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

In the Matter of	)	
	)	
	)	Initial Public Draft of the NIST
Cybersecurity Framework 2.0	)	Cybersecurity Framework 2.0
	)	

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]
www.ctia.org

November 6, 2023

Table of Contents

I. INTRODUCTION

CTIA[1] is pleased to continue to collaborate with the National Institute of Standards and Technology ("NIST") as it updates the *NIST Cybersecurity Framework* ("CSF" or "Framework") by commenting on the Initial Public Draft of *The NIST Cybersecurity Framework 2.0* ("Draft CSF 2.0" or "Draft").[2] The Draft is part of a process to update the Framework from its current Version 1.1 *Framework for Improving Critical Infrastructure Cybersecurity* ("CSF 1.1")[3] to Version 2.0 ("CSF 2.0").

CTIA commends NIST on its commitment to providing opportunities for stakeholders to contribute to this process. NIST has provided extensive opportunities for community involvement by issuing a Request for Information ("RFI"),[4] hosting workshops[5] and working sessions,[6] seeking comments on a Concept Paper[7] and *CSF 2.0 Core Discussion Draft* ("Draft

[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, Public Draft : The NIST Cybersecurity Framework 2.0 (Aug. 8, 2023) https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.ipd.pdf ("Draft CSF 2.0").

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

[4] *Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management*, Notice and Request for Information, 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] NIST, *Journey to the NIST Cybersecurity Framework (CSF) 2.0: Workshop #1* (Aug. 17, 2017), https://www.nist.gov/news-events/events/2022/08/journey-nist-cybersecurity-framework-csf-20-workshop-1; NIST, *Journey to the NIST Cybersecruity Framework (CSF) 2.0: Workshop #2* (Feb. 15, 2023), https://www.nist.gov/news-events/events/2023/02/journey-nist-cybersecurity-framework-csf-20-workshop-2.

[6] NIST, *Journey to the NIST Cybersecurity Framework (CSF) 2.0: In-Person Working Sessions* (Jan. 11, 2023), https://www.nist.gov/news-events/events/2023/02/journey-nist-cybersecurity-framework-csf-20-person-working-sessions (last updated Feb. 16, 2023).

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

2.0 Core"),[8] and now releasing the full Draft CSF 2.0 for feedback. CTIA is proud to have provided feedback throughout the entirety of the process—including by commenting on the RFI,[9] the Concept Paper,[10] and most recently, the Draft 2.0 Core.[11] NIST's collaborative approach will help to ensure that CSF 2.0 remains a successful framework, which supports information security and risk management activities of organizations of all sizes and types around the globe.

The current Draft is a promising next step in the evolution of the CSF. In particular, NIST has taken the right approach to preserve the most important features of the CSF—the Draft remains process-oriented, risk-based, flexible, and voluntary. As NIST proceeds to finalize CSF 2.0, CTIA urges NIST to continue to prioritize these principles, and specifically to: reject calls to turn the discussion of cybersecurity supply chain risk management into a seventh Function; communicate to government partners that the CSF is not intended as a regulatory baseline; make modest edits to ensure Implementation Examples use voluntary and flexible terminology and address select cybersecurity policy priorities; limit minor changes to terms and explanations between CSF 1.1 and CSF 2.0; and provide additional resources to support adoption of CSF 2.0, such as a detailed change analysis.

---

[8] NIST, Discussion Draft of the NIST Cybersecurity Framework 2.0 Core(Apr. 24, 2023), https://www.nist.gov/system/files/documents/2023/04/24/NIST%20Cybersecurity%20Framework%202.0%20Core%20Discussion%20Draft%204-2023%20final.pdf ("Draft 2.0 Core").

[9] Comments of CTIA, Request for Information on Evaluating and Improving Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management (filed Apr. 25, 2022), https://www.nist.gov/system/files/documents/2022/05/03/04-25-2022%20-%20CTIA.pdf.

