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

In the Matter of

Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management	))))	Docket Number: 220210-0045

COMMENTS OF CTIA

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

John A. Marinho
Vice President, Technology and Cybersecurity

Melanie K. Tiano
Assistant Vice President, Cybersecurity and Privacy

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

April 25, 2022

Table of Contents

I. INTRODUCTION AND SUMMARY.

CTIA[1] appreciates the opportunity to provide input to the National Institute of Standards and Technology ("NIST") for its Request for Information ("RFI")[2] that asks about the *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1* ("CSF" or "CSF 1.1")[3] and potential updates to the CSF ("Updated CSF"). NIST also asks how it can improve guidance about cybersecurity in supply chains[4] and seeks input on the National Initiative for Improving Cybersecurity in Supply Chains ("NIICS"), a new public-private partnership that will address cybersecurity risks in supply chains. CTIA has been an active participant in NIST CSF proceedings and applauds NIST's work to convene private and public sector expertise to build a voluntary, flexible, consensus-based document that provides value to public and private sector organizations of all sizes. As a result of NIST's stakeholder engagement, the CSF is a tool that global organizations rely on.

CTIA makes several recommendations. *First*, while CTIA supports keeping the CSF current, NIST should consider waiting to update the CSF in light of the myriad cybersecurity activities currently underway. Further, when NIST does update the CSF, it must be careful not

---

[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] *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 ("RFI").

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

[4] RFI at 9,579.

to make major changes to the document's core structure and approach. Wholesale changes would have broad and likely disruptive effects across organizations of all sizes and sectors that use the CSF in their cybersecurity programs, as well as in cybersecurity and risk management tools built on the CSF. NIST should focus on fine-tuning the CSF, for example, by refreshing Informative References, instead of rewriting it. Essentially, NIST should work towards a version 1.2 of the CSF instead of a version 2.0.

Second, NIST should ensure that any Updated CSF: (1) remains voluntary and flexible, as these features have made the CSF a reliable risk management tool; (2) remains process-oriented and technology- and threat-agnostic; and (3) emphasizes how it can be used as a common foundation for cybersecurity guidance, both at NIST and across the government.

Third, NIST should approach cybersecurity supply chain risk management ("C-SCRM"), with caution. Supply chain issues are important to cyber risk management but are already subject to extensive work by multiple other agencies. NIST should refresh the CSF's Informative References and mappings to ensure that an Updated CSF reflects the robust treatment of C-SCRM issues that has developed in many venues since the release of CSF 1.1.

Finally, NIST should use the NIICS public-private partnership—which ideally will represent many sectors, including Communications—to harmonize federal C-SCRM initiatives.

II. THE WIRELESS SECTOR LEVERAGES THE CSF AS PART OF ITS COMMITMENT TO CYBERSECURITY.

The CSF serves as the foundation for numerous cybersecurity initiatives in which the wireless sector has engaged. For example, soon after the CSF was first published, the Federal Communications Commission's ("FCC") Communications Security, Reliability, and Interoperability Council ("CSRIC") conducted a comprehensive mapping of the CSF for each of

the Communications Sector's five segments.[5] Among other things, the CSRIC Final Report found that the CSF's Functions, Categories, and Subcategories were helpful for articulating outcomes and illustrating use-case scenarios for wireless technologies, networks, and services.[6] Subsequent CSRIC cybersecurity guidance documents have drawn heavily on the CSF, including on topics such as security-by-design, Next Generation 9-1-1, and cybersecurity workforce development.[7]

Like many organizations, CTIA has launched cybersecurity initiatives that rely on or build from the CSF. Both CTIA's IoT Testing Program and its new 5G Security Industry Test Bed build on the CSF and CSRIC documents.[8] CTIA also contributed to the C2 Consensus on IoT Device Security Baseline Capabilities,[9] an IoT security framework informed by NIST documents that use the CSF.[10] NIST has leveraged the CSF as a model for wireless

[5] Cybersecurity Risk Management and Best Practices Final Report, CSRIC IV Working Group 4 (Mar. 2015), https://www.atis.org/wp-content/uploads/01_legal/docs/CSRICIV/CSRIC_IV_WG4_Final_Report_031815.pdf.

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

[7] *See* Secure Hardware and Software: Security-by-Design Final Report, 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 on Small Carrier NG9-1-1 Transition Considerations, CSRIC VI Working Group 1, at 28, 30-33 (Sept. 2018), *available at* 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), *available at* https://www.fcc.gov/files/csric7reportsecuirtyrisk-bestpracticesmitigation-legacytransitionalng911pdf; Cybersecurity Workforce: Status Update, CSRIC V Working Group 7, at 3, 7 (Dec. 3, 2015), *available at* https://transition.fcc.gov/bureaus/pshs/advisory/csric5/WG7_Presentation_120315.pptx.

[8] Cybersecurity Certification Program for IoT Devices, Version 1.5, CTIA, at 6-7 (Sept. 2021), *available at* https://ctiacertification.org/wp-content/uploads/2021/09/CTIA-Cybersecurity-Certification-Program-for-IoT-Devices-V-1-5.zip ("The following documents are referenced in this document… NIST Cybersecurity Framework v1.1."); *CTIA Launches 5G Security Test Bed for Commercial 5G Networks*, PR Newswire (Jan. 12, 2022), https://www.prnewswire.com/news-releases/ctia-launches-5g-security-test-bed-for-commercial-5g-networks-301459627.html ("The [Security Test Bed] primarily focuses on verifying the [CSRIC] VII recommendations for 5G networks. [It] will also serve as a valuable industry resource for CSRIC VIII.").

