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

In the Matter of

NIST Cybersecurity Framework 2.0) Concept Paper
Concept Paper: Potential)
Significant Updates to the Cybersecurity)
Framework)

COMMENTS OF CTIA

Thomas K. Sawanobori
Senior Vice President and Chief Technology
Officer

John A. Marinho
Vice President, Technology and Cybersecurity

Justin C. Perkins
Manager, Cybersecurity and Policy

CTIA
[redacted]

March 6, 2023

Table of Contents

I. INTRODUCTION AND SUMMARY.

CTIA[1] welcomes the opportunity to continue working with the National Institute of Standards and Technology ("NIST") on updates to the *Framework for Improving Critical Infrastructure Cybersecurity* ("CSF") by commenting on the *NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework* ("Concept Paper").[2] CTIA has actively participated in a decade of NIST CSF proceedings, including by commenting on last year's Request for Information ("RFI") that asked questions about updating the CSF and NIST's National Initiative for Improving Cybersecurity in Supply Chains.[3]

Consistent with its work in other proceedings, NIST is conducting extensive stakeholder engagement as it moves towards CSF 2.0 by seeking comment on the RFI,[4] hosting workshops[5] and working sessions ("February Working Sessions"),[6] and seeking comment on the Concept

[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] NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework, NIST (Jan. 19, 2023), https://www.nist.gov/system/files/documents/2023/01/19/CSF_2.0_Concept_Paper_01-18-23.pdf ("Concept Paper").

[3] Comments of CTIA, Docket Number: 220210-0045(filed Apr. 25, 2022), https://www.nist.gov/system/files/documents/2022/05/03/04-25-2022%20-%20CTIA.pdf.

[4] *Request for Information on Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management*, Department of Commerce, NIST, 87 Fed. Reg. 9,579, 9,579 (Feb. 22, 2022), https://www.govinfo.gov/content/pkg/FR-2022-02-22/pdf/2022-03642.pdf.

[5] *Journey to the NIST Cybersecurity Framework (CSF) 2.0 | Workshop #1*, NIST, https://www.nist.gov/news-events/events/2022/08/journey-nist-cybersecurity-framework-csf-20-workshop-1 (last updated Sept. 8, 2022); *Journey to the NIST Cybersecurity Framework (CSF) 2.0 | Workshop #2*, NIST, https://www.nist.gov/news-events/events/2023/02/journey-nist-cybersecurity-framework-csf-20-workshop-2 (last updated Feb. 28, 2023).

[6] *Journey to the NIST Cybersecurity Framework (CSF) 2.0 | In-Person Working Sessions*, NIST, https://www.nist.gov/news-events/events/2023/02/journey-nist-cybersecurity-framework-csf-20-person-working-sessions (last updated Feb. 16, 2023).

Paper.[7] CTIA applauds NIST's work to build consensus and refine this voluntary and flexible cybersecurity framework that global organizations can use in their information security efforts.

With these comments, CTIA makes several recommendations. *First*, NIST should recognize that the CSF serves as the foundation for countless enterprise cybersecurity initiatives and should avoid making significant changes to the CSF Core that may have harmful impacts on backward compatibility, particularly given the reliance both domestically and internationally by businesses and governments alike.

Second, NIST should adopt certain changes proposed in the Concept Paper that are grounded in flexibility and would promote broad adoption of the CSF. Specifically, it should: (1) adopt its proposals to maintain the current level of detail and specificity in the CSF; (2) continue to emphasize that the CSF is intended to be scalable, flexible, simple, and easy-to-use; (3) retain the CSF as a vendor- and technology-neutral enterprise risk management tool; and (4) retain the CSF's voluntary nature and refrain from transforming the CSF into quasi-regulation or a proxy for regulation.

Third, while CTIA supports addressing governance issues in the CSF, NIST should ensure that any updates do not create issues for backward compatibility or create redundancy within the CSF itself. To address important governance issues without disrupting the CSF's Core, NIST should consider incorporating governance issues into its discussion of Tiers and adding governance-specific outcomes throughout the existing CSF Core, rather than adding a new Govern Function that may not align easily with other Functions, may duplicate Subcategories that support governance, and would be disruptive to the CSF's Core. Importantly, any governance guidance must be flexible to account for the wide variance of organizational

[7] Concept Paper at 1.

structures and management approaches among CSF stakeholders, which range from very large global public companies to small companies, and startups to non-profits, among others. Governance may be better addressed in separate CSF profiles or other guidance documents, as those workstreams could enable NIST to gather more input about the diverse organizational structures of potential CSF users.

Fourth, NIST should treat cybersecurity supply chain risk management ("C-SCRM") with a light touch, as it did in CSF 1.1, which is appropriate for the complex and variable nature of C-SCRM. Third party issues are diverse and present many different complexities for organizations' cyber risk management, among other risk considerations. A great deal of C-SCRM work has been done since CSF 1.1 was released, but there is no universal approach or set of best practices that can cover the diversity of supply chain issues and roles that NIST may want to address. NIST can address certain third-party risks in the existing Core and can meaningfully update its Informative References and mappings to ensure CSF 2.0 reflects ongoing and robust public and private efforts to promote C-SCRM.

Fifth, NIST should align CSF 2.0 with SP 800-55 Rev. 2, *Performance Measurement Guide for Information Security* ("800-55 Rev. 2"), by adopting its proposal to provide substantive cyber measurement guidance in 800-55 Rev. 2 rather than the CSF. Addressing measurement challenges in 800-55 Rev. 2 will help keep the CSF a practical and usable framework and will also streamline NIST workstreams by addressing cyber measurement guidance in one document.

Sixth, NIST should take steps to improve the practical implementation and continued relevance of the CSF, including by expanding its definition of Tiers, leveraging and publicizing the Online Informative References ("OLIR") Program to keep Informative References up-to-date, and bolstering its mappings to other relevant guidance documents and standards.

II. THE CSF IS A BEDROCK OF MODERN ENTERPRISE CYBERSECURITY, WHICH COUNSELS IN FAVOR OF NARROW, TARGETED CHANGES IN CSF 2.0.

A. The Wireless Sector Leverages the CSF in Various Cybersecurity Initiatives.

The wireless sector applies the CSF in various contexts. For example, the FCC's Communications Security, Reliability, and Interoperability Committee ("CSRIC") conducted a comprehensive mapping of the CSF to the five segments of the Communications Sector (wireless, cable, broadcast, wireline, and satellite).[8] CSRIC determined that the structure of the CSF Core is useful for describing outcomes and illustrating use cases.[9] Subsequent CSRIC guidance has drawn heavily on the CSF, including on topics such as security-by-design, Next Generation 9-1-1, and cybersecurity workforce development.[10]

CTIA has used the CSF as the foundation for its own cybersecurity initiatives, including its 5G Security Test Bed, which brings together "wireless providers, equipment manufacturers, cybersecurity experts, academia, and government agencies to demonstrate and validate how 5G security will work, using real 5G networks."[11] CTIA's Internet of Things ("IoT") Cybersecurity

[8] Cybersecurity Risk Management and Best Practices Final Report, CSRIC IV Working Group 4 (Mar. 2015), https://transition fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf

[9] *Id*. at 20, 28.

[10] *See* Secure Hardware and Software: Security-by-Design, Final Report Best Practices Recommendations for Hardware and Software Critical to the Security of the Core Communications Network, CSRIC V Working Group 6, at 10 (Mar. 2016), https://www.atis.org/wp-content/uploads/01_legal/docs/CSRIC%20V/WG6_FINAL_%20wAppendix_0316.pdf; Final Report Small Carrier NG9-1-1 Transition Considerations, CSRIC VI Working Group 1, at 28, 30-33 (Sept. 2018), https://www.fcc.gov/files/csric6wg1sept18ng911reportdocx; Report on Security Risks and Best Practices for Mitigation in 9-1-1 Legacy, Transitional and NG 9-1-1 Implementations, CSRIC VII Working Group 4, at 31-80 (Sept. 16, 2020), https://www fcc.gov/files/csric7reportsecuirtyrisk-bestpracticesmitigation-legacytransitionalng911pdf; Cybersecurity Workforce: Status Update, CSRIC V Working Group 7, at 3, 7 (Dec. 3, 2015), https://transition fcc.gov/bureaus/pshs/advisory/csric5/WG7_Presentation_120315.pptx.

[11] *5G Security Test Bed*, 5G Security Test Bed, https://5gsecuritytestbed.com/ (last visited Feb. 1, 2023)

Certification Program, which establishes a baseline for IoT device security on wireless networks, also builds on the CSF.[12] Further, CTIA and other Communications Sector stakeholders contributed to the C2 Consensus on IoT Device Security Baseline Capabilities, which leverages the CSF.[13]

B. The CSF Is a Foundational Document that Underpins Numerous Cybersecurity Tools, Guidance Documents, and Approaches, Both Domestically and Overseas.