[10] Comments of CTIA, NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework (filed Mar. 6, 2023), https://www.nist.gov/system/files/documents/2023/04/04/2023-03-06%20CTIA_508_Redacted.pdf ("CTIA Concept Paper Comments").

[11] Comments of CTIA, Discussion Draft of the NIST Cybersecurity Framework 2.0 Core, (filed May 31, 2023), https://www.nist.gov/system/files/documents/2023/08/04/CTIA%20Comments%2005312023%20Discussion%20Draft_Redacted.pdf ("CTIA Draft 2.0 Core Comments").

II. NIST HAS PRESERVED THE MOST IMPORTANT FEATURES OF THE FRAMEWORK.

A. The Draft Has Correctly Retained a Process-Oriented Approach that Is Adaptable to Changing Threats and Technologies.

The CSF's process-oriented approach contributes to the document's utility. Maintaining a process-oriented approach enables the CSF and its users to keep pace as threats and technologies continuously change. Today's priority threat or commonly used technological capability may be obsolete in months or years. Accordingly, it is not possible to address every type of threat or significant technology development in a single document. As NSA's Director of Cybersecurity Rob Joyce recently put it on X, "Cybersecurity is a timeless game of cat and mouse. Attackers advance, defenders respond, and the chase continues. Stay agile, stay secure."[12]

Draft CSF 2.0 maintains its generally applicable, process-oriented focus, rather than focusing on a specific threat or a technology, as some had asked.[13] CTIA supports this approach, which will help ensure that the CSF remains a foundational cybersecurity risk management tool.

B. The Latest Draft Remains Flexible.

NIST recognizes that a "one-size-fits-all approach" is not appropriate for cybersecurity risk management.[14] This is why flexibility is one of the core attributes of the CSF. For example, the document takes an outcome-focused approach, identifying desired outcomes and a range of activities and Informative References that may support those outcomes, rather than a specific set

[12] @NSA_CSDirector, X (Oct. 29, 2023, 10:42) https://x.com/nsa_csdirector/status/1718639445346287930?s=46&t=sndPg3WwWCWdt61H08aMoQ.

[13] *See* Letter from CTIA to NIST, (June 9, 2022), at 2 ("Despite some calls in the record for NIST to apply the CSF to more specific operating environments or for the CSF to address specific threats, the same reasoning that NIST has applied in the IoT context applies across other technologies, operating environments, and threats: narrowing the focus of the CSF will undermine the document's utility").

[14] Draft CSF 2.0 at 2 ("The voluntary Framework is not a one-size-fits-all approach to managing cybersecurity risks.)

of processes or prescriptive controls.[15] NIST has explained that "[t]he outcomes are sector- and technology-neutral, so they provide organizations with the flexibility needed to address their unique risk, technology, and mission considerations."[16] The document's flexibility is one of the main reasons for its widespread adoption, both domestically and internationally.[17]

Draft CSF 2.0 retains this key characteristic, noting that the "Framework is designed to be used by organizations of all sizes and sectors."[18] As NIST moves to finalize CSF 2.0, it should continue to retain this flexibility so that the framework can be used by a range of organizations in a variety of contexts.

C. NIST Has Appropriately Refrained from Adding Substantive Measurement Guidance to the CSF 2.0 Draft.

In previous advocacy, CTIA recommended that NIST refer stakeholders to its dedicated information security performance measurement publication, rather than seek to address the complex and fact-specific topic of cybersecurity metrics and measurement in the CSF.[19] Draft CSF 2.0 is consistent with this advocacy. Specifically, it provides helpful guidance on metrics and measurement, emphasizing that companies can "innovate and customize how they incorporate measurement,"[20] and highlighting how organizations can use the CSF to generate

[15] *See, e.g., id.* at 9 (describing a current profile as "cover[ing] the Core's outcomes that an organization is currently achieving" and a target profile as "cover[ing] the desired outcomes that an organization has selected and prioritized").

