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

In the Matter of)
)
Cybersecurity Framework 2.0) Discussion Draft of the NIST
) Cybersecurity Framework 2.0 Core
)

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

May 31, 2023

Table of Contents

I. INTRODUCTION AND SUMMARY.

CTIA[1] is pleased to collaborate with the National Institute of Standards and Technology ("NIST") as NIST updates the *Framework for Improving Critical Infrastructure Cybersecurity* ("CSF" or "Framework") from its current Version 1.1 ("CSF 1.1").[2] CTIA has participated in the development of the CSF from the beginning, including by commenting on last year's Request for Information ("RFI"),[3] as well as the *NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework*.[4] CTIA welcomes the opportunity for continued engagement with these comments on the *Discussion Draft of the Cybersecurity Framework 2.0 Core* ("Draft 2.0 Core").[5]

Throughout this process, NIST has demonstrated a commitment to an open and collaborative approach to updating the CSF—conducting extensive stakeholder engagement as it

[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] Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, NIST (Apr. 16, 2018), https://doi.org/10.6028/NIST.CSWP.04162018 ("CSF 1.1").

[3] Comments of CTIA, Evaluating and Improving Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management, Docket No. 220210-0045 (filed Apr. 25, 2022), https://www.nist.gov/system/files/documents/2022/05/03/04-25-2022%20-%20CTIA.pdf.

[4] Comments of CTIA, NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework, NIST (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").

[5] Discussion Draft of the NIST Cybersecurity Framework 2.0 Core, NIST (Apr. 24, 2023), https://www.nist.gov/system/files/documents/2023/04/24/NIST Cybersecurity Framework 2.0 Core Discussion Draft 4-2023 final.pdf ("Draft 2.0 Core").

moves towards CSF 2.0, by issuing the RFI,[6] hosting workshops[7] and working sessions,[8] seeking comments on the Concept Paper,[9] and now releasing the Draft 2.0 Core for stakeholder feedback. NIST has also taken important steps—including in the most recent Draft 2.0 Core—to maintain a voluntary and flexible cybersecurity framework that global organizations can use in their information security and risk management activities. As NIST moves forward to draft the full Draft CSF 2.0, it should: take steps to limit negative downstream impacts from wholesale substantive and structural changes to the CSF; retain the CSF's outcome-focused, technology- and threat-neutral approach; ensure that any new content is explicitly flexible; reinforce that adoption of the CSF is voluntary; reject calls to reorganize the CSF or add substantially more detailed guidance to address cybersecurity supply chain risk management or assessment and measurement; provide additional guidance on the use of the Tiers while underscoring that they are not a maturity model; and work to ensure the CSF continues to be an influential foundation for other cybersecurity guidance and standards.

II. NIST'S DRAFT 2.0 CORE TAKES IMPORTANT STEPS TO RETAIN THE CSF'S KEY FEATURES.

A. The Draft 2.0 Core Rightly Keeps the CSF's Process-Oriented Approach and

[6] *Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management*, Notice and Request for Information, Department of Commerce ("DOC") & NIST, 87 Fed. Reg. 9,579, 9,579 (Feb. 22, 2022), https://www.federalregister.gov/documents/2022/02/22/2022-03642/evaluating-and-improving-nist-cybersecurity-resources-the-cybersecurity-framework-and-cybersecurity.

[7] *Journey to the NIST Cybersecurity Framework (CSF) 2.0 | Workshop #1*, NIST (July 15, 2022), https://www.nist.gov/news-events/events/2022/08/journey-nist-cybersecurity-framework-csf-20-workshop-1 (last updated Sept. 8, 2022); *Journey to the NIST Cybersecurity Framework (CSF) 2.0 | Workshop #2*, NIST (Jan. 6, 2023), https://www nist.gov/news-events/events/2023/02/journey-nist-cybersecurity-framework-csf-20-workshop-2 (last updated Feb. 28, 2023).

[8] *Journey to the NIST Cybersecurity Framework (CSF) 2.0 | In-Person Working Sessions*, NIST (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).

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

Is Technology- and Threat-Agnostic.