The CSF is a foundational cybersecurity document that has been the bedrock of public and private enterprise cybersecurity efforts over the last decade.

SRMA Resources. Each federal Sector Risk Management Agencies ("SRMA") "develops a sector-specific [risk management] plan through a coordinated effort involving its public and private sector partners."[14] The Communications Sector-Specific Plan, for example, "tailors the strategic guidance provided in the [National Infrastructure Protection Plan] to the unique operating conditions and risk landscape of the Communications Sector."[15] A variety of other sector-specific resources relate to the CSF.[16]

CSF Profiles. NIST has done the hard work to create numerous profiles that tailor CSF objectives with various specific missions, business objectives, threats, or technologies, allowing organizations to understand where they currently stand and where they need to be to meet their

[12] *See* Cybersecurity Certification Test Plan for IoT Devices, Version 2.0, CTIA Certification (Dec. 2021), https://ctiacertification.org/wp-content/uploads/2020/10/CTIA-Certification-Cybersecurity-Test-Plan-V2.0.pdf.

[13] The C2 Consensus on IoT Device Security Baseline Capabilities, Council to Secure the Digital Economy, at 20, 28 (Sept. 2019), https://csde.org/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf.

[14] Communications Sector, CISA, https://www.cisa.gov/communications-sector (last visited Feb. 28, 2023).

[15] Communications Sector-Specific Plan: An Annex to the NIPP 2013, DHS, at 1 (2015), https://www.cisa.gov/sites/default/files/publications/nipp-ssp-communications-2015-508.pdf.

[16] See Cybersecurity Framework: Critical Infrastructure Resources, NIST, https://www.nist.gov/cyberframework/critical-infrastructure-resources (last updated Dec. 8, 2021).

security goals.[17] CTIA encourages NIST and the NIST National Cybersecurity Center of Excellence ("NCCoE") to expand its profile work, raise the public awareness of proceedings, and work to engage more stakeholders in profiles, as an alternative to further expanding the CSF to address unique considerations for particular critical infrastructure ("CI") sectors or to anticipate concerns from particular regulators.

NIST Frameworks. NIST uses the CSF as a model for risk management frameworks in other contexts, including *the Privacy Framework*, [18] the *Risk Management Framework for Information Systems and Organizations* ("RMF"),[19] and the recently finalized *Artificial Intelligence Risk Management Framework*.[20]

Other NIST Guidance. A wealth of other NIST guidance relies on or maps to the CSF.[21] This includes documents specific to supply chain risk management ("SCRM"), such as NIST SP

[17] *Examples of Framework Profiles*, NIST, https://www.nist.gov/cyberframework/examples-framework-profiles (last updated Jan. 31, 2023).

[18] NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0, NIST (Jan. 16, 2020), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf.

[19] NIST SP 800-37, Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, NIST (Dec. 2018), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf.

[20] NIST AI 100-1, Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST (Jan. 2023), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

[21] *See, e.g.*, NISTIR 8170, Approaches for Federal Agencies to Use the Cybersecurity Framework, NIST (Mar. 2020), https://nvlpubs nist.gov/nistpubs/ir/2021/NIST.IR.8170-upd.pdf; NISTIR 8286A, Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management, NIST (Nov. 2021), https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8286A.pdf; Draft (2nd) NISTIR 8270, Introduction to Cybersecurity for Commercial Satellite Operations, NIST (Feb. 2022), https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8270-draft2.pdf; NIST SP 800-171, Rev. 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, NIST (Feb. 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf; NIST SP 1800-23, Energy Sector Asset Management: For Electric Utilities, Oil & Gas Industry, NIST (May 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-23.pdf; NIST SP 1800-24, Securing Picture Archiving and Communication System (PACS): Cybersecurity for the Healthcare Sector, NIST (Dec. 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-24.pdf.

800-161, Rev. 1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* (“800-161”).[22]

International Guidance. NIST’s leadership has pioneered the use of the CSF by other countries, making structural changes particularly fraught because of the potential for disruption. The CSF has been translated into nine different languages, allowing stakeholders across the world to leverage the CSF’s guidance. Further, and as NIST recognizes in the Concept Paper, numerous countries have adopted or adapted the CSF.[23] For example:

- The Israeli government built its *Cyber Defense Methodology for the Organization* (“ICDM”) on the CSF.[24] The Israeli government has discussed the importance of harmonizing the ICDM with the CSF, stating that “harmonizing our methodology with leading standards creates an international cyber defense language which supports collaboration against global cyber threats.”[25]

- The Italian government has adopted an Italian *National Framework for Cybersecurity and Data Protection*, which is based on the CSF.[26] As stated during NIST’s most recent CSF 2.0 workshop by an official from Italy’s National Cyber Risk Management Division, Agenzia per la Cybersicurezza Nazionale,

[22] NIST SP 800-161, Rev. 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (May 2022), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf; *see also* NISTIR 8276, Key Practices in Cyber Supply Chain Risk Management: Observations from Industry, NIST (Feb. 2021), https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8276.pdf.

[23] Concept Paper at 5; *Cybersecurity Framework: International Resources*, NIST, https://www.nist.gov/cyberframework/international-resources (last updated Nov. 9, 2022).

[24] Cyber Defense Methodology for an Organization, Ver. 1.0, Prime Minister’s Office National Cyber Directorate, National Cyber Security Authority (June 2017), https://www.gov.il/BlobFolder/policy/cyber_security_methodology_for_organizations/he/Cyber1.0_english_617_A4.pdf.

[25] Cybersecurity’s Framework Success Story: Israeli National Cyber Directorate, NIST https://www.nist.gov/system/files/documents/2020/07/23/Israeli%20National%20Cyber%20Directorate%20Success%20Story%20062920%20508.pdf.

[26] *A National Cybersecurity Framework*, National Cyber Security Framework, https://www.cybersecurityframework.it/en (last visited Feb. 28, 2023); *see also* Macro Angelini et al, *Italian National Framework for Cybersecurity and Data Protection*, 12121 Privacy Technologies 127 (2020), https://link.springer.com/chapter/10.1007/978-3-030-55196-4_8.

organizations in Italy are subject to monetary penalties for failing to adopt the framework.[27]

- Japan’s Ministry of Economy, Trade and Industry developed *The Cyber/Physical Security Framework*, which is built on the CSF and includes a comprehensive mapping to CSF 1.1.[28]

- The Japanese Cross-Sector Forum, which consists of major CI companies from across Japanese industries, has used the CSF to create “a shared language among different industry sectors and facilitate[] our comprehensive discussions between member companies in Japan and their subsidiaries outside Japan.”[29]

- The Ontario Energy Board (“OEB”) adapted the CSF into its *Cyber Security Framework*, which “is used as the common basis for assessing and reporting capability to the OEB.”[30]

- Scotland’s *Safe, Secure and Prosperous: A Cyber Resilience Strategy for Scotland* is based on the CSF and outlines actions designed to enhance the cyber resilience of the Scottish government.[31]

- The United Kingdom’s (“UK”) *Minimum Cybersecurity Standard*, which UK government departments are required to implement, takes the CSF into account and adopts the five CSF functions.[32]

[27] *Journey to the NIST Cybersecurity Framework (CSF) 2.0 | Workshop #2*, NIST, https://www.nist.gov/news-events/events/2023/02/journey-nist-cybersecurity-framework-csf-20-workshop-2 (last updated Feb. 28, 2023) (statement by panelist Luca Montanari at 36:35-37:30 of Panel #2 video).

[28] The Cyber/Physical Security Framework, Version 1.0, Cyber Security Division Commerce and Information Policy Bureau Ministry of Economy, Trade and Industry, at 10, Appendix 3 (Apr. 18, 2019), https://www.meti.go.jp/english/press/2019/pdf/0418_001b.pdf.

[29] *Success Story: Japanese Cross-Sector Forum*, NIST, https://www nist.gov/cyberframework/success-stories/japanese-cross-sector-forum (last updated Dec. 8, 2021).

[30] *Cybersecurity Framework: International Resources*, NIST, https://www.nist.gov/cyberframework/international-resources (last updated Nov. 9, 2022); Ontario Cyber Security Framework, Version 1.0 (Dec. 6, 2017), https://www.oeb.ca/sites/default/files/Ontario-Cyber-Security-Framework-20171206.pdf.

[31] *Cybersecurity Framework: International Resources*, NIST, https://www.nist.gov/cyberframework/international-resources (last updated Nov. 9, 2022); *Cyber resilience: public sector action plan 2017-2018*, Scottish Government (Nov. 8, 2017), https://www.gov.scot/publications/cyber-resilience-strategy-scotland-public-sector-action-plan-2017-18/.