[16] *Id*. at 1.

[17] *See* NIST, *Initial Summary Analysis of Responses to the Request for Information (RFI) Evaluating and Improving Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management*, at 2, (June 3, 2022), https://www.nist.gov/system/files/documents/2022/06/03/NIST-Cybersecurity-RFI-Summary-Analysis-Final.pdf ("The Framework serves as a prominent resource to manage cybersecurity risks holistically across an organization. It has been downloaded over 1.7 million times and is used by organizations of varying sectors, sizes, and locations. It has been adopted internationally, with the English version complemented by nine translations").

[18] Draft CSF 2.0 at 3.

[19] CTIA Concept Paper Comments at 31.

[20] Draft CSF 2.0 at 12.

discussions about measurement among key stakeholders.[21] That said, NIST wisely does not provide detailed guidance on how to conduct cybersecurity measurements, and instead refers readers to its *Cybersecurity Measurement* project page and the associated Special Publication ("SP") 800-55: *Performance Measurement Guide for Information Security*.[22] This is the right approach because providing substantive measurement guidance for the wide variety of needs and uses of CSF stakeholders would complicate and lengthen the CSF. NIST should not make further changes to its measurement guidance as it finalizes the Draft.

D. NIST's Discussion of Profiles Is Useful and Appropriate.

NIST's expanded discussion of "Ways to Use Profiles" in CSF 2.0 supports the overall goal of providing voluntary and flexible guidance that can be adapted to more targeted needs. As NIST explains, "Profiles are used to understand, assess, prioritize, and tailor" the CSF Core to an organization's unique needs.[23] The development of profiles facilitates the CSF's widespread use as threats and technologies evolve, so CTIA supports NIST's expansion of the Profile guidance in the Draft CSF 2.0. As CTIA pointed out earlier in the CSF 2.0 development process, NIST's work with stakeholders to build Profiles has been fruitful and should remain a focus.[24]

Profiles are particularly suited to address unique considerations for critical infrastructure sectors. Indeed, as other federal agencies such as the Cybersecurity and Infrastructure Security

[21] *Id*. at 13.

[22] NIST, *NIST SP 800-55 Rev. 2 (Initial Working Draft): Performance Measurement Guide for Information Security*, https://csrc.nist.gov/publications/detail/sp/800-55/rev-2/draft (last visited Oct. 28, 2023).

[23] Draft CSF 2.0.at 9.

[24] CTIA Concept Paper Comments at 6 (encouraging NIST to "expand its profile work"). *See also* Comments of CTIA, Draft NISTIR 8323, Cybersecurity Profile for the Responsible Use of Positioning Navigation and Timing (PNT) Services (filed Nov. 23, 2020), https://www.nist.gov/system/files/documents/2020/12/01/11.23.20%20Comments%20of%20CTIA%20-%20Draft%20NISTIR%208323%20PNT%20Profile.pdf.

Agency ("CISA") develop sector-specific guidance,[25] they should look to CSF 2.0 and collaborate with the private sector to leverage longstanding CSF profiles and mappings that critical infrastructure sectors have already contributed to.[26]

III. NIST SHOULD REJECT CALLS TO CREATE A NEW FUNCTION FOCUSED ON SUPPLY CHAIN RISK MANAGEMENT.

CTIA and members agree that Cyber Supply Chain Risk Management ("C-SCRM") is important and they have demonstrated a commitment to C-SCRM, including by participating in the Department of Homeland Security's ("DHS") Information and Communications Technology Supply Chain Management ("ICT SCRM") Task Force,[27] among other efforts.

Consistent with this commitment, CTIA supports the steps that NIST has taken in Draft CSF 2.0 to address C-SCRM. In particular, NIST added four C-SCRM subcategories: GV.SC-04, GV.SC-06, GV.SC-09, and GV.SC-10, which address assessment and prioritization of suppliers throughout the life cycle of a supplier relationship.[28] NIST also moved the C-SCRM Category's location within the CSF from the Identify Function to the new Govern Function.