The Draft 2.0 Core continues to envision the CSF as a framework—not as a substantive set of guidance—for a wide variety of organizations to be able to identify and mitigate cybersecurity risks in a wide variety of contexts. For example, new Functions, Categories, and Subcategories in the Draft 2.0 Core describe outcomes but do not specify the methods by which they are accomplished. Also, the new and edited Categories and Subcategories are not substantially more detailed or specific than they have been in previous iterations of the CSF. Likewise, the Draft 2.0 Core rightly does not focus on specific threats. Rather, it continues to be generally applicable to a variety of risks and threats—including those that may arise in the future. The Draft 2.0 core maintains a technology-neutral approach. New and revised Subcategories describe outcomes at a high level, and limit references to specific types of technologies.[10]

This is the right approach. It is critical to retain the CSF as a process-oriented, threat- and technology-agnostic document, so that the CSF can continue to be a universal and flexible tool for a wide range of organizations. At the same time, this approach helps to ensure that the CSF will be "future-proof" and not become obsolete when new threats and technologies emerge. In particular, CTIA concurs with NIST's decision to reject calls for adding in-depth treatment of specific technological approaches.[11] As NIST has noted, any additional guidance tailored towards specific technologies or applications may be best accomplished by CSF Profiles,

[10] *E.g.*, Draft 2.0 Core at 19 (revising new Subcategory PR.PS-01: "Configuration management practices are applied (e.g., least functionality, least privilege)" from CSF 1.1 Subcategory PR.IP-1: "A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality")).

[11] 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, NIST at 6 (June 3, 2022), https://www.nist.gov/system/files/documents/2022/06/03/NIST-Cybersecurity-RFI-Summary-Analysis-Final.pdf ("RFI Summary").

mappings to specific standards or guidance, or implementation examples.[12]

B. NIST Has Included Helpful Implementation Examples, Reinforcing the Flexible and Risk-Based Nature of the CSF While Providing Practical Examples for Organizations To Use It.

As CTIA has explained in previous comments, the wireless industry supports NIST's proposal—from the Concept Paper—that the CSF 2.0 "will include notional implementation examples of concise, action-oriented processes and activities to help achieve the outcomes of the CSF Subcategories . . . ."[13] It is important for NIST to include notional implementation examples that will provide more detail on certain topics while still maintaining the CSF's structure and flexibility and not disrupting the CSF Core.[14]

The Draft 2.0 Core takes important steps in this direction. It provides a selection of implementation examples for Subcategories from the Identify, Protect, and Detect Functions.[15] These examples offer more options for how an organization might implement a particular Subcategory, while maintaining flexibility. Helpfully, NIST notes that the "examples would not be a comprehensive list of all actions that could be taken by an organization to meet CSF outcomes, nor would they represent a baseline of required actions to address cybersecurity risk."[16] In short, the Implementation Examples represent flexible, notional examples, not prescriptive requirements. Further, NIST's proposed placement of the Implementation Examples within the CSF appears not to disrupt the CSF Core. The Implementation Examples are placed alongside Subcategories in a chart format, enabling readers to maintain a view of the alignment

[12] Concept Paper at 7.

[13] *Id.* at 8 (emphasis omitted).

[14] CTIA Concept Paper Comments at 13.

[15] Draft 2.0 Core at 4-5.

[16] *Id.* at 4.

between Functions, Categories, and Subcategories.[17] As NIST moves to draft the full Draft CSF 2.0, it should ensure that all of its Implementation Examples follow the same approach by remaining flexible and not prescriptive, and by not disrupting the CSF Core in a way that would negatively impact backward compatibility between CSF 1.1 and CSF 2.0.

Additionally, NIST should consider adding more flexible Implementation Examples regarding highly complex cybersecurity operations. In particular, NIST should consider creating additional Implementation Examples for the Govern Function Subcategories that specifically address communicating with internal stakeholders about cybersecurity risk, as NIST suggested in its Concept Paper.[18] Implementation Examples dealing with the new Govern Function may include cross references to other related Functions, Categories, and Subcategories in the CSF Core.

C. The Treatment of Cybersecurity Supply Chain Risk Management in the Draft 2.0 Core Is Appropriate in Scope, Scale, and Detail.