[32] *Guidance: Minimum Cyber Security Standard*, GOV.UK (June 25, 2018), https://www.gov.uk/government/publications/the-minimum-cyber-security-standard; NIST Cybersecurity Framework (CSF): A comprehensive approach to cybersecurity, at 9 (2019), https://www.oas.org/en/sms/cicte/docs/OAS-AWS-NIST-Cybersecurity-Framework(CSF)-ENG.pdf.

- Uruguay's Agency for the Development of Electronic Government and Information Society and Knowledge adapted the CSF to create its own *Cybersecurity Framework*.[33]

As NIST notes in the Concept Paper,[34] the CSF has had a significant influence on security guidance documents published by the International Organization for Standardization ("ISO"), such as the ISO/IEC 27000 series on information security[35] and the ISO/IEC 31000 series on risk management.[36] The breadth of the CSF's international reach cannot be understated and must be considered as NIST evaluates updates that could disrupt the CSF Core.

Private Sector Resources. There are countless private sector applications of the CSF, including tools, consulting programs, and evaluations that are built on the CSF.[37] Private organizations have used those services and may be in the midst of various organizational change programs to move from one Tier to another or to better make use of the CSF. Also included within these resources are the many products and services that use the CSF as an input, such as the following offerings by CTIA member companies:

[33] *Cybersecurity Framework: International Resources*, NIST, https://www.nist.gov/cyberframework/international-resources (last updated Nov. 9, 2022); *Marco de Ciberseguridad*, gub.uy (Dec. 12, 2022), https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/marco-ciberseguridad.

[34] Concept Paper at 5.

[35] *ISO/IEC 27001 and related standards: Information security management*, ISO, https://www.iso.org/isoiec-27001-information-security.html (last visited Feb. 28, 2023).

[36] *ISO 31000: Risk management*, ISO, https://www.iso.org/iso-31000-risk-management html (last visited Feb. 28, 2023).

[37] *See, e.g.*, Deloitte's NIST capabilities: Helping you to adopt NIST frameworks, Deloitte, https://www2.deloitte.com/us/en/pages/advisory/articles/nist-compliance html (last visited Feb. 28, 2023); NIST Cybersecurity Framework Gap Analysis: Identify Security Weaknesses in Your Critical Infrastructure, Cylance Consulting, https://www.blackberry.com/content/dam/bbcomv4/blackberry-com/en/services/strategic-services/EU_NIST_Gap_Analysis_Datasheet.pdf; *A common ground guidance for cybersecurity risk management*, Kyber Security, https://kybersecure.com/nist-csf/ (last visited Feb. 28, 2023).

- Amazon Web Services offers different cloud-based service offerings that align to the CSF.[38]

- AT&T's AlienVault USM Anywhere,[39] a cloud-based security management solution, combines essential security capabilities into a single platform to accelerate an organization's adoption of the CSF.[40]

- Cisco has numerous solutions that draw on the CSF's Core.[41] For example, Cisco Cloudlock, a cloud cybersecurity platform, "helps organizations implement the functions, categories and subcategories of the [CSF]."[42]

- Ericsson's Security Manager, a security management automation solution, draws on CSF principles.[43]

- Proofpoint provides a number of different products and services that align to the CSF, including its Targeted Attack Protection that detects email attacks and threats to cloud apps.[44]

In addition to these resources, organizations use the CSF to provide a common language for individuals in an organization—from subject matter experts to C-suite executives—to communicate about enterprise cybersecurity challenges and solutions. CSF 1.1 states that the

[38] NIST Cybersecurity Framework (CSF): Aligning to the NIST CSF in the AWS Cloud, Amazon, https://d1.awsstatic.com/whitepapers/compliance/NIST_Cybersecurity_Framework_CSF.pdf (last updated Oct. 2021).

[39] *USM Anywhere*, AT&T, https://cybersecurity.att.com/products/usm-anywhere (last visited Feb. 28, 2023).

[40] *NIST Cybersecurity Framework Compliance with AlienVault USM Anywhere*, AT&T, https://cybersecurity.att.com/resource-center/solution-briefs/nist-compliance-usm-anywhere (last visited Feb. 28, 2023).

[41] Pranav Kumar, *Cisco Secure: Supporting NIST Cybersecurity Framework*, Cisco Blogs (June 18, 2021), https://blogs.cisco.com/security/cisco-secure-supporting-nist-cybersecurity-framework.

[42] *Cisco Cloudlock: NIST Cybersecurity Framework for Cloud Applications*, CISCO, https://learn-cloudsecurity.cisco.com/umbrella-resources/umbrella/nist-compliance-guide-2#page=1 (last visited Feb. 28, 2023).

[43] *See* Kari-Pekka Perttula, *Your guide to end-to-end security when introducing 5G core*, Ericsson (Dec. 3, 2020), https://www.ericsson.com/en/blog/2020/10/how-to-master-e2e-network-security-when-introducing-5g-core.

[44] How Proofpoint Helps Organizations Meet NIST Cybersecurity Guidelines, Proofpoint, https://www.proofpoint.com/sites/default/files/pfpt-us-ds-how-proofpoint-helps-organizations-meet-nist-cybersecurity.pdf (last visited Apr. 12, 2022).

CSF "provides a common taxonomy and mechanism for organizations to . . . [c]ommunicate among internal and external stakeholders about cybersecurity risk."[45]

Fundamentally, the CSF is a guide for organizations' enterprise cyber risk management. NIST should protect that uniquely beneficial function even as it expands the CSF beyond CI. The CSF is not a guide for product development or service offerings, but is an effective tool for organizations to use to assess, build, and mature their organizational approaches to cybersecurity risk. NIST must keep this foundational purpose top-of-mind as it develops CSF 2.0.

C. Any Changes to the CSF Will Have Significant Ripple Effects—Within Organizations and Throughout the Broader Cybersecurity Ecosystem.

Given the breadth of the CSF's influence and its relationship to modern cybersecurity initiatives, any changes the CSF's Core will have significant impacts. For example, organizations that have used the CSF to inform their own cybersecurity programs will have to update internal assessments and programs, including updating organizational profiles and mappings. These activities are time consuming and costly, and may be particularly burdensome for small and mid-sized organizations. Many organizations may be in the midst of moving from one Tier to another, or otherwise maturing their programs, making it disruptive to substantially change the baseline. This may discourage or delay use of CSF 2.0. Across the broader ecosystem, documents and guidance that relies on or maps to the CSF will need to be updated. As illustrated above, this will be a massive task across the federal government and internationally. For these reasons, NIST must account for significant problems that are likely to

[45] Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, NIST, at 2, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (Apr. 16, 2018) ("CSF 1.1").

arise with respect to backward compatibility from "[p]otential [s]ignificant [u]pdates" to the CSF, particularly with respect to the CSF Core.[46]

Further, the CSF's widespread influence on cybersecurity also counsels in favor of NIST aiming to provide for predictable and fixed releases of future updates to the CSF. Stakeholders would benefit from having more clarity about the cadence of future CSF updates so that they can plan accordingly. With that said, NIST must take care not to update the CSF's core elements too frequently. Frequent updates to the CSF itself are not needed given the utility of CSF profiles, NIST interagency reports ("NISTIR"), and other guidance and tools from NIST, other agencies, and third parties.

NIST and SRMAs may find it helpful to work with particular sectors and small and midsized businesses to develop guidance or profiles to apply the CSF in various settings, or to address more robustly issues such as SCRM, governance, applications to operational technology, or product development. But the CSF itself cannot do everything, and it should not be expected to be updated to meet every new threat or sector-specific need.

III. NIST SHOULD ADOPT ASPECTS OF THE CONCEPT PAPER THAT ARE GROUNDED IN FLEXIBILITY AND WILL PROMOTE BROAD ADOPTION OF THE CSF.

A. Maintaining the CSF's Current Level of Detail and Specificity Will Best Promote Flexibility and Widespread Use of the CSF.

In the Concept Paper, NIST proposes that it will "maintain the current level of detail and specificity in CSF 2.0 to ensure it remains scalable and flexible for a wide range of organizations."[47] CTIA supports this approach.

[46] Concept Paper at 1.

[47] Concept Paper at 5.

Flexibility is an indispensable characteristic of the CSF. Given the multi-faceted, nuanced, and dynamic nature of cybersecurity, there are no “one-size-fits-all” solutions. Determinations about which cybersecurity solutions to adopt are complex and involve risk, resource, and threat assessment considerations that are often unique to each individual organization. NIST recognizes the importance of flexible cybersecurity guidance and has designed the CSF to allow organizations to “customize practices described in the [CSF],” “determine activities that are important to critical service delivery,” and “prioritize investments to maximize the impact of each dollar spent.”[48]

This dynamic has led CSF stakeholders to make clear to NIST that the CSF’s “key attributes – including its flexible, simple, and easy-to-use nature – have been beneficial for implementation by organizations of varying sizes, types, and sectors.”[49] NIST should heed stakeholder consensus on this issue and ensure that CSF 2.0 remains simple and flexible to account for the variable nature of cybersecurity and the many different organizations that seek to implement the CSF.