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

[10] *See id.* at 8.

cybersecurity guidance. For example, the NIST National Cybersecurity Center of Excellence ("NCCoE") has examined issues related to 5G technology using standards built off the CSF.[11]

CTIA members use the CSF as an input into their cybersecurity programs.

- AT&T's Security Policy and Requirements are "based, in part, on leading industry standards such as ISO/IEC 27001:2013" and align to the CSF.[12]
- Verizon maintains an information security policy that is "based on various recognized industry security standards and is aligned to the [CSF]."[13]
- T-Mobile's data security program "incorporates core functions from the widely recognized [CSF] and is constantly evolving to address new threats as they arise, including enhancing existing safeguards."[14]
- Intel conducted a pilot security project to test the CSF's use at Intel and found that it "helped us harmonize our risk management technologies and language, improve our visibility into Intel's risk landscape, inform risk tolerance discussions across our company, and enhance our ability to set security priorities, develop budgets, and deploy security solutions."[15] This project featured a modification of the CSF's Categories and Subcategories to match Intel's business needs and security processes.[16]

In sum, the CSF is a key resource that wireless sector stakeholders use in various contexts.

---

[11] *See* 5G Cybersecurity: Preparing a Secure Evolution to 5G, NIST (Apr. 2020), https://www.nccoe.nist.gov/sites/default/files/legacy-files/5G-pse-project-description-final.pdf. NCCoE's project, *5G Cybersecurity, Preparing a Secure Evolution to 5G*, offers several templates mapping communications security to the CSF and other important NIST cybersecurity guidance, including NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations.*

[12] *AT&T Issue Briefs: Network & Data Security*, AT&T, https://about.att.com/csr/home/reporting/issue-brief/network-data-security.html (last visited Apr. 12, 2022).

[13] *Verizon Security Summary*, Verizon, https://www.verizon.com/about/privacy/verizon-internal-systems-information-security-exhibit (last visited Apr. 12, 2022).

[14] 2020 Corporate Responsibility Report, T-Mobile, at 49 (2020), https://www.t-mobile.com/content/dam/t-mobile/assets/pdf/T-Mobile_CSR20_10921.pdf.

[15] Tim Casey et al., *The Cybersecurity Framework in Action: An Intel Use Case*, at 1 (2015), https://supplier.intel.com/static/governance/documents/The-cybersecurity-framework-in-action-an-intel-use-case-brief.pdf.

[16] *See id.* at 6.

III. THE CSF IS USED ACROSS THE PRIVATE SECTOR AND GOVERNMENT AND IN NUMEROUS RISK MANAGEMENT APPROACHES, SO NIST SHOULD CAREFULLY CONSIDER MAJOR CHANGES.

A. NIST Should Reconsider the Timing of the CSF Update.

The wireless sector supports keeping the CSF up to date, and agrees that "[m]uch has changed in the cybersecurity landscape" since NIST updated the CSF four years ago.[17] However, now may not be the time for a full-scale update. Given the amount of cybersecurity activity currently underway, it may be prudent for NIST to consider waiting on a major update. International events have exposed companies to heightened risks[18] at the same time that multiple agencies are looking at substantive requirements (such as Security Directives for certain critical infrastructure sectors)[19] and incident reporting (at the Department of Homeland Security ("DHS"),[20] Securities and Exchange Commission,[21] and Federal Trade Commission).[22] Letting these proceedings settle out before updating the CSF would ensure that stakeholders can meaningfully engage in the update process, which has been a hallmark of past NIST CSF proceedings and a critical factor in the CSF's success.

---

[17] RFI at 9,580.

[18] FACT SHEET: Act Now to Protect Against Potential Cyberattacks, White House (Mar. 21, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/fact-sheet-act-now-to-protect-against-potential-cyberattacks/.

[19] *E.g.*, DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators, DHS (July 20, 2021), https://www.dhs.gov/news/2021/07/20/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators.

[20] Consolidated Appropriations Act, 2022, Pub. L. No. 117-103, Div. Y (2022) (the "Cyber Incident Reporting for Critical Infrastructure Act of 2022").

[21] *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.

[22] *Standards for Safeguarding Customer Information*, FTC, 86 Fed. Reg. 70,062 (Dec. 9, 2021), https://www.govinfo.gov/content/pkg/FR-2021-12-09/pdf/2021-25064.pdf.

B. Because the CSF Is a Foundational Cyber Risk Management Tool, Any Update Should Focus on Fine-Tuning It, Not Rewriting It.

The CSF is a foundational document with far-reaching impacts on government and private sector users. As detailed below, there is an abundance of cybersecurity documents, developed by a diverse group of stakeholders, that build off the CSF's content and structure.