NIST's treatment of Cybersecurity Supply Chain Risk Management ("C-SCRM") issues in CSF 1.1 is appropriate and adequate.[19] Specifically, CSF 1.1 includes a C-SCRM Category and associated Subcategories, addresses C-SCRM in the Tiers, and includes succinct discussion of C-SCRM's role in addressing risk associated with commercial products and across the broader digital economy. However, CSF 1.1 does not include additional in-depth or detailed C-SCRM guidance, which would be overly complex and misplaced. This approach strikes the right balance in dealing with complex and evolving C-SCRM issues.

NIST is right to retain this approach with its CSF 2.0 update and to reject calls to create a

[17] *Id*.

[18] *See* Concept Paper at 12 (discussing providing "examples of how organizations have used the CSF to assess and communicate their cybersecurity capabilities").

[19] *See* CTIA Concept Paper Comments at 29.

new C-SCRM Function or to create a major expansion of C-SCRM expectations.[20] While the Draft 2.0 Core makes some adjustments regarding C-SCRM—namely by moving some C-SCRM Subcategories into the Govern Function,[21] and adding new supply chain-related content in new Subcategories[22]—these updates are appropriate and do not raise the same concerns that wholesale changes to make the CSF more supply-chain specific would raise.

As NIST moves towards a full draft of CSF 2.0, it should maintain this approach. In addition, NIST should consider updating the Informative References and mappings to reflect the most recent work on C-SCRM, including both government and industry efforts. References should include the updated Revision 5 to SP 800-53: *Security and Privacy Controls for Information Systems and Organizations*,[23] the Secure Software Development Framework,[24] the SP 800-161: *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* Revision 1,[25] and other guidance documents developed by industry and government, such as those published by the Department of Homeland Security ("DHS")-hosted Information and Communications Technology ("ICT") Supply Chain Risk Management ("SCRM") Task Force.[26] These updates would address community demand for further treatment of supply chain risks in the CSF without significantly expanding or changing the CSF Core.

[20] *See* Concept Paper at 12.

[21] Draft 2.0 Core at 6-9.

[22] *Id.* at 13.

[23] NIST 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 (last updated Dec. 10, 2020).

[24] NIST SP 800-218, Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities, NIST (Feb. 3, 2022), https://csrc nist.gov/publications/detail/sp/800-218/final.

[25] NIST SP 800-161, Rev. 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, NIST (May 2022), https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final.

[26] *See, e.g.*, Securing Small and Medium-Sized Business (SMB) Supply Chains: A Resource Handbook to Reduce Information and Communication Technology Risks, CISA, ICT SCRM Task Force (Jan. 26, 2023), https://www.cisa.gov/sites/default/files/2023-01/Securing-SMB-Supply-Chains_Resource-Handbook_508.pdf.

III. NIST SHOULD CONTINUE TO WORK TO LIMIT THE DOWNSTREAM EFFECTS OF PROPOSED CHANGES TO THE CSF TO PROMOTE BACKWARD COMPATIBILITY AND CONTINUED FLEXIBILITY.

A. NIST's Decision To Create a Govern Function Will Have Major Downstream Effects.

CTIA supports the inclusion of important governance considerations in the CSF; however, there are still outstanding concerns about the "ripple effect" of the major changes involved with adding "Govern" Function. Specifically, adding a sixth Function to the CSF will create significant work for organizations that have aligned their cybersecurity programs and guidance with the CSF, including government agencies, public-private partnerships, standards bodies, and many private companies. For example, organizations that have used the CSF to inform their own cybersecurity programs will have to update internal assessments and programs, including updating organizational profiles and mappings. These activities are time-consuming and costly and may be particularly burdensome for small and mid-sized organizations. Moreover, the success of the CSF has resulted in other government guidance documents relying on it. For example, DHS Cybersecurity and Infrastructure Security Agency ("CISA") recently updated its Cross-Sector Performance Goals ("CPGs") to map to the CSF.[27] These types of guidance documents, including but not limited to the CPGs, will need to be updated to adapt to the new structure and content of CSF 2.0.

As NIST moves forward with the full draft of CSF 2.0, it should take steps to ensure that the CSF can remain the foundation for organization- and ecosystem-level cybersecurity approaches and to limit the downstream impact from changes to the CSF. Some aspects of the Draft 2.0 Core already work towards this goal—for example, NIST's decision to populate the

[27] CISA, CPG Cross-Sector Cybersecurity Performance Goals, Version 1.0.1, at 7 (Mar. 21, 2023), https://www.cisa.gov/sites/default/files/2023-03/CISA_CPG_REPORT_v1.0.1_FINAL.pdf ("CISA has reorganized the CPGs to align to NIST CSF functions").