NIST states that CSF 2.0 “will include notional implementation examples of concise, action-oriented processes and activities to help achieve the outcomes of the CSF Subcategories. . . .”[50] CTIA supports this approach and believes that notional implementation examples are an effective way of providing more detail on certain topics while still maintaining the CSF’s structure and flexibility and not disrupting the CSF Core. For example:

- ***Intra-organizational communication***. As described above, the CSF is designed to provide a common taxonomy and mechanism for individuals within an

[48] CSF 1.1 at 2.

[49] Concept Paper at 5.

[50] *Id.* at 8.

organization to discuss cybersecurity.[51] NIST can bolster the CSF's utility as an intra-organizational communication tool by providing notional examples of how an organization can use the CSF to communicate with internal stakeholders about cybersecurity risk.

- ***Benchmarking***. While NIST should adopt its plan to provide substantive measurement guidance in 800-55 Rev. 2 as opposed to the CSF, as discussed below, NIST could provide notional implementation examples of how the CSF can be leveraged to assist an organization with benchmarking its implementation of the CSF.

As NIST continues its work on CSF 2.0, it should take care to maintain the CSF's simplicity and flexibility, while also identifying areas in which notional implementation examples could provide value to CSF stakeholders.

B. NIST Should Retain the CSF's Process-Oriented Approach for Enterprises, Including by Keeping It Technology- and Threat-Agnostic.

In the Concept Paper, NIST announces that "CSF 2.0 will remain technology- and vendor-neutral."[52] CTIA supports this approach and urges NIST to ensure that the CSF remains threat-agnostic.

Despite significant changes in the threat landscape since NIST first published the CSF in 2014, the CSF remains a staple of cybersecurity guidance both domestically and internationally for a wide range of business models and approaches to cybersecurity. The CSF has withstood the test of time in large part due to its process-oriented nature. Rather than seeking to explicitly address specific technologies or threats, the CSF focuses on processes that can universally promote positive cybersecurity outcomes, no matter the specific technology or threat at issue. The CSF is not designed to explicitly address every possible cybersecurity threat, and NIST should not attempt to do so now. Just as redesigning the CSF to address specific technologies or

[51] CSF 1.1 at 2.

[52] Concept Paper at 7.

vendors could "jeopardiz[e] the broad applicability of the CSF,"[53] so too could redesigning the CSF to address current threats, given the quickly evolving nature of the cyber threat landscape.

Organizations seeking more detailed guidance on how to achieve CSF outcomes in light of specific technologies or threats can avail themselves of other resources that apply the CSF to specific scenarios. NIST and other organizations have led in mappings and applications of the CSF, and can continue to do so for specific contexts. For example, NIST has published NISTIR 8374, *Ransomware Risk Management: A Cybersecurity Framework Profile*, which applies CSF objectives to the threat of ransomware and informs how an organization can leverage the CSF to address ransomware-specific issues.[54] This approach satisfies the desire from certain organizations for more detailed guidance without turning the CSF into a laundry list of cybersecurity threats that happen to be top-of-mind at the time that CSF 2.0 is published.

CSF profiles are not the only NIST documents that can inform specific applications of the CSF. As NIST notes in the Concept Paper, the NCCoE recently published a new Volume E of its Draft SP 1800-35 Practice Guide, *Implementing a Zero Trust Architecture*, which provides "an initial mapping between [Zero Trust Architecture] characteristics and the CSF."[55] NCCoE Practice Guides are important resources that organizations can use as they work to achieve CSF outcomes through specific security principles and technologies,

Likewise, the CSF should remain a tool for enterprises to address cybersecurity. As the cybersecurity ecosystem evolves, there will be a need for additional, complementary tools for

[53] *Id.*

[54] NISTIR 8374, Ransomware Risk Management: A Cybersecurity Framework Profile, NIST (Feb. 2022), https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8374.pdf.

[55] Concept Paper at 7; NIST SP 1800-35E, Implementing a Zero Trust Architecture, Volumen E: Risk and Compliance Management, at 9-26 (Dec 2022), https://www.nccoe.nist.gov/sites/default/files/2022-12/zta-nist-sp-1800-35e-preliminary-draft.pdf.

product-level cybersecurity frameworks, but the CSF is not the right vehicle for those approaches. Maintaining the CSF as an enterprise tool is critical to its continuity and continued relevance.

C. NIST Should Emphasize the CSF's Voluntary Nature and Make Clear that It Is Not Designed To Be a Template or Basis for Regulation.

Some stakeholders may seek to turn the CSF into a tool to harness emerging regulatory obligations, or they may want to expand the CSF to be so robust that it staves off future emerging regulation. The CSF is not a vessel for regulation, nor it is a proxy for regulation. Diverse sectors and organizations face myriad existing and potential regulations that may touch on topics addressed in the CSF. The threat of regulation should not distort the role and utility of the CSF as NIST moves to version 2.0. NIST should retain the CSF's voluntary nature and resist any impulse or urging to transform the CSF into quasi-regulation or a proxy for regulation.

To that end, NIST should make clear that any changes it makes to the CSF are not intended to make the document more prescriptive or turn it into a template or basis for regulation. As NIST has made clear time and again, the CSF is a *voluntary* guidance document.[56] Indeed, a NIST official stated during NIST's *Journey to the NIST Cybersecurity Framework (CSF) 2.0 Workshop #1* last year that, "from the NIST perspective, the CSF is voluntary. It will always be voluntary for us. . . . It is important to maintain it as voluntary. I think we have seen a lot of success in that approach."[57]

Other federal agencies have noted the benefits of NIST's voluntary, flexible approach and urged organizations to adopt the CSF. The FTC has stated that the CSF "is not, and isn't

[56] *E.g.*, CSF 1.1 at v.

[57] *Journey to the NIST Cybersecurity Framework (CSF) 2.0 | Workshop #1*, NIST, https://www.nist.gov/news-events/events/2022/08/journey-nist-cybersecurity-framework-csf-20-workshop-1 (last updated Sept. 8, 2022)(statement by NIST's Adam Sedgewick at 44:59-45:32 of Panel #1 video).

intended to be, a standard or checklist;"[58] rather, it "gives [your] business an outline of best practices to help you decide where to focus your time and money for cybersecurity protection."[59] As a result of this flexible nature, the FTC asserts that "[t]he [CSF]'s five Core functions can serve as a model for companies of all sizes to conduct risk assessments and mitigation."[60] Following the release of CSF 1.1, the Department of Homeland Security's ("DHS") Cybersecurity and Infrastructure Security Agency ("CISA") recommended that Chemical Sector organizations adopt the CSF, stating that "[e]arly adoption of the [CSF]'s principles may better position Chemical Sector organizations to receive additional potential benefits in the future."[61] Further, the Treasury Department has touted the benefits of the CSF's flexibility, stating that "[f]or larger firms with already robust cyber risk management, [the CSF] can serve to highlight specific best practices and standards that might be used," while "[s]maller institutions may use the [CSF] to better understand their risk profile and establish protocols for ensuring proper controls are in place to meet that profile."[62]

Regulators across the government recognize the utility of the CSF as a tool. It may not address every regulatory issue in every sector, but it was not designed to do so and should not be

[58] Andrea Arias, *The NIST Cybersecurity Framework and the FTC*, FTC (Aug. 31, 2016), https://www.ftc.gov/business-guidance/blog/2016/08/nist-cybersecurity-framework-and-ftc.

[59] Cybersecurity for Small Business: Understanding the NIST Cybersecurity Framework, https://www.ftc.gov/system/files/attachments/understanding-nist-cybersecurity-framework/cybersecurity_sb_nist-cyber-framework.pdf.

[60] Andrea Arias, *The NIST Cybersecurity Framework and the FTC*, FTC (Aug. 31, 2016), https://www.ftc.gov/business-guidance/blog/2016/08/nist-cybersecurity-framework-and-ftc.

[61] Chemical Sector Cybersecurity: Framework Implementation Guidance, at 4 (May 2020), https://www.cisa.gov/sites/default/files/publications/Chemical_Sector_Cybersecurity_Framework_Implementation_Guidance_FINAL_508.pdf.

[62] *What they're saying about the cybersecurity framework*, Federal News Network (Feb. 13, 2014), https://federalnewsnetwork.com/technology-main/2014/02/what-theyre-saying-about-the-cybersecurity-framework/.

used in that way. NIST should continue to emphasize that the CSF is purely voluntary and, further, that it is not intended to be a template for regulation.

IV. AS NIST CONSIDERS INTEGRATING GOVERNANCE GUIDANCE INTO THE CSF, IT SHOULD BE CAREFUL TO DO SO IN A WAY THAT PRESERVES BACKWARD COMPATIBILITY AND ENSURES THE GUIDANCE CAN BE APPLIED FLEXIBLY TO A WIDE RANGE OF ORGANIZATIONAL STRUCTURES.