While CTIA supports NIST's additional C-SCRM considerations in Draft CSF 2.0, NIST should not further expand its treatment in the CSF. As CTIA has indicated in a separate letter on this topic,[29] C-SCRM is not appropriate for elevation to a Function for CSF 2.0 for a number of reasons. *First*, government guidance on C-SCRM activities continues to evolve, with active

[25] *See* CISA, *Cybersecurity Performance Goals: Sector-Specific Goals* (July 26, 2023), https://www.cisa.gov/news-events/news/cybersecurity-performance-goals-sector-specific-goals.

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

[27] CISA, *ICT SCRM Task Force Members*, https://www.cisa.gov/ict-scrm-task-force-members (last visited Oct. 26, 2023).

[28] Draft CSF 2.0 at 31-32.

[29] Letter from Thomas K. Sawanobori, Senior Vice President & Chief Technology Officer, CTIA, et. al., to NIST, (November 6, 2023) (regarding NIST Cybersecurity Framework 2.0 initial public draft).

workstreams on ICT supply chain risk management and software provenance,[30] among others. Fundamental questions remain unanswered in these spaces, precluding their adaptation into the CSF at this time. *Second*, SCRM risks and considerations can require the involvement of disciplines such as procurement, logistics, quality control, and privacy—these issues go beyond cybersecurity risk management and information security. *Third*, NIST should not make further structural changes to the Framework Core in the move from CSF 1.1 to CSF 2.0. Given the enormous influence that the CSF has had on cybersecurity approaches, standards, and initiatives around the world, any substantive changes to the CSF—including by adding another Function—will require companies and governments to undertake time consuming and expensive updates to systems and policies within their ecosystems.[31] Moreover, substantive updates at this time would increase the likelihood that users will face additional challenges in backward compatibility. [32]

For these reasons, NIST should reject calls to elevate C-SCRM guidance to a Function in the CSF 2.0.[33] Instead, NIST should continue developing additional C-SCRM specific guidance in documents outside the CSF, such as NIST SP 800-161.

IV. AS NIST FINALIZES THE FULL DRAFT CSF 2.0, NIST SHOULD BOLSTER FEATURES THAT HAVE DRIVEN THE DOCUMENT'S SUCCESS TO DATE.

[30] See, e.g., CISA, ICT SCRM Task Force, Securing Small and Medium-Sized Business (SMB) Supply Chains: A resource handbook to reduce information and communication technology risks(Jan. 26, 2023), https://www.cisa.gov/sites/default/files/2023-01/Securing-SMB-Supply-Chains_Resource-Handbook_508.pdf.

[31] CTIA Draft 2.0 Core Comments at 7.

[32] CTIA is aware of proposals recommending the elevation of C-SCRM to a seventh Function. *See* Comments of Cyber Risk Institute, CRI Response to Proposed Changes to the CSF v2.0 Core (filed June 15, 2023), https://www.nist.gov/system/files/documents/2023/08/04/Cyber%20Risk%20Institute%2006152023%20Discussion%20Draft_Redacted.pdf ("CRI Comments"). However, some of these proposals go beyond merely reorganizing and consolidating C-SCRM content to create a new Function. Instead, they propose adding substantive and prescriptive new content, such as recommending documentation of a third party's cybersecurity practices as opposed the organization's own practices. Given the diversity among the types of organizations that rely on the CSF and the evolving best practices in the C-SCRM space, providing flexible and risk-based guidance on these specific proposals at the level required to elevate C-SCRM to a Function would be extremely challenging at this time and would require significant further community input. Such an expansion would also likely result in the adoption of new terminology that would require additional community input and harmonization.

[33] CRI Comments at 1-2.

