework Version 1.0 and update it. While some additions add complexity, NIST has retained the key characteristics—flexibility and voluntariness—that made the Framework a success. We urge NIST to keep changes to the Framework simple and minimal; to clearly state its voluntary nature; and to emphasize the diversity of users' contexts. CTIA members look forward to working with NIST and others on future Framework efforts.

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

John A. Marinho
Vice President, Technology and Cybersecurity

Melanie K. Tiano
Director, Cybersecurity and Privacy

CTIA
1400 16th Street, NW, Suite 600
Washington, DC 20036
202-736-3200
www.ctia.org

XI. APPENDIX OF SUGGESTED CHANGES

CTIA proposes several modest changes and additions to improve clarity, preserve the best parts of the Framework, and avoid a prescriptive approach. For ease of reference, we identify here some specific suggested language changes:

- Page 1 (lines 80-83): "Consistent with the Cybersecurity Enhancement Act, the Framework that was developed under EO 13636 and continues to evolve. It is voluntary for the private sector, flexible, and risk-based, and uses a common language to address and manage cybersecurity risk in a cost-effective way based on organization needs without placing additional regulatory requirements."

- Page 1 (lines 95-96): "This document was developed to improve cybersecurity risk management in critical infrastructure, and is now mandatory for Federal agencies. The Framework is adaptable so that it can be voluntarily used by organizations of varying sizes and abilities, in any sector or community. All these uses will vary substantially."

- Page 2 (lines 107-108): "… or connected devices more generally in the context of enterprise users and buyers, including the Internet of Things (IoT)."

- Page 16 (lines 621-624): "Supply chains begin with the sourcing of products and services, and include various inputs, including people like third-party vendors and consultants. They extend from the design, development, manufacturing, processing, handling, and delivery of products and services to the end user. People are involved at every step of the supply chain and may introduce risk, which should be appropriately considered in the SCRM process."

- Page 17 (line 624-Cyber SCRM discussion): Draft 2's discussion of supply chain should include a statement to the effect that "Private organizations may have challenges in analyzing and managing risk in existing relationships and contracts, which may be numerous and complex. This may make it prudent to devote resources elsewhere. Likewise, some organizations will have limited ability to make security related demands on suppliers or to actively monitor vendors' activities, and those of the vendors' supply chain."

- Page 17 (lines 625-626): "While all organizations may not have the maturity or resources needed to address every aspect of their supply chain, cyber SCRM is the set of voluntary activities undertaken to manage cybersecurity risk associated with external parties."

- Page 21 (line 752): "Over time, self-assessment and measurement should improve the decision making about investment priorities.

- Page 21 (lines 756-758): "An organization that wants to engage in self-assessment can accomplish this internally or by seeking third-party help. The process and results of such assessments are likely to be sensitive and proprietary. Depending on the assessment's goal and structure, results may not be useful or understandable outside the organization doing them. Organizations that intend to share their results may want to structure their

assessment activities differently than those who expect to use them exclusively for internal use."

- Page 31 (PR.AC-7): "Users, devices, and other assets are authenticated [as appropriate] (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)."