SRMA Plans and Other Critical Infrastructure Resources. Each Critical Infrastructure ("CI") Sector Risk Management Agency ("SRMA") "develops a sector-specific [risk management] plan through a coordinated effort involving its public and private sector partners."[23] The Communications Sector-Specific Plan "tailors the strategic guidance provided in the [National Infrastructure Protection Plan] to the unique operating conditions and risk landscape of the Communications Sector."[24] DHS, the Communications Sector's SRMA, discusses how, with respect to managing cyber risks, "[t]he Communications Sector takes a collaborative approach to cyber risk by working with DHS to evaluate the cybersecurity threats, vulnerabilities, and consequences to these critical functions and establish the sector's cyber-risk priorities."[25] Further, there is a wealth of resources that have been developed for CI sectors to manage cyber risk, all related to the CSF.[26]

NIST Profiles. NIST has created numerous profiles that allow organizations to align CSF security objectives with a specific mission, business objective, threat, or technology.[27] These

---

[23] *Communications Sector*, CISA, https://www.cisa.gov/communications-sector (last visited Apr. 12, 2022).

[24] 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.

[25] *Id*. at 20.

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

[27] *See NCCoE Learning Series Fireside Chat – A Look at the Cybersecurity Framework: Where We've Been, Where We Are, and Where We're Going*, NCCoE (Feb. 24, 2022), https://www.nccoe.nist.gov/get-involved/attend-events/nccoe-learning-series-fireside-chat-look-cybersecurity-framework-where/post-webinar-materials ("February CSF Webinar").

profiles help organizations chart a path of where they are and where they need to be to meet their security goals. Examples of NIST CSF profiles include: (1) NISTIR 8323, *Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services*;[28] (2) NISTIR 8374, *Ransomware Risk Management: A Cybersecurity Framework Profile* ("Ransomware CSF Profile");[29] (3) NISTIR 8183, Rev. 1, *Cybersecurity Framework Version 1.1 Manufacturing Profile*;[30] (4) Draft NISTIR 8310, *Cybersecurity Framework Election Infrastructure Profile*;[31] and (5) Draft NISTIR 8401, *Satellite Ground Segment: Applying the Cybersecurity Framework to Assure Satellite Command and Control*.[32]

NIST Frameworks. NIST has used the CSF as a model to create frameworks that address other areas of risk that an organization may confront. For example, NIST published a Privacy Framework[33] and a Risk Management Framework for Information Systems and Organizations.[34] NIST also released an initial draft of its Artificial Intelligence Risk Management Framework

[28] NISTIR 8323, Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services, NIST (Feb. 2021), https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8323.pdf.

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

[30] NISTIR 8183 Rev. 1, Cybersecurity Framework Version 1.1 Manufacturing Profile, NIST (Oct. 2020), https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8183r1.pdf.

[31] Draft NISTIR 8310, Cybersecurity Framework Election Infrastructure Profile, NIST (Mar. 2021), https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8310-draft.pdf.

[32] Draft NISTIR 8401, Satellite Ground Segment: Applying the Cybersecurity Framework to Assure Satellite Command and Control, NIST (Apr. 18, 2022), https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8401.ipd.pdf.

[33] 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 ("Privacy Framework").

[34] NIST SP 800-37, 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 ("RMF").

("AI RMF").[35] These frameworks are modeled on, or closely align with, the CSF.[36]

Other NIST Cybersecurity Guidance. There is no shortage of NIST cybersecurity guidance that relies on or maps to the CSF. Guidance spans technology—such as commercial satellite operations, energy sector asset management, and healthcare communication—and includes: (1) NISTIR 8170, *Approaches for Federal Agencies to Use the Cybersecurity Framework*;[37] (2) NISTIR 8286A, I*dentifying and Estimating Cybersecurity Risk for Enterprise Risk Management*;[38] (3) Draft (2nd) NISTIR 8270, *Introduction to Cybersecurity for Commercial Satellite Operations*;[39] (4) NIST SP 800-171, Rev. 2, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*;[40] (5) SP 1800-23, *Energy Sector Asset Management: For Electric Utilities, Oil & Gas Industry*;[41] and (6) SP 1800-24, *Securing Picture Archiving and Communication System (PACS): Cybersecurity for the Healthcare Sector*.[42]

Supply Chain Resources. As discussed below, several NIST supply chain security documents rely on or are mapped to the CSF, including NIST SP 800-161, Rev. 1 (2nd Draft),

---

[35] AI Risk Management Framework: Initial Draft, NIST, at i (Mar. 17, 2022), https://www.nist.gov/system/files/documents/2022/03/17/AI-RMF-1stdraft.pdf ("Draft AI RMF")

[36] *See, e.g.*, Privacy Framework at 6-9 (providing a Core, Profiles, and Implementation Tiers); RMF at xiv ("Each task in the RMF includes references to specific sections in the [CSF]. For example, Task P-2, Risk Management Strategy, aligns with the [Identity Function in the CSF]."); Draft AI RMF at 14-20 (providing a Core and Profiles).

[37] 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.

[38] 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.

[39] 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.

[40] 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.

[41] 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.

[42] 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.

Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations ("Draft SP 800-161, Rev. 1")[43] and NISTIR 8276, *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry* ("NISTIR 8276").[44]

Private Sector CSF Applications. There are many private sector applications of the CSF. Companies, including CI owners and operators, conduct assessments to ensure alignment with the CSF,[45] and companies procure CSF gap analyses to assist in building out their cybersecurity programs.[46] Some companies may require adherence to NIST guidelines as a proxy for cyber hygiene in contracts. A number of products and services use the CSF as an input. For example:

- Ericsson's Security Manager, a security management automation solution, draws on CSF principles.[47]
- AT&T's AlienVault USM Anywhere, a cloud-based security management solution,[48] combines essential security capabilities into a single platform to accelerate an organization's adoption of the CSF.[49]
- Cisco has developed numerous solutions that draw on the CSF's Core.[50] For example, Cisco Umbrella, a cloud-based Secure Internet Gateway, maps to

[43] NIST SP 800-161, Rev. 1 (2nd Draft), Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, NIST (Oct. 2021), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1-draft2.pdf ("Draft SP 800-161, Rev. 1").

[44] 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 ("NISTIR 8276").

[45] *See, e.g.*, *Cybersecurity Framework: Success Story: Saudi Aramco*, NIST (last updated Jan. 25, 2021), https://www.nist.gov/cyberframework/success-stories/saudi-aramco.

[46] *See, e.g.*, *NIST Gap Analysis & Implementation*, Razorthorn, https://www.razorthorn.com/cyber-security-consultancy/cyber-security-compliance/nist-gap-analysis-and-implementation/ (last visited Apr. 12, 2022).

[47] *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.

[48] *USM Anywhere*, AT&T, https://cybersecurity.att.com/products/usm-anywhere (last visited Mar. 29, 2022).

[49] *NIST Cybersecurity Framework Compliance with AlienVault USM Anywhere*, AT&T, https://cybersecurity.att.com/resource-center/solution-briefs/nist-compliance-usm-anywhere (last visited Apr. 12, 2022).

[50] Cisco and the NIST Cybersecurity Framework: Effective Cybersecurity Risk Management, Cisco (2019), https://www.cisco.com/c/dam/en/us/products/collateral/security/nist-cybersecurity.pdf.

several CSF Functions and Categories.[51]

- Amazon Web Services offers different cloud-based service offerings that align to the CSF.[52]

- Proofpoint provides a number of different products and services that align to the CSF,[53] including its Targeted Attack Protection[54] that detects email attacks and threats to cloud apps.[55]

International Uses. The CSF is influential internationally, as well as domestically. Japan's METI was an early user, with "security measures organized in consideration of the concept of NIST cybersecurity frameworks."[56] NIST recently announced that the CSF 1.1 has been translated into Ukrainian, which adds to the list of international adaptations of the CSF.[57]

Given the success of the CSF and its global use, NIST should be careful in making changes. As outlined above, both the structure and substance of the CSF are relied upon by a wide range of organizations, as well as in numerous tools that public and private sector organizations rely on to improve their security posture. As such, NIST should not disrupt the core structure and approach of the CSF; such changes, even if well-intentioned, would have disruptive effects on cybersecurity resources that rely on the CSF, potentially limiting the utility of these resources, unsettling the reliance of organizations that use the CSF and derivative

---

[51] *Id.* at 5, 9, 12, 13, 17.

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

[53] 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).

[54] *Id.* at 3, 4, 7-10.

[55] *Targeted Attack Protection*, Proofpoint, https://www.proofpoint.com/us/products/advanced-threat-protection/targeted-attack-protection (last visited Apr. 12, 2022).

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

[57] *Cybersecurity Framework: International Resources*, NIST (last updated Mar. 30, 2022), https://www.nist.gov/cyberframework/international-resources.

documents, and potentially requiring revisions to countless government and private programs.

For example, any Updated CSF should retain the CSF's Implementation Tiers ("Tiers"). The Tiers "provide context on how an organization views cybersecurity risk and the processes in place to manage that risk."[58] While the concept of Tiers is useful overall, NIST should continue to make clear—as the CSF 1.1 does—that the CSF is not a maturity model and that the Tiers are not to be used as a proxy for a maturity assessment.[59] The CSF 1.1 is right to distinguish tiering from maturity; in contrast to 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 the well-established differences between tiering and maturity, NIST should continue to make explicit in any Updated CSF that the Tiers are not a proxy for a maturity assessment.

To the extent NIST decides to make changes to the CSF, they need to be focused and tailored to limit disruptions to other resources. For example, one update that NIST *should* undertake is to refresh the CSF 1.1's Informative References under each Subcategory. As discussed below, NIST should continue to leverage the National Online Information References Program ("OLIR") to keep these Informative References up to date and accurate following its refresh, which will allow NIST to incorporate and map the CSF to new approaches and frameworks as they are developed.[60] This should include, for example, the Department of

[58] *Cybersecurity Framework: Questions and Answers*, NIST (last updated Feb. 24, 2022), https://www.nist.gov/cyberframework/frequently-asked-questions/framework-basics ("CSF Q&A").

[59] CSF 1.1 at 8 (explaining that "[t]iers do not represent maturity levels. Tiers are meant to support organizational decision making about how to manage cybersecurity risk, as well as which dimensions of the organization are higher priority and could receive additional resources.").

[60] National Online Information References Program (OLIR), NIST (last updated Feb. 28, 2022), https://csrc.nist.gov/projects/olir ("OLIR").