A. NIST Should Emphasize that the CSF Is Not a Baseline for Regulations.

A key reason that the CSF has enjoyed such success is its voluntary nature. As NIST pointed out in its analysis of community input on its earlier RFI, "[t]he flexible and voluntary nature of the CSF has been beneficial for implementation by organizations of varying sizes and capabilities."[34] Accordingly, in the CSF 2.0, NIST should state clearly that the CSF is not intended or constructed to be the basis for regulatory mandates.

Moreover, calls for NIST to align the CSF with regulations are in tension with its voluntary nature, and are therefore misplaced.[35] While the CSF may be a useful tool for regulated companies and can support reasonable safe harbor protections,[36] the CSF is not well suited for use itself as a regulatory mandate. It provides risk management guidance that should be tailored for each unique context in which it is deployed; it is not a compliance checklist that can be "cut and pasted" from one organization to the next. As the Federal Trade Commission explained in a resource for small businesses, the CSF is "voluntary [and] gives your business an outline of best practices to help you decide where to focus your time and money for cybersecurity protection."[37]

Further, as NIST coordinates with agencies—consistent with calls in the National

[34] NIST, "NIST Updates to the Cybersecurity Framework," (July 13, 2022), at 6, "The flexible and voluntary nature of the CSF has been beneficial for implementation by organizations of varying sizes and capabilities."

[35] The White House, National Cybersecurity Strategy Implementation Plan, at 13 (July 13, 2023), https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov .pdf ("NIST will issue the final CSF 2.0 and provide technical assistance on alignment of regulations with international standards and the NIST CSF, as requested by Federal agencies.").

[36] *See* Ohio. Rev. Code. Ann. §1354.03; *see also* Utah Code Ann. § 78B-4-703.

[37] Federal Trade Commission, "Understanding the NIST Cybersecurity Framework," https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework (last visited Oct. 28, 2023).

Cybersecurity Strategy Implementation Plan[38]—it should take the opportunity to emphasize to regulators the function and purpose of the CSF. As NIST notes in Draft CSF 2.0, the CSF 2.0 Core's outcomes "are not a checklist of actions to perform; the specific actions taken to achieve a cybersecurity outcome will vary by organization and use case, as will the individual responsible for those actions."[39] NIST should emphasize to agencies that the CSF is meant to provide a framework for organizations to follow to build a plan to achieve cybersecurity risk management goals. It is *not* intended to identify or define mandatory actions or outcomes. Educating agencies about the core risk management principles that undergird the CSF, as well as the voluntary and flexible nature of the document, is especially crucial now, in light of recent efforts by other government agencies to use NIST's CSF as a foundational aspect of new mandates.[40] And as noted above, to the extent that sector-specific agencies and other federal agencies want to improve cybersecurity outcomes, NIST should point them to the Profile development process as a proven method to collaborate with the private sector on tailored guidance.

B. NIST's Implementation Examples Are Generally Valuable, Practical, Flexible, and Risk-Based; However, Select Implementation Examples Could Be More Flexible.

With the Draft CSF 2.0, NIST has crafted Implementation Examples that balance the need to maintain flexibility while providing actionable information to users. These Implementation Examples contain "concise, action-oriented processes and activities to help

[38] The White House, National Cybersecurity Strategy Implementation Plan, at 13, (July 2023), https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf.

[39] Draft CSF 2.0 at 4.

[40] *See, e.g.*, *Connect America Fund: A National Broadband Plan for Our Future High-Cost Universal Service Support, et. al*, Final Rule, 88 Fed. Reg. 55918, 55930, (Aug. 17, 2023), https://www.govinfo.gov/content/pkg/FR-2023-08-17/pdf/2023-16674.pdf.

achieve the outcomes of the CSF Subcategories."[41] For example, the Draft includes Implementation Examples in the Govern Function Subcategories that address communication with internal stakeholders about cybersecurity risk.[42] These Implementation Examples are consistent with CTIA advocacy, and help illustrate options for addressing communication with internal stakeholders about cybersecurity risk.[43] Moreover, CTIA supports the current chart format of the Implementation Examples, which is easy to read and illustrates well the relationship between Functions, Categories, and Subcategories.