A. The Wireless Industry Prioritizes Cyber Governance.

CTIA member companies prioritize cyber governance. The wireless industry is meeting market demands by exercising prudent cyber governance for themselves and by offering tools and support that companies across the economy can procure. For example, with respect to CTIA members' diverse organizations:

- The AT&T Board Audit Committee oversees the company's risk management strategy, which includes cybersecurity and network defense.[63]

- Qualcomm[64] and Verizon[65] assign a cyber governance role to its board's Audit Committee (in addition to dedicated executives).

- T-Mobile notes that "strong oversight and governance controls," combined with "technical and physical safeguards," are part of its data security program.[66]

[63] *AT&T Issue Briefs: Network & Data Security*, AT&T, https://about.att.com/csr/home/reporting/issue-brief/network-data-security.html (last visited Feb. 6, 2023)

[64] *Privacy and Security*, Qualcomm, https://www.qualcomm.com/company/corporate-responsibility/responsible-business/privacy-security (last visited Feb. 6, 2023).

[65] *Audit Committee Key Responsibilities*, Verizon, https://www.verizon.com/about/investors/corporate-governance/audit-committee-key-responsibilities (last visited Feb. 27, 2023) ("Assess and discuss with management Verizon's significant business risk exposures (including those related to cybersecurity, data privacy, [and] data security . . . .)").

[66] 2021 Corporate Responsibility Report, T-Mobile, at 22 (2021), https://www.t-mobile.com/content/dam/t-mobile/ntm/specific-use/annual-report/TMobile_CSR21_16822_tagged.pdf?icid=MGPO_TMO_U_TMOCPSOCRS_OSKYG8OK2Z6QJZS9V30948 at 22.

Beyond these internal governance procedures, numerous professional services firms, including AT&T,[67] offer cybersecurity risk management consulting services. These internal policies and external business offerings that promote cybersecurity governance are tailored to individual organization needs.

B. Addressing Governance in the CSF Tiers and the Existing CSF Functions Will Best Promote Governance While Maintaining Backward Compatibility.

Governance was discussed at some length in the recent February Working Sessions.[68] There appear to be varied views on the proper treatment of governance in a revised CSF. NIST can address governance in a CSF update, but it is not timely to create an entirely new "Function" for governance, which is already addressed in several parts of the existing Core.[69] Arguably, the entire CSF is a governance tool that helps enterprises address and mange cyber risk, but if NIST wants to emphasize governance more explicitly it has several alternatives.

CTIA recognizes the value of integrating governance into the CSF, and recommends that NIST do so by addressing governance in the Tiers. Specifically, NIST should address governance in the CSF 2.0's definitions of Tiers, providing flexible indicia on what elements of cybersecurity governance make an organization more likely to be in a particular Tier. This approach would allow NIST to promote cybersecurity governance and "highlight that cybersecurity governance is critical to managing and reducing cybersecurity risk,"[70] without making wholesale changes to the CSF Core. This is critical, as it will allow the CSF to maintain

[67] *E.g.*, *Cybersecurity consulting services*, ATT, https://www.business.att.com/categories/cybersecurity-consulting-services.html (last visited Feb. 28, 2023).

[68] *Journey to the NIST Cybersecurity Framework (CSF) 2.0 | In-Person Working Sessions*, NIST, https://www.nist.gov/news-events/events/2023/02/journey-nist-cybersecurity-framework-csf-20-person-working-sessions (last updated Feb. 16, 2023).

[69] *See, e.g.*, CSF 1.1 at 23 (listing ID.GV ("Governance") and ID.RA ("Risk Assessment"), each of which has several associated subcategories); *see id.* at 19 (discussing "[g]overnance of cybersecurity risk").

[70] Concept Paper at 10.

its backward compatibility and avoid the significant negative downstream effects that could result from making such drastic changes to the structure and content of the CSF Core. On the other hand, creating a separate Govern Function, as NIST contemplates, may have significant negative impacts on the CSF's backward compatibility. NIST must seriously weigh the negative impacts that this could create against any benefits.

Further, integrating governance issues into the Tiers would allow NIST to achieve its goal of "promot[ing] alignment of cybersecurity activities with enterprise risks and legal requirements" while also ensuring that the CSF Core is focused on cybersecurity-specific outcomes rather than broader enterprise risk management issues.[71] Given that organizations can leverage the RMF for broader enterprise risk management guidance, it is important that NIST maintain the CSF Core's focus on security.

In addition to addressing governance in the Tiers, NIST could add governance-specific considerations throughout the existing CSF Core. It could do this by: (1) noting throughout the document that governance can support each of the CSF functions, and may promote particular outcomes; (2) adding additional subcategories to existing functions, such as in ID.GV and ID.RA; and (3) adding governance-specific Informative References throughout the Core. These Informative References will allow organizations to leverage leading cyber governance guidance as part of their efforts to implement the CSF. Indeed, the fact that each existing function has governance aspects counsels in favor of this type of approach instead of creating a Govern Function, as "Govern" is differently positioned than other Functions, which are not as broad.

NIST could also address governance in the current seven step illustration in Section 3.2 of how an organization could use the CSF. It could, for example, note that an organization may

[71] *Id.*

make choices about how to use the CSF that may be subject to various kinds of internal oversight and validation. This approach would still allow NIST to provide governance guidance without disrupting the Core. Were NIST to create a sixth function for Governance, it might be inclined to move Subcategories and other considerations relevant to governance into a new Govern Function. This may duplicate considerations and functions and confuse users of the CSF.

In short, NIST can integrate governance issues into the CSF, as it has done in other documents,[72] without disrupting the longstanding and existing structure of the Core, as well as the multitude of cyber tools and guidance documents that are built off of it.

C. It Is Essential That Any Governance Guidance in CSF 2.0 Is Sufficiently Flexible to Account for Diverse Organizational Structures.

No matter how NIST decides to incorporate governance guidance into CSF 2.0, it is absolutely critical that NIST do so flexibly.

Corporate and organizational governance and risk management structures in the United States have tremendous diversity. Consider, for example, the difference between (1) a large, multinational publicly traded financial services company with significant cybersecurity business risk, and (2) a small government contractor in the manufacturing sector. These organizations will have vastly different corporate structures, and any governance guidance will need to be sufficiently flexible and high-level to be applicable and workable for both types of organizations. As another example, educational institutions and non-profits may have relatively simple organization structures, or they may have enormous institutional capabilities. In recognition of this inherent diversity, the international standard on social responsibility, ISO 26000, defines organizational governance as "a system by which an organization makes and implements

[72] *See* AI RMF 1.0 at 21-24.

decisions in pursuit of its objectives. Governance systems include management processes designed to deliver on performance objectives while considering stakeholder interests."[73]

There is no one "right" way to address organizational governance, nor is there one single approach to cyber risk management. As CTIA has long explained, cyber risk management is a "team sport" that will require various combinations of information technology, third party risk management, human resources, legal services, physical security, and more. Governance guidance must avoid prescribing, or appearing to prescribe, the structure, composition, or selection of corporate governance organization, processes, or personnel. There are myriad successful governance models, and CSF 2.0 must be flexible enough to account for all of them.

Any governance guidance in CSF 2.0 should look to encourage CSF users to identify what is unique to cybersecurity governance, as compared with risk management generally. Cybersecurity risk is just one of many enterprise-wide risks that organizations manage.
To that end, NIST should make clear how any governance guidance in CSF 2.0 interacts with the RMF, which is designed to address general enterprise risk management issues. NIST should also carefully review the proposals from the Securities and Exchange Commission ("SEC"),[74] as well as guidance from the FTC[75] and third-party associations that address aspects of governance, in order to assess the complexity of these issues and the tradeoffs that attend various governance proposals. For example, as CTIA and numerous other commenters explained to the SEC, mandates about particular roles or expertise expected of a Board of Directors would encroach on

[73] *What is Organizational or Corporate Governance?*, ASQ https://asq.org/quality-resources/governance (last visited Feb. 28, 2023).

[74] *Proposed Rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, SEC, 87 Fed. Reg. 16,590 (Mar. 23, 2022), https://www.govinfo.gov/content/pkg/FR-2022-03-23/pdf/2022-05480.pdf.

[75] Jared Ho, *Corporate boards: Don't underestimate your role in data security oversight*, FTC (Apr. 28, 2021), https://www.ftc.gov/business-guidance/blog/2021/04/corporate-boards-dont-underestimate-your-role-data-security-oversight.

corporate governance decisions best left to senior management, directors and shareholders.[76] NIST, having lengthy experience working with federal agencies that have unique oversight and mandates, may need to treat governance as a separate workstream about which it can learn more.

V. C-SCRM SHOULD BE TREATED WITH A LIGHT TOUCH IN CSF 2.0, CONSISTENT WITH NIST'S PAST APPROACH AND RECOGNIZING MYRIAD ONGOING FEDERAL SUPPLY CHAIN EFFORTS.