Defense's Cybersecurity Maturity Model Certification ("CMMC") program.[61] By keeping OLIR up to date, NIST can facilitate further private sector engagement with this helpful NIST resource.

In short, CTIA encourages NIST not to embark on a wholesale re-draft, but instead to do a targeted refresh. Indeed, while the current effort to evaluate and update the CSF has been referred to as the "CSF 2.0,"[62] CSF 1.2 would be a more appropriate description.

IV. ANY UPDATED CSF SHOULD REMAIN VOLUNTARY, FLEXIBLE, AND TECHNOLOGY- AND THREAT-AGNOSTIC.

A. It Is Critical that Use of the CSF Remains Voluntary for the Private Sector.

The CSF is a voluntary tool for the private sector. Executive Order 13636, *Improving Critical Infrastructure Cybersecurity* ("EO 13636"),[63] directed NIST to develop the CSF and is premised on the notion that the CSF would be voluntary. EO 13636 states that the CSF "shall incorporate *voluntary* consensus standards and industry best practices" and "shall be consistent with *voluntary* international standards."[64] Congress has endorsed the utility of this non-regulatory, voluntary approach for the private sector. By enacting the Cybersecurity Enhancement Act of 2014,[65] Congress authorized NIST to "facilitate and support the development of a *voluntary*, consensus-based, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to cost-effectively reduce cyber risks to

[61] *Securing the Defense Industrial Base: CMMC 2.0*, Department of Defense, https://www.acq.osd.mil/cmmc/ (last visited Apr. 14, 2022).

[62] February CSF Webinar (asking NIST's Kevin Stine about plans for a CSF "2.0").

[63] Exec. Order No. 13636, *Improving Critical Infrastructure Cybersecurity*, 78 Fed. Reg. 11,739 (Feb. 19, 2013), https://www.govinfo.gov/content/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

[64] *Id*. at 11,741 (emphasis added).

[65] Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274, 128 Stat. 2971 (2014) (codified in relevant part at 15 U.S.C. § 272).

critical infrastructure."[66] Although federal agencies are now required to apply the CSF to federal information systems,[67] the CSF remains a voluntary resource for the private sector.[68]

Given this established voluntary approach, NIST must make explicit in any Updated CSF that the document is to be purely voluntary for the private sector and, importantly, is not intended to serve as a basis or foundation for a regulatory standard. This is the right way to promote cybersecurity in CI and across the private sector. The CSF is made up of *voluntary* standards, guidelines, and practices. The documents were designed to be applied as appropriate by organizations and were not developed as prescriptive requirements. As a result, the CSF is intended to be used voluntarily to help private organizations evaluate and mature their operations and programs in ways that make sense for the organization. Its utility as a flexible, voluntary framework has led to its success and its use as the foundation for other cybersecurity guidance, as discussed. It is imperative that NIST make explicit in any Updated CSF that it is intended purely for voluntary use within the private sector.

B. The CSF Should Retain Its Flexibility.

As NIST has recognized, cybersecurity does not lend itself to a one-size-fits-all solution.[69] Cybersecurity is multi-faceted, nuanced, and dynamic. Determining optimal cybersecurity solutions to challenging security issues is complex and requires an organization to balance risk, resource, and threat assessment considerations, among other things. Two different

---

[66] Confronting the Challenge of Cybersecurity, Hearing Before the S. Comm. on Com., Science and Transp., 114th Cong. 1 (Sept. 3, 2015) (testimony of Kevin Stine, Leader, Security Outreach and Integration Group, NIST) https://www.commerce.senate.gov/services/files/629B3130-C0D3-44AF-ADCE-88237096A14C (emphasis added).

[67] Exec. Order No. 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, 82 Fed. Reg. 22,391, 22,392 (May 16, 2017), https://www.govinfo.gov/content/pkg/FR-2017-05-16/pdf/2017-10004.pdf.

[68] CSF 1.1 at vi ("Expanded and more effective use and sharing of best practices of this *voluntary* Framework are the next steps to improve the cybersecurity of our Nation's critical infrastructure" (emphasis added)); *see* CSF Q&A.

[69] *See, e.g.*, CSF Q&A ("There are no 'silver bullets' when it comes to cybersecurity and protecting an organization.").

organizations looking to address similar security concerns may devise different solutions based on the circumstances confronting the organizations.

Accordingly, the CSF "is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure. Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances. They also will vary in how they customize practices described in the [CSF]. Organizations can determine activities that are important to critical service delivery and can prioritize investments to maximize the impact of each dollar spent."[70] This is the right approach. To provide maximum value, the CSF must be capable of being tailored as appropriate for any organization, product, or service to address a wide variety of cybersecurity challenges. As a result, it is critical that NIST continue to recognize the importance of flexibility and eschew any recommendations from government stakeholders or other parties to develop an Updated CSF that is more rigid or prescriptive.

C. Any Updated CSF Should Remain Process-Oriented and Technology- and Threat-Agnostic.

One of the CSF's key strengths is its longevity. Despite changes in the cybersecurity landscape since the CSF was last updated, the document remains a staple of process-based cybersecurity efforts. The CSF is applicable, both domestically and internationally, to a range of business models and approaches to cybersecurity, including for enterprises that enter into service level agreements for cybersecurity risk management services. To maintain this critical feature of the CSF, NIST should continue to focus on process and reject any recommendations to turn the CSF into a document that seeks to explicitly address specific incidents or threats. Such an approach would be a poor fit for the dynamic and quickly evolving nature of cybersecurity.