Building from these helpful additions, NIST should consider adding Implementation Examples related to secure routing and the Border Gateway Protocol ("BGP"). These issues are timely and could be useful to certain CSF user particularly because security work on BGP is inherently multistakeholder and requires flexibility. Improving routing security is a priority under the National Cybersecurity Strategy,[44] and addressing them in the CSF can help to raise awareness of the need for stakeholders to support secure routing. But because the issues are technology and threat specific—not generally applicable outcomes or activities—the Implementation Example section of the CSF 2.0 is an appropriate place for NIST to highlight them in a way that is beneficial and consistent with the Framework's structure and principles; that is, without jeopardizing the core principle of the CSF's technological neutrality. Already,

[41] Concept Paper at 8.

[42] NIST, Discussion Draft of the NIST Cybersecurity Framework 2.0 Core with Implementation Examples, at 2, 5, 10 (Aug. 8, 2023), https://www.nist.gov/system/files/documents/2023/08/07/CSF%202.0%20Core%20with%20Examples%20Discussion%20Draft%5B74%5D.pdf ("Draft Examples") (Implementation Examples at GV.RR-01.Ex2, GV.RM-05, and GV.OC-02).

[43] CTIA Concept Paper Comments at 14.

[44] The White House, National Cybersecurity Strategy Implementation Plan, at 38 (July 2023), https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf.

the Draft CSF 2.0 mentions BGP in the Draft Examples at the Continuous Monitoring Category (DE.CM-01).[45] An additional Implementation Example could be added to the Data Security Category at PR.DS-02, "The confidentiality, integrity, and availability of data-in-transit are protected."[46] The Implementation Example could read: "Ex. 5: Use practices that support secure routing and domain services, as applicable for Autonomous System operators and owners of Internet Protocol ("IP") address space."

While most of the Implementation Examples in Draft CSF 2.0 appropriately balance actionable guidance with flexibility, there are some areas for improvement. NIST should bolster flexibility and avoid prescriptive language in specific Implementation Examples to ensure that the Examples are useful across a range of organizations and contexts. In particular:

- **GV.RM-06.Ex1** provides an example of "[e]stablish[ing] criteria for using a quantitative approach to cybersecurity risk analysis, and specify probability and exposure formulas." Reliance on quantitative formulas—built on assumptions that can easily become outdated—may engender false confidence about the level of cyber-risk exposure a company faces.[47] GV.RM-06.Ex1 may be improved, for example, by substituting "quantitative approach" with "empirical approach" in recognition of the fact that risk analysis may include both quantitative *and* qualitative inputs.
- **GV.SC-02.Ex.3** provides an example of "[c]reating responsibility matrixes to document who will be responsible and accountable for cybersecurity supply chain risk management activities and how those teams and individuals will be consulted and informed." NIST should consider replacing "responsibility matrixes" with "documents" or other synonyms to avoid being overly prescriptive.[48]
- **GV.SC-05 Ex.8** provides the example of "[c]ontractually require[ing] suppliers to vet their employees and guard against insider threats." NIST should clarify the term "insider threats" by adding "both intentional and unintentional."[49]
- **GV.RR-03 Ex.3** provides the example of "[p]roviding adequate and sufficient people, process, and technical resources to support the cybersecurity strategy." NIST should consider changing this Implementation Example to "Provide adequate and sufficient

[45] Draft Examples at 30 ("Ex.1: Monitor DNS, BGP, and other network services for adverse events").

[46] *Id* at 24.

[47] *Id.* at 5.

[48] *Id.* at 6.