A. C-SCRM Is Being Actively Addressed in Many Efforts Across the Federal Landscape.

C-SCRM is an important and complex issue facing organizations across the U.S. economy, who are working to increase their capabilities, better assess risks, and meet the changing landscape of domestic policy. Since CSF 1.1 was published in 2018, myriad federal proceedings have addressed SCRM issues. While there is no one settled approach or set of considerations, examples of evolving approaches and best practices include the following:

- The FCC has issued several orders to address information and communications technology ("ICT") supply chain integrity by prohibiting the use of federal universal service funds for "covered" communications equipment and services provided by entities that pose a threat to national security.[77] Last year, in response to direction from Congress in the Secure Equipment Act of 2021, the FCC adopted rules prohibiting the authorization of "covered" equipment.[78] The FCC is currently seeking comment on several outstanding issues.[79]

- The DHS ICT SCRM Task Force—a public-private partnership that CTIA and several member companies support—has been addressing cyber threats to ICT supply chains through a "collective defense approach . . . bringing together

[76] *E.g.*, Comments of CTIA, SEC File No. S7–09–22 (filed May 9, 2022), https://www.sec.gov/comments/s7-09-22/s70922-20128384-291287.pdf.

[77] *See, e.g. Proposed Rule on Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, FCC, 86 Fed. Reg. 15,165 (Mar. 22, 2021), https://www.govinfo.gov/content/pkg/FR-2021-03-22/pdf/2021-04692.pdf (implementing a reimbursement program to expedite removal of harmful equipment and services).

[78] Report and Order, Order, and Further Notice of Proposed Rulemaking, ET Docket No. 21-232, EA Docket No. 21-233, at ¶ 1 (rel. Nov. 25, 2022), https://docs.fcc.gov/public/attachments/FCC-22-84A1.pdf.

[79] *Id.* at ¶¶ 267-332 (outstanding issues include: components parts, modules, and composite systems; revocations of existing authorizations for covered equipment; and competitive bidding certifications, among others).

industry and government to identify challenges and devise workable solutions."[80] This Task Force has issued numerous reports, as noted below.

- In 2020, NIST updated SP 800-53, *Security and Privacy Controls for Information Systems and Organizations* to, among other things, establish a new SCRM control family.[81]

- Congress enacted "section 889" in the National Defense Authorization Act for Fiscal Year 2019, addressing the equipment of certain Chinese companies in the ICT and government contractor supply chain.[82] The Federal Acquisition Security Council is developing supply chain information sharing criteria and recommending exclusion or removal orders related to federal procurement, among other responsibilities.[83]

- The Department of Commerce issued an interim final rule on review of information and communication technology and services transactions and is also working on an advance licensing process for the same.[84] It has also taken various actions with respect to the Export Administration Regulations that are targeted at the semiconductor industry.[85]

- President Biden signed Executive Order 14028, *Improving the Nation's Cybersecurity* ("Cyber EO"), which directed several federal agencies to launch initiatives designed to improve the security and integrity of the software supply chain.[86] Pursuant to the Cyber EO, the National Telecommunication and Information Administration published the minimum elements for a Software Bill

[80] Press Release, CISA, DHS And Private Sector Partners Establish Information And Communications Technology Supply Chain Risk Management Task Force, CISA, https://www.cisa.gov/news/2018/10/30/dhs-and-private-sector-partners-establish-information-and-communications-technology (last updated Feb. 5, 2021).

[81] SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations, NIST (Sept. 2020), https://csrc nist.gov/publications/detail/sp/800-53/rev-5/final ("800-53 Webpage").

[82] 41 U.S.C.A. § Subt. I, D. C, Ch. 39, Refs & Annos.

[83] *See, e.g. Interim Final Rule with Request for Comments on Federal Acquisition Supply Chain Security Act*, OMB, 85 Fed. Reg. 54,263 (Sept. 1, 2020), https://www.govinfo.gov/content/pkg/FR-2020-09-01/pdf/2020-18939.pdf.

[84] *Interim Final Rule with Request of Comments on Securing the Information and Communications Technology and Services Supply Chain*, Dep't of Commerce, 86 Fed. Reg. 4,909 (Jan. 19, 2021), https://www.govinfo.gov/content/pkg/FR-2021-01-19/pdf/2021-01234.pdf; *Advanced Notice of Proposed Rulemaking on Securing the Information and Communications Technology and Services Supply Chain: Licensing Procedures*, Dep't of Commerce, 86 Fed. Reg. 16,312 (Mar. 29, 2021), https://www.govinfo.gov/content/pkg/FR-2021-03-29/pdf/2021-06529.pdf.

[85] *E.g., Implementation of Additional Export Controls: Certain Advanced Computing and Semiconductor Manufacturing Items; Supercomputer and Semiconductor End Use; Entity List Modification*, Department of Commerce, Bureau of Industry and Security, 87 Fed. Reg. 62,186 (Oct. 13, 2022), https://www.govinfo.gov/content/pkg/FR-2022-10-13/pdf/2022-21658.pdf.

[86] *See* Exec. Order No. 14028, *Improving the Nation's Cybersecurity*, 86 Fed. Reg. 26,633, 26,637-41 (May 12, 2021), https://www.govinfo.gov/content/pkg/FR-2021-05-17/pdf/2021-10460.pdf.

of Materials[87] while NIST issued SP 800-218, *Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities* ("SSDF"),[88] among other software supply chain guidance documents.[89]

- President Biden signed Executive Order 14017, *America's Supply Chains*, which launched several initiatives to strengthen America's supply chains. The White House issued a 100-day Supply Chain Review report of critical industries[90] and several agencies issued reports and devised strategies,[91] including one report dedicated to the ICT industrial base.[92]

- Last year, the White House announced additional actions to build resilience across critical supply chains, including: (1) launching a new domestic manufacturing initiative through the Export-Import Bank; (2) hosting roundtables focused on scaling innovative technologies, promoting sector-based regional workforce initiatives, partnering with unions, and supporting small- and medium-sized suppliers; (3) releasing funding opportunities related to different Infrastructure Investment and Jobs Act grant programs; and (4) issuing a new Buy American rule to create a new category of critical products that will be eligible for enhanced price preferences.[93]

- In the National Defense Authorization Act for Fiscal Year 2023, Congress prohibited federal agencies from: (1) procuring, obtaining, or contracting for any

[87] The Minimum Elements For a Software Bill of Materials (SBOM), NTIA (July 12, 2021), https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf.

[88] NIST SP 800-218, Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities, NIST (Feb. 2022), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf ("SSDF").

[89] Software Supply Chain Security Guidance Under Executive Order (EO) 14028 Section 4e, NIST (Feb. 4, 2022), https://www.nist.gov/system/files/documents/2022/02/04/software-supply-chain-security-guidance-under-EO-14028-section-4e.pdf; Software Security in Supply Chains, NIST (May 11, 2022), https://www.nist.gov/system/files/documents/2022/05/11/Guidance%20on%20Software%20Supply%20Chain%20Security_EO14028%20Sections%204c_4d%5B71%5D.pdf.

[90] Building Resilient Supply Chains, Revitalizing American Manufacturing, and Fostering Broad-based Growth: 100 Day Reviews under Executive Order 14017, The White House (June 2021), https://www.whitehouse.gov/wp-content/uploads/2021/06/100-day-supply-chain-review-report.pdf.

[91] *E.g.*, Securing Defense-Critical Supply Chains: An Action Plan Developed in Response to President Biden's Executive Order 14017, Dep't of Defense (Feb. 2022), https://media.defense.gov/2022/Feb/24/2002944158/-1/-1/1/DOD-EO-14017-REPORT-SECURING-DEFENSE-CRITICAL-SUPPLY-CHAINS.PDF.

[92] Assessment of the Critical Supply Chains Supporting the U.S Information and Communications Technology Industry, Dep't of Commerce and DHS (Feb. 24, 2022), https://www.commerce.gov/sites/default/files/2022-02/Assessment-Critical-Supply-Chains-Supporting-US-ICT-Industry.pdf.

[93] Press Release, The White House, The Biden-Harris Plan to Revitalize American Manufacturing and Secure Critical Supply Chains in 2022 (Feb. 24, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/02/24/the-biden-harris-plan-to-revitalize-american-manufacturing-and-secure-critical-supply-chains-in-2022/.