[70] CSF 1.1 at 2.

NIST is right to acknowledge changes "in terms of threats, capabilities, [and] technologies" since the CSF was last updated.[71] Because threats and solutions will continue to evolve, the CSF will be most useful if it remains process oriented and technology- and attack-agnostic. The CSF is designed to help an organization "align and prioritize its cybersecurity activities with its business/mission requirements, risk tolerances, and resources."[72] It is not designed to address a list of every possible cybersecurity threat, and NIST should not attempt to do so now.

NIST's work on ransomware threats illustrates the correct approach. In developing the Ransomware CSF Profile, NIST applied CSF security objectives to the specific threat of ransomware.[73] By publishing profiles that apply the CSF to specific cybersecurity threats or technologies, as outlined above, NIST uses the CSF to inform how an organization might address emerging issues while avoiding the downstream effects of making substantive changes to the CSF's content and structure, or trying to address each new threat in the document. NIST should continue to use CSF profiles to address specific threats rather than do so in the Updated CSF.

V. IN ANY UPDATE, NIST SHOULD EMPHASIZE THE NEED FOR A HARMONIZED APPROACH TO CYBERSECURITY WITHIN NIST AND ACROSS GOVERNMENT.

A. Within NIST, the CSF Should Serve as a Common Thread to Help Ensure Continuity and Consistency Across NIST's Cybersecurity Workstreams.

The RFI seeks "[s]uggestions for improving alignment or integration of the [CSF] with other NIST risk management resources."[74] CTIA recommends that NIST take this opportunity to

[71] RFI at 9,580.

[72] CSF 1.1 at v.

[73] Ransomware CSF Profile.

[74] RFI at 9,580.

promote continuity across its cybersecurity resources, including by discussing how the CSF relates to other guidance and by providing updated mappings.

As outlined, NIST has an array of cybersecurity and risk management guidance aligned with the CSF that addresses different technologies, threats, and risk management considerations. To ensure that these documents retain their utility, any changes to the CSF should be accompanied by corresponding changes to other NIST resources to account for new features in the Updated CSF, including through new or updated mappings. Moreover, NIST should make sure that it articulates the relationship between its other documents and the Updated CSF. It is important that public and private sector organizations alike understand how NIST's technology- and sector-specific guidance fits into the broader, process-based framework of the CSF.

B. The CSF Should Be the Touchstone of Regulatory Efforts by Other Federal Agencies.

CTIA is committed to a voluntary approach to managing cybersecurity risks, led by industry. As agencies and Congress look to potential regulatory approaches or increased oversight, they should rely on the CSF as a touchstone. The CSF has been widely successful in improving CI cybersecurity across sectors and technologies, and NIST's extensive work on cybersecurity risk management through the CSF and other documents built on top of the CSF provides a critical foundation for other cybersecurity efforts across government. Federal agencies should align any new cybersecurity policy approaches with the CSF, as there is no need for federal agencies or Congress to reinvent the wheel when NIST created a consensus-based and flexible cybersecurity framework that is useful across sectors and widely lauded.

Similarly, NIST should recognize in any Updated CSF the need for harmonization and coordination across agencies about standards of care and emergent regulatory regimes. Other agencies can learn from the NIST experience in developing the CSF and pursue an approach that

aligns with the CSF. By promoting harmonization and coordination across government, NIST can further lay the groundwork for a successful approach to federal cybersecurity policy.

VI. AN UPDATED CSF SHOULD PRESERVE A LIGHT TOUCH FOR SUPPLY CHAIN RISK MANAGEMENT, WHICH WAS PROPERLY ADDRESSED IN CSF 1.1.

A. The Complex and Varying Nature of C-SCRM Cautions Against Changing Its Treatment in the CSF.

In the RFI, NIST seeks comment on C-SCRM, including "[w]hether and how [C-SCRM] considerations might be further integrated into an [Updated CSF]."[75] NIST should approach any changes to C-SCRM in the CSF with caution, as this is a complex and variable issue.

In CSF 1.1, NIST expanded its guidance on using the CSF to address C-SCRM issues. 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;"[76] (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;"[77] (3) incorporated C-SCRM into Tiers;[78] and (4) added a supply chain risk management ("SCRM") Category and Subcategories to the Core.[79]

In considering updates to the CSF's treatment of C-SCRM, NIST should recognize that C-SCRM is complex and varies between organizations and sectors. Supply chains "encompass[] business functions and enterprises interconnected by resource flows of goods, services,

[75] RFI at 9,581.

[76] CSF 1.1 at ii, 17.

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

[78] *Id.* at ii, 9-11.

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

information and funds."[80] Supply chain management "spans these interconnected networks to acquire, produce and deliver goods and services in our global economy."[81] Addressing the cybersecurity of such complex systems without compromising interconnectivity is challenging.