[49] *Id*. at 8.

financial, human, technical, and other capital or resources to support the cybersecurity strategy" to give a wider range of examples about the types of resources that organizations may leverage.[50]

- **ID.RA-01 Ex. 5** provides the example of "[m]onitoring sources of cyber threat intelligence for information on new vulnerabilities in products and services." NIST should replace "monitor" with "use" to avoid unduly restricting the means through which an organization obtains and uses threat intelligence.[51]

These modest revisions will help avoid the perception that the Implementation Examples are a prescriptive checklist of required actions.

C. NIST Has Made Important Updates to the Implementation Tiers To More Completely Address Governance Matters.

In general, the Draft's revisions to the Tiers are in line with CTIA's recommendations about maintaining flexibility, and they more fully capture a range of organizational structures, practices, and behavior of current and potential users. For example, in Draft 1.1, Tier 1's description of Risk Management Process included "Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business/mission requirements."[52] Draft CSF 2.0 made the language more general by saying "Prioritization is ad hoc and not formally based on objectives or threat environment."[53] The current version now recognizes that organizations may respond based on objectives or threats but do so in an ad hoc and informal manner.[54]

With respect to governance, CTIA previously recommended that NIST address governance issues in the Tiers.[55] Consistent with this call, NIST's renaming the organizational

[50] *Id.* at 11.

[51] *Id*. at 16.

[52] CSF 1.1 at 9.

[53] Draft CSF 2.0 at 26.

[54] *Compare* Draft CSF 2.0 at 26 *with* CSF 1.1 at 9.

[55] CTIA Concept Paper Comments at 32.

columns of the Tiers in Draft CSF 2.0 to "Cyber Risk Governance, Cyber Risk Management, and Third Party Cyber Risks" appropriately focuses the Tiers on organizational governance and management activities. To build on this, NIST should consider how to widen the scope of the "Third Party Cybersecurity Risks" column to address awareness of cybersecurity risks and threats beyond an organization's supply chain. For example, the "External Participation" Category in CSF 1.1's Tier 3 included language about awareness of, collaboration about, and contribution to cyber threat intelligence and information sharing more generally, rather than specific to an organization's own particular threats and risks.[56]

Additionally, CTIA reiterates the need for NIST to clarify that the Tiers are not intended to serve as a proxy for a maturity model.[57] NIST declared its intent in the Concept Paper to "better describe the relationship between Tiers and maturity model concept[.]"[58] While CSF 1.1 had helpful language to clarify that Tiers do not represent maturity levels, unfortunately that language was removed in Draft CSF 2.0.[59] NIST should follow through on its suggestion in the Concept Paper and explain that CSF 2.0 does not "provide a distinct maturity model to meet CSF outcomes at the Function, Category, or Subcategory level."[60]

Finally, CTIA reiterates its call for NIST to consider adding another Tier between Tiers 3 and 4 for organizations that do not have the resources or expertise to meet the full Tier 4 definition but have the experience and capabilities to evolve beyond Tier 3.[61] This addition

[56] CSF 1.1 at 10 ("The organization understands its role, dependencies, and dependents in the larger ecosystem and may contribute to the community's broader understanding of risks").

[57] CTIA Draft 2.0 Core Comments at 12.

[58] Concept Paper at 14.

[59] *Compare* Draft CSF 2.0 at 13-14 *with* Draft 1.1 at 8 ("While organizations identified as Tier 1 (Partial) are encouraged to consider moving toward Tier 2 or greater, *Tiers do not represent maturity levels*.") (emphasis added).

[60] Concept Paper at 14.

[61] CTIA Concept Paper Comments at 32.

would not require any change to the CSF Core and would promote wider adoption among small and medium-sized organizations.

D. NIST's Proposal to Maintain and Update Informative References Online Will Provide Easily Accessible and Useful Guidance and Avoid Disrupting the CSF Core.