> electronic parts, products, or services that include semiconductor products or services produced by certain Chinese companies; and (2) contracting with an entity to procure or obtain electronic parts or products that use electronic parts or products that include semiconductor products or services produced by certain Chinese companies.[94] The FAR Council will issue regulations implementing these prohibitions, which will take effect in 2027.[95]

In addition to these C-SCRM initiatives, there are myriad SCRM guidance materials, many of which are built on the CSF. These include: (1) SP 800-161;[96] (2) NISTIR 8276, *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry*;[97] (3) NISTIR 8179, *Criticality Analysis Process Model: Prioritizing Systems and Components*;[98] (4) the SSDF;[99] (5) NIST's Project Description White Paper, *Validating the Integrity of Computing Devices: Supply Chain Assurance*;[100] and (6) numerous ICT SCRM Task Force publications.[101]

The landscape of federal C-SCRM initiatives and guidance is vast and reflects changing domestic policy and learning about experiences and best practices. When combined with the

[94] FY23 NDAA, H.R. 7776, 117th Cong. §§ 5949(a), (b), https://www.congress.gov/117/bills/hr7776/BILLS-117hr7776enr.pdf.

[95] *Id*. § 5949(c).

[96] NIST SP 800-161, Rev. 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, NIST, at 38, 49-50 (May 2022), https://nvlpubs nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf.

[97] NISTIR 8276, Key Practices in Cyber Supply Chain Risk Management: Observations from Industry, NIST, at 15, 19, 23-24 (Feb. 2021), https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8276.pdf.

[98] NISTIR 8179, Criticality Analysis Process Model: Prioritizing Systems and Components, NIST, at 20, 21, 23, 32 (Apr. 2018), https://nvlpubs nist.gov/nistpubs/ir/2018/NIST.IR.8179.pdf

[99] SSDF at 2, 5-19.

[100] Project Description, Validating the Integrity of Computing Devices: Supply Chain Assurance, NIST, at 13-14 (Mar. 2022), https://www nccoe nist.gov/sites/default/files/legacy-files/tpm-sca-project-description-final.pdf.

[101] *E.g.*, Information and Communications Technology Supply Chain Risk Management Task Force Year 2 Report: Status Update on Activities and Objectives of the Task Force, CISA, at 18 (Dec. 2020), https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force_year-two-report_508.pdf; Information and Communications Technology Supply Chain Risk Management Task Force: Threat Evaluation Working Group: Supplier, Products, and Services Threat Evaluation (to include Impact Analysis and Mitigation) Version 3.0, CISA, at 17-18, 98-100, 120, 122, 123, 125-28 (July 2021), https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force-threat-scenarios-report-v3.pdf; Mitigating ICT Supply Chain Risks With Qualified Bidder and Manufacturer Risks: Recommendations on the Use of Qualified Lists and Considerations for the Evaluation of Supply Chain Risks, CISA, at 10-12, 33 (Apr. 2021), https://www.cisa.gov/sites/default/files/publications/ICTSCRMTF_Qualified-Bidders-Lists_508.pdf.

complex and variable nature of C-SCRM, as described below, it becomes all the more important for NIST to proceed with caution on this topic in CSF 2.0.

B. C-SCRM Is Complex and Variable.

C-SCRM is complex, and many of the complexities do not apply universally across the private sector or even within CI sectors. Supply chains "encompass[] business functions and enterprises interconnected by resource flows of goods, services, information and funds," and supply chain management "spans these interconnected networks to acquire, produce and deliver goods and services in our global economy."[102] Securing such complex and interwoven systems without compromising interconnectivity is an inherently challenging process, and there are varying considerations and complexities depending on the context.

For example, certain C-SCRM complexities are common across many industrial sectors, such as the presence of legacy systems whose provenance may not be known or relevant and whose contracts may be difficult to amend, as well as software supply chain issues. Other complexities, however, are unique to certain sectors and organizations. For example, in the mobile ICT sector, there are significant differences between hardware and software sourcing. Although "[h]ardware specifications can be verified on delivery in most instances, . . . software functionality cannot . . . [and] may exhibit undesired behavior when confronted with conditions not considered during development . . . ."[103] All of these complexities make it challenging for the CSF to address supply chain and related third party issues, and suggest that updates to

[102] Brittain Ladd, *Tangled: Why Global Supply Chains Are So Complex*, Forbes (June 8, 2020), https://www.forbes.com/sites/forbescommunicationscouncil/2020/06/08/tangled-why-global-supply-chains-are-so-complex/?sh=2fce27e15bf5 (quoting C. John Langley, Managing Supply Chains: A Logistics Approach (2008)).

[103] Software Supply Chain Risk Management: From Products to Systems of Systems, Software Engineering Institute, Carnegie Mellon, at 1 (Dec. 2010), https://resources.sei.cmu.edu/asset_files/TechnicalNote/2010_004_001_15194.pdf.

Informative References or the creation of additional mappings and profiles may be most helpful to CSF users.

An added complexity is the fact that SCRM addresses many different activities and risks, beyond just cybersecurity. As NIST states in the RMF, an organization's SCRM policy supports numerous organizational policies beyond cybersecurity, including "acquisition and procurement," "privacy," "logistics," and "quality."[104] SCRM risks extend far beyond security and include issues such as "the insertion of counterfeits, unauthorized production, tampering, theft," and "poor manufacturing and development practices in the supply chain."[105] The ICT SCRM Task Force also addresses supply chain risks in a context that is much broader than just security. The Task Force's report on lessons learned from the COVID-19 pandemic focused on developing SCRM tools for availability purposes, in addition to security purposes. The Task Force concluded that customers need more visibility into upstream supply chain constraints such as single-source or single-region "junior-tier" suppliers, and advised that the ICT industry may benefit from "development of standardized mapping and other illumination tools."[106] In a separate report, the Task Force concluded that, in addition to introducing security risks, hardware components can introduce "economic risks" associated with untrusted or compromised components.[107]

[104] NIST SP 800-37, Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, NIST, at 20 (Dec. 2018), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf.

[105] *Id.* See also NISTIR 8286, Integrating Cybersecurity and Enterprise Risk Management (ERM), NIST, at 4 (Oct. 2020), https://nvlpubs nist.gov/nistpubs/ir/2020/NIST.IR.8286.pdf (stating that "[c]ybersecurity risk is one portion of the spectrum of an enterprise's core risks" and distinguishes cybersecurity risk from "other risk disciplines, such as safety, privacy, and *supply chains* that ultimately anchor in [enterprise risk management]." (emphasis added)).

[106] Building a More Resilient ICT Supply Chain: Lessons Learned During the COVID-19 Pandemic, CISA, at iii (Nov. 2020), https://www.cisa.gov/sites/default/files/publications/lessons-learned-during-covid-19-pandemic_508_2.pdf.

[107] Information and Communications Technology Supply Chain Risk Management Task Force: Threat Evaluation Working Group: Supplier, Products, and Services Threat Evaluation (to include Impact Analysis and Mitigation)

C. NIST Can Promote C-SCRM in CSF 2.0 by Expanding on Third Party Issues in Existing Subcategories and by Updating Informative References and Mappings—While Still Maintaining a Light Touch.

In light of the challenges to crafting universally applicable C-SCRM guidance, NIST used a light-touch approach to C-SCRM in CSF 1.1. Specifically, NIST: (1) expanded Section 3.3, *Communicating Cybersecurity Requirements with Stakeholders*, with the goal of helping stakeholders understand C-SCRM issues and its role "in addressing cybersecurity risk in [CI] and the broader digital economy;"[108] (2) highlighted in a new Section 3.4, *Buying Decisions*, the use of the CSF "in understanding risk associated with commercial off-the-shelf products and services;"[109] (3) incorporated C-SCRM into the Tiers;[110] and (4) added a SCRM Category and Subcategories to the Core.[111]

CTIA supports this light touch approach to C-SCRM in the CSF 1.1, and urges NIST to retain it in CSF 2.0, given the myriad of work on C-SCRM issues across the federal government and the numerous complexities, as detailed above. Accordingly, CTIA recommends that NIST eschew the options it outlines in the Concept Paper to "include additional C-SCRM-specific outcomes" to the CSF Core.[112] NIST should reject calls, such as were made at the February Working Sessions, to create a new C-SCRM "Function" or insert into the CSF a major expansion of C-SCRM expectations, and instead continue to take a targeted approach that respects ongoing

Version 3.0, CISA, at 18 (July 2021), https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force-threat-scenarios-report-v3.pdf

[108] CSF 1.1 at ii, 17.

[109] *Id.* at ii, 18.

[110] *Id.* at ii, 8-11.

[111] *Id.* at ii, 28-29.

[112] Concept Paper at 12. NIST states that options "may include" the following: (1) "further integrating C-SCRM outcomes throughout the CSF Core across Functions (integration may include supply chain separately or as a consideration as part of broader outcomes);" (2) "creation of a new Function focused on outcomes related to oversight and management of C-SCRM;" and (3) "expanding C-SCRM outcomes within the current ID.SC Category in the Identify Function." *Id.*

C-SCRM work. Given the complex and variable nature of C-SCRM, it will be immensely challenging to provide more detailed C-SCRM guidance that can be applied to the wide universe of CSF stakeholders. And given that C-SCRM activities must be understood within the much broader context of SCRM, providing substantially more granular C-SCRM expectations in CSF 2.0 would expand the CSF's scope beyond cybersecurity. Further, some of NIST's suggested options for addressing C-SCRM would require significant changes to the CSF Core. If NIST were to pursue one of these options, it would have significant negative downstream effects by hindering the backward compatibility of not only the CSF itself, but also the many different guidance documents that stem from the CSF.