Further complicating this task is the varying nature of C-SCRM complexities. While certain C-SCRM complexities are common to many industrial sectors—including legacy systems whose provenance may not be known or relevant and whose contracts may be difficult to amend—other complexities are unique to certain sectors and organizations. For example, in the mobile information and communications technology ("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. . . ."[82] These examples show that providing uniform C-SCRM guidance is a difficult task. As a result, NIST should be careful not to disrupt the current C-SCRM guidance in CSF 1.1.

B. The Federal Government is Heavily Engaged in Supply Chain Initiatives.

The government has been active with regulatory and non-regulatory SCRM initiatives since the CSF was updated in 2018.

- The FCC has issued several orders to address ICT supply chain integrity by prohibiting the use of federal universal service funds for communications equipment and services provided by entities that pose a threat to national

[80] 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=5a2b1ec85bf5 (quoting C. John Langley, Managing Supply Chains: A Logistics Approach (2008)).

[81] *Id.*

[82] Robert J. Ellison, et al., *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.

security.[83] The FCC is presently evaluating additional actions it may take.[84]

- 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 industry and government to identify challenges and devise workable solutions."[85] As discussed below, this Task Force has issued many reports on ICT SCRM.

- NIST updated SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, in 2020.[86] The most recent version, Rev. 5 ("SP 800-53, Rev. 5"), established a new supply chain risk management control family.[87]

- 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.[88]

- The Department of Commerce issued an interim final rule on review of information and communication technology and services ("ICTS") transactions and is also working on an advance licensing process for ICTS transactions.[89]

- Last year, President Biden signed Executive Order 14028, *Improving the Nation's Cybersecurity*, which directed several federal agencies to launch initiatives designed to improve the security and integrity of the software supply chain.[90] Pursuant to the Cyber EO, NTIA published the minimum elements for a Software

---

[83] *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) (implementing a reimbursement program to expedite removal of harmful equipment and services).

[84] *Request for Comments on Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program*, FCC, 86 Fed. Reg. 46,641 (Aug. 19, 2021).

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

[86] 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").

[87] *Id*. (providing "Mappings: Cybersecurity Framework and Privacy Framework to Rev. 5" as supplemental material).

[88] *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).

[89] *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); *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).

[90] *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.

Bill of Materials[91] while NIST issued SP 800-218, *Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities* ("SSDF")[92] as well as its *Software Supply Chain Security Guidance Under Executive Order (EO) 14028 Section 4e*.[93]

- President Biden signed Executive Order 14017, *America's Supply Chains* ("Supply Chains EO"), which launched several initiatives to strengthen America's supply chains. The White House issued a 100-day Supply Chain Review report of critical industries[94] and several agencies issued reports and devised strategies,[95] including one report dedicated to the ICT industrial base.[96]

- Earlier this year, on the one-year anniversary of the Supply Chains EO, the White House announced plans to take 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.[97]

Beyond these federal initiatives, numerous SCRM materials published by NIST and other

---

[91] 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.

[92] 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").

[93] 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.

[94] Building Resilient Supply Chains, Revitalizing American Manufacturing, and Fostering BroadBased 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.

[95] *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.

[96] 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.

[97] 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/.

entities rely on the CSF and apply its guidance. In addition to SP 800-53, Rev. 5, discussed above, these include: (1) Draft SP 800-161, Rev. 1;[98] (2) NISTIR 8276,[99] (3) NISTIR 8179, *Criticality Analysis Process Model: Prioritizing Systems and Components*;[100] (4) the SSDF;[101] (5) NIST's Project Description White Paper on *Validating the Integrity of Computing Devices: Supply Chain Assurance*;[102] and (6) numerous ICT SCRM Task Force publications.[103] The number of pending federal initiatives on supply chain, combined with the widespread application of the CSF to various SCRM guidance documents, make it even more important that NIST proceed with caution on this topic in any Updated CSF.

C. NIST Should Maintain Its Treatment of C-SCRM in the CSF, While Updating Informative References and Mappings and Improving OLIR.

As NIST updates the CSF, it should maintain its helpful and appropriate treatment of C-SCRM from CSF 1.1. Specifically, NIST's ID.SC category in the CSF 1.1 remains the appropriate level of treatment of SCRM issues for the process-oriented CSF. NIST should avoid providing more detailed or prescriptive treatment of SCRM issues in the Updated CSF. As

[98] Draft SP 800-161, Rev. 1 at 46-47, 249-50, 313.

[99] NISTIR 8276 at 15, 19, 23-24.

[100] *E.g.*, 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.

[101] SSDF at 2, 5-19.

[102] Project Description, Validating the Integrity of Computing Devices: Supply Chain Assurance, NIST, at 3, 9 (Mar. 2020), https://www.nccoe.nist.gov/sites/default/files/legacy-files/tpm-sca-project-description-final.pdf.

[103] *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.

discussed above, the process-oriented CSF is not the appropriate document to address in detail specific issues like supply chain security. Any attempt to do so will have detrimental effects on the CSF and would quickly cause it to become outdated.