CTIA concurs with NIST's proposal to maintain Informative References in a separate online format while leveraging its National Online Informative References ("OLIR") program.[62] NIST's commitment to regularly updating Informative References, and crowdsourcing their identification, will help address concerns about such references becoming outdated between formal version updates to the CSF.[63]

E. NIST Should Refrain from Making Unnecessary Changes to Terminology and Descriptions.

The Draft includes some minor changes to Subcategory descriptions that do not seem to substantively alter the Subcategory's content. As CTIA has suggested,[64] minor updates nonetheless can create additional mapping work for users and stakeholders, so NIST should consider whether the benefits derived from those changes justify the resources required for an update. This is especially true where changes do not appear to have a substantive underpinning. Examples of proposed minor changes that NIST should reconsider include:

- **GV.OC-04**. "Critical objectives, capabilities, and services that stakeholders *expect* are determined and communicated" became "Critical objectives, capabilities, and services that stakeholders *depend on or expect* from the organization are determined and communicated;"[65] and
- **GV.RR-01**. "Organizational leadership takes responsibility for decisions associated with cybersecurity risks and establishes a culture that is risk-aware, behaves in an ethical manner, and promotes continuous improvement" became "Organizational leadership is

[62] Draft CSF 2.0 at 7.

[63] Concept Paper at 6.

[64] CTIA Draft 2.0 Core Comments at 8.

[65] *Compare* Draft 2.0 Core at 6 *with* Draft CSF 2.0 at 30 (emphasis added).

responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving."[66]

NIST should reconsider these word changes, or in the alternative, provide a more detailed explanation of why the changes are proposed. Doing so would help justify any additional work to revise current uses of CSF 1.1 towards the new CSF 2.0.

F. NIST Should Support Organizations' Transitions to CSF 2.0 By Producing a More Comprehensive Change Analysis.

As CTIA has noted in past advocacy, it is important that NIST clearly explain substantive changes to Subcategories between CSF 1.1, CSF Discussion Draft 2.0, and Draft CSF 2.0.[67] In addition to providing valuable insight to users, explanations serve as a safeguard against mistaken assumptions that may affect outcomes and recommendations.

NIST has provided some helpful resources. The change log included in the Note to Reviewers discusses the main changes in this Draft,[68] and the table depicting the CSF 2.0 Core in Appendix C of the Draft CSF 2.0 helpfully indicates where Categories or Subcategories moved or were consolidated.[69] Still, users would benefit from a more comprehensive and detailed explanations of what has changed between CSF 1.1 and Draft CSF 2.0. To meet this gap, NIST should consider developing a Change Analysis that explains NIST's reasoning behind changes to the text between CSF 1.1 and Draft CSF 2.0, as NIST did for the SP 800-171 Draft Revision 3.[70]

V. CONCLUSION

CTIA supports NIST's Draft CSF 2.0 because it has kept the key features that have made

[66] *Compare* Draft 2.0 Core at 8 *with* Draft CSF 2.0 at 32.

[67] CTIA Draft 2.0 Core Comments at 8.

[68] Draft CSF 2.0 at Note to Reviewers.

[69] Draft CSF 2.0 at 30-44.

[70] NIST, SP 800-171 Rev. 3, Initial Public Draft, Change Analysis (Rev. 2 to IPD Rev. 3), (May 10, 2023), https://csrc.nist.gov/files/pubs/sp/800/171/r3/ipd/docs/sp800-171r2-to-r3-ipd-analysis.xlsx.

the CSF an indispensable global resource for cyber risk management. CTIA applauds NIST for wisely declining to further alter the foundation of the CSF by not creating a new, seventh Function for C-SCRM and by not attempting to address cybersecurity measurement and metrics in the CSF. CTIA appreciates NIST's efforts to add several useful elements to the Draft CSF 2.0, such as Implementation Examples, more detailed guidance on the use of Tiers, and expanded reference materials and capabilities through OLIR. NIST should continue in this approach as it finalizes CSF 2.0, as well as make targeted updates—as described above—to further bolster the process-oriented, risk-based, flexible, and voluntary nature of this critical risk management tool.

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]
www.ctia.org

November 6, 2023