Importantly, however, NIST can still promote C-SCRM and add value to the CSF's C-SCRM guidance—without creating the negative downstream effects that would result from disrupting the CSF Core—by updating its Informative References and mappings to reflect the most recent work on C-SCRM, both inside and outside of government. For example, NIST should: (1) reference SP 800-53 Rev. 5 in CSF 2.0, not SP 800-53 Rev. 4 as is provided in CSF 1.1;[113] (2) include a mapping between CSF 2.0 and SP 800-53 Rev. 5, similar to the mapping NIST has already created between SP 800-53 Rev. 5 and CSF 1.1;[114] and (3) update the ID.SC Informative References to include the SSDF, SP 800-161 Rev. 1, and other guidance documents developed by industry and government, such as those published by the ICT SCRM Task Force. NIST could also expand on third party issues in its existing supply chain discussions in the ID.SC section.

[113] CSF 1.1 at 24-44.

[114] NIST Cybersecurity Framework Version 1.1 to NIST Special Publication 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations, NIST https://csrc nist.gov/CSRC/media/Publications/sp/800-53/rev-5/final/documents/csf-pf-to-sp800-53r5-mappings.xlsx (last visited Feb. 28, 2023).

There may be areas for NIST to augment the current CSF to recognize C-SCRM issues, but any additions should minimize disruption and promote flexibility by modestly adjusting language in the CSF and using new material and resources as Informative References.

VI. NIST SHOULD PROVIDE SUBSTANTIVE MEASUREMENT AND ASSESSMENT GUIDANCE IN 800-55 REV. 2 RATHER THAN IN THE CSF.

In the Concept Paper, NIST states that "[t]he underlying fundamentals of cybersecurity measurement process and implementation will not be included in the CSF, but rather in [800-55 Rev. 2]."[115] CTIA supports this approach and urges NIST to provide a formal link between CSF 2.0 and 800-55 Rev. 2. CSF 1.1 already provides general guidance on the purpose of cyber measurement and the ways in which "the cybersecurity outcomes of the [CSF] Core support self-assessment of investment effectiveness and cybersecurity activities."[116] Attempting to update the CSF with more substantive measurement guidance than is already provided in CSF 1.1 would be a mistake.

Put simply, cyber measurement is complex and variable. There are many diverse use cases for metrics, which vary significantly between organizations based on sector and industry, size and resources, cyber maturity, and organizational goals, among other factors. As The MITRE Corporation has explained, an organization will need to consider its threat environment, operational needs, capabilities, and goals.[117] Between sectors, these differences are likely to be significant. Measurements that properly drive investment decisions for a rail operator may be very different from those that are relevant to a health care provider, financial services company,

[115] Concept Paper at 14.

[116] CSF 1.1 at 20.

[117] Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring: Enabling Systems Engineers and Program Managers to Select the Most Useful Assessment Methods, MITRE, at ix (Sept. 2018), https://www.mitre.org/sites/default/files/publications/pr-18-2579-cyber-resiliency-metrics-measures-of-effectiveness-and-scoring.pdf.

or internet service provider. Even within the same sector, companies of different sizes, goals, and levels of cyber maturity will need to use different measurements to inform investment decisions and cyber risk management. For a large company with disparate business offerings and objectives, optimal measures may vary between divisions of the company or between product and service offerings.

NIST is already proposing to tackle a number of other complex topics in the CSF, including governance, C-SCRM, and international alignment.[118] NIST need not further complicate CSF 2.0 by adding extensive guidance on cyber measurement. Further, providing substantive cyber measurement guidance in 800-55 Rev. 2 rather than CSF 2.0 will streamline NIST's cyber measurement guidance and avoid the fragmentation that would result if NIST provides substantive measurement guidance in both documents. This approach will thus facilitate ease of use for stakeholders and reduce the risk of public confusion.

VII. NIST SHOULD CONSIDER TARGETED UPDATES TO THE CSF THAT WILL IMPROVE ITS PRACTICAL IMPLEMENTATION AND CONTINUED RELEVANCE.

A. NIST Should Expand Its Discussion of CSF Tiers and Emphasize that the Tiers Are Not Intended To Be Used as a Maturity Model.

NIST should further develop its discussion of CSF Tiers, which serve as a practical framework for implementing the CSF across diverse settings.

First, NIST should expand the discussion of Tiers to help to address issues such as governance, as discussed above. *Second*, NIST should consider adding an additional Tier in between the current Tier 3 (Repeatable) and Tier 4 (Adaptive). An organization seeking to leverage the CSF could reasonably interpret the Tiers as leaving a significant gap between Tier 3

[118] Concept Paper at 5, 10-12.

and Tier 4. Providing an additional Tier between Tier 3 and Tier 4 could facilitate improved security practices from small- or medium-sized organizations that are unable to meet certain aspects of the Tier 4 definition due to lack of resources or other inhibiting factors. This targeted change to the structure of the CSF Tiers will best serve the broad range of CSF stakeholders—which includes organizations of all sizes—without risking the downstream effects that could result from broad changes to the CSF Core.

Third, as NIST updates the Tiers, it should clarify that the Tiers are not to be used as a proxy for a maturity model. In the Concept Paper, NIST writes that it plans to "better describe the relationship between Tiers and maturity model concepts," but makes clear that "CSF 2.0 will not provide a distinct maturity model to meet CSF outcomes at the Function, Category, or Subcategory level."[119] CTIA supports this approach. Unlike a maturity model, Tiers can facilitate an organization's communication of its assessment of its cybersecurity risk management program into its broader risk management processes, which involve considerations about organization-wide priorities, resource availability and allocation, and risk tolerance, among other things. Given these distinct differences, NIST's plan to "better describe the relationship between Tiers and maturity model concept[]"—without creating a separate CSF maturity model—will provide necessary clarity to stakeholders on this important issue.[120]

B. NIST Should Take Steps to Ensure that the CSF Remains Up-to-Date Amidst Constant Change and Development Across the Cybersecurity Ecosystem.

During the February Working Sessions, some participants appeared less familiar with OLIR and with other NIST publications such as the many NISTIRs that develop CSF profiles.[121]

[119] *Id.* at 14.

[120] *Id.*

[121] *See Cybersecurity Framework: Examples of Framework Profiles*, NIST, https://www.nist.gov/cyberframework/examples-framework-profiles (last updated Jan. 31, 2023).

This is an area for NIST attention that can occur outside of the CSF update process.

To that end, NIST should continue to leverage and promote the OLIR Program by: (1) building into CSF 2.0's Informative References column a link to the relevant OLIR references and mappings; (2) providing in CSF 2.0 a clear description of OLIR and how users can benefit from it; (3) on an ongoing basis, continuing to keep Informative References—as well as separate references to NIST documents—up-to-date for all CSF 2.0 Subcategories; and (4) bolstering mappings between the CSF and the documents that are built off of or reference the CSF, including international standards.

Beyond OLIR, NIST should continue to engage with stakeholders—both domestic and international—who are developing and deploying cybersecurity standards and best practices, including international standards organizations. NIST should make these engagements not only in the context of CSF 2.0, as proposed in the Concept Paper,[122] but also in the context of its other cybersecurity workstreams, as well.

VIII. CONCLUSION.

CTIA is pleased to continue its longstanding collaboration with NIST on the CSF. As NIST proceeds with updating its flagship cybersecurity guidance document, CTIA recommends that NIST: (1) recognize the CSF's ubiquity and avoid making significant changes to the CSF Core that may have harmful impacts on the document's backward compatibility; (2) adopt certain changes proposed in the Concept Paper that are grounded in flexibility and would promote broad adoption of the CSF; (3) incorporate governance issues into the discussion of Tiers and add governance-specific outcomes throughout the existing CSF Core, rather than

[122] Concept Paper at 5 ("NIST will continue to participate in international standards activities that leverage the CSF as part of a broader effort and priority to engage strategically in the work of international standards developing organizations. This includes continuing ongoing work in the [ISO] where several documents reference the CSF.").

adding a new Govern Function; (4) continue to treat C-SCRM with a light touch, consistent with CSF 1.1; (5) adopt its proposal to provide substantive cyber measurement guidance in 800-55 Rev. 2 rather than the CSF; and (6) take steps to improve the practical implementation and continued relevance of the CSF.

Respectfully submitted,

/s/ *Thomas K. Sawanobori*
Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

John A. Marinho
Vice President, Technology and Cybersecurity

Justin C. Perkins
Manager, Cybersecurity and Policy

CTIA
[redacted]

March 6, 2023