Rather than oversaturating the CSF with new supply chain guidance, NIST should take this opportunity to refresh its Informative References and mappings to reflect the most recent work and thinking in this complex area. In particular, the current Informative References in CSF 1.1 are outdated and incomplete, and thus should be updated. For example, CSF 1.1 references SP 800-53, Rev. 4, not Rev. 5.[104] NIST has already completed a helpful mapping of the CSF to 800-53, Rev. 5, which is available as a supplemental resource on the 800-53, Rev. 5 webpage[105] and in the OLIR Catalog.[106] Any update to the CSF should include this updated mapping, and the ID.SC Informative References should be updated as well. Similarly, the ID.SC Informative References should include the SSDF as well as Draft SP 800-161, Rev. 1 once that document is finalized. Likewise, any Updated CSF should show the extensive work that industry and government have developed since 2018, including guidance documents from the DHS ICT SCRM Task Force.

To ensure that users of the Updated CSF have access to the wealth of existing C-SCRM guidance, NIST should continue to leverage and promote OLIR. OLIR is a valuable resource, and NIST should redouble efforts to increase its helpful mappings and references. To further improve OLIR, NIST should provide a clear link between the Updated CSF and OLIR. Already,

[104] CSF 1.1 at 24-44.

[105] 800-53 Webpage.

[106] National Online Informative References Program, 800-53-v5-to-Framework-v1.1 Informative Reference Details, NIST (last updated Apr. 19, 2022), https://csrc.nist.gov/projects/olir/informative-reference-catalog/details/20.

on NIST's main page for the CSF, there is a tab dedicated to Informative References.[107] This is a good start; NIST should build into the Updated CSF's "Informative References" column a link to the relevant OLIR references and mappings, and the Updated CSF should provide a clear description of OLIR and how users can benefit from it. Moreover, and as noted above, NIST should engage in this refresh and ongoing work to keep the Informative References up to date for all of the CSF's Subcategories, not just those relating to SCRM. Doing so will further promote private sector engagement with this important tool.

VII. BEYOND THE CSF, NIST SHOULD LEVERAGE THE NIICS TO HARMONIZE THE MULTITUDE OF FEDERAL SUPPLY CHAIN INITIATIVES.

The RFI seeks input on NIST's new NIICS initiative and the "greatest challenges related to the cybersecurity aspects of [SCRM] that the NIICS could address."[108] According to NIST, the NIICS will be a "wide-ranging public-private partnership [that] will focus on identifying tools and guidance for technology developers and providers, as well as performance-oriented guidance for those acquiring such technology."[109] CTIA welcomes NIST's commitment to addressing cybersecurity issues through public-private partnerships, and appreciates the opportunity to comment on the use of the NIICS to advance C-SCRM.

Given the array of work being done in industry and across government on C-SCRM, NIST should focus the NIICS on bringing together workstreams to help reduce fragmentation and promote harmonization of federal supply chain initiatives. A key challenge for industry is

---

[107] *Cybersecurity Framework*, NIST, https://www.nist.gov/cyberframework (last visited Apr. 11, 2022).

[108] RFI at 9,581. The concept of the NIICS was born out of a White House cybersecurity summit on August 25, 2021 that featured senior Administration officials and private sector leaders. *See, e.g.*, Press Release, Dep't of Commerce, U.S. Secretary of Commerce Gina M. Raimondo Joins White House Cybersecurity Summit (Aug. 25, 2021), https://www.commerce.gov/news/press-releases/2021/08/us-secretary-commerce-gina-m-raimondo-joins-white-house-cybersecurity.

[109] RFI at 9,579.

the multiplicity of workstreams, as outlined earlier. Overlapping federal efforts strain resources for companies of all sizes and undermine U.S. businesses' ability to work with overseas partners and investors, hurting competitiveness and fragmenting international markets.

The fragmentation and regulatory uncertainty created by the number of relevant workstreams is harmful for companies and industries, such as ICT, whose supply chain strategies cannot turn on a dime. Network equipment and design are years-long investments in which substantial costs are sunk, making it challenging for companies to quickly pivot to other sources. By advocating for a unified federal strategy to C-SCRM and devising strategies that will facilitate harmonization, the NIICS can provide value to the government by reducing unnecessary burdens on industry, encouraging innovation, minimizing confusion and overlap, and reducing administrative burdens on both the federal government and the private sector.

Additionally, it is critical that the NIICS includes the Communications Sector. The ICT industrial base as a whole plays a critical role in the overall supply chain ecosystem. For the NIICS to meet NIST's stated goal of "increas[ing] trust and assurance in technology products, devices, and services," it is critical that the NIICS includes significant representation across a wide range of sectors, including the Communications Sector.[110]

VIII. CONCLUSION.

CTIA is pleased to continue collaborating with NIST on the CSF. As it considers updates to the CSF, NIST should: (1) consider waiting to update the CSF, and when it does update the CSF, refresh it instead of rewrite it; (2) ensure that any Updated CSF remains voluntary, flexible, and process-oriented, and also emphasize its utility as a common foundation for cybersecurity guidance both within NIST and across government; (3) approach any C-SCRM updates with

[110] *Id*. at 9,581.

caution and avoid converting the CSF into a supply chain-specific tool; and (4) leverage the NIICS to harmonize federal supply chain initiatives.

Respectfully submitted,

/s/ Melanie K. Tiano
Melanie K. Tiano
Assistant Vice President, Cybersecurity and Privacy

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

John A. Marinho
Vice President, Technology and Cybersecurity

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

April 25, 2022