Govern Function with existing Categories and Subcategories from other Functions, rather than to add significant new content, will help to mitigate downstream impacts of this significant change. However, other aspects of the Draft 2.0 Core should be reconsidered to avoid unnecessary downstream impacts. Specifically, some proposed changes to Categories and Subcategories go beyond what is necessary. For example, the Draft 2.0 Core consolidates Subcategories PR.AT-2 and PR-AT.5 into a single new Subcategory PR.AT-02.[28] While consolidation has its benefits, the extra work of mapping an additional change may not be worth the benefit of shortening the CSF by one Subcategory.

Overall, in reviewing the proposed changes from CSF 1.1 to the Draft 2.0 Core, NIST should assess whether relatively minor updates will create additional mapping work that may not be necessary. As a guiding principle, NIST should only move or consolidate Subcategories when the associated Category is removed or moved to another Function.

Further, NIST should consider additional practical tools that will help organizations transition from CSF 1.1 to CSF 2.0. For example:

- NIST should include a clear guide labeling which Categories and Subcategories have moved or been updated, and which ones are new. This will provide clear and consistent information about CSF 2.0 and will be especially important for small- to mid-sized companies. The Table released as part of the Draft 2.0 Core is helpful,[29] but NIST should consider ways to better highlight which material is new guidance as it moves forward with the full draft of the CSF 2.0.

- NIST should also look to add explanatory material that addresses the reasoning behind other changes that were not previewed in the Concept Paper. Indeed, even seemingly minor changes such as retitling a Category may result in additional work for organizations in understanding and implementing such changes, so more explanation and clarity is generally helpful. For example, the Draft 2.0 Core modifies Category Adverse Event Analysis (DE.AE) to "Adverse cybersecurity events are analyzed to find and characterize possible attacks and compromises, unauthorized and

[28] Draft 2.0 Core at 16.

[29] *Id.* at 6.

> inappropriate activities, protection deficiencies, and other activity with a potentially negative impact on cybersecurity."[30] In CSF 1.1, this Category was Anomalies and Events (DE.AE): "Anomalous activity is detected and the potential impact of events is understood."[31] NIST should explain its intent behind the language change. Without an authoritative explanation, users of the CSF will have to guess as to the difference between an "anomalous activity" and an "adverse cybersecurity event."

B. Any New Content in CSF 2.0 Should Remain Clearly Flexible.

NIST should make clear that any changes it makes to the CSF are not intended to make the document more prescriptive. As NIST has noted, organizations have unique risks and "will vary in how they customize practices described in the Framework."[32] It is therefore paramount that updates made to the CSF 2.0 reflect the need for tailoring.

Specifically, NIST should ensure that the language in any new Categories or Subcategories is flexible. While the Draft 2.0 Core contains helpful language around flexibility,[33] some of the new content should be adjusted to better reflect this key principle. For example, new Subcategory GV.PO-02 reads "The same policies used internally are applied to suppliers."[34] While in adding this Subcategory NIST appears to be responsive to calls from stakeholders to provide guidance on "supplier relationship management and contracts[,]"[35] NIST should modify the language to include a discussion of risk and business need in applying organizational policies to suppliers. Organizations, particularly large and complex enterprises, will have many different types of suppliers that perform diverse functions and bring varying degrees of potential cybersecurity risk. The preceding Subcategory GV.PO-01 qualifies that

[30] Draft 2.0 Core at 21.

[31] *Id*.

[32] CSF 1.1 at vi.

[33] *See* Draft 2.0 Core at 9 ("GV.RM-03: Risk appetite and risk tolerance statements are determined and communicated *based on the organization's business environment*") (emphasis added).

[34] Draft 2.0 Core at 21.

[35] RFI Summary at 31.

organizational policies should be “based on organizational context, risk management strategy, and priorities[,]”[36] and GV.PO-02 should do the same.

IV. AS NIST PREPARES THE FULL DRAFT CSF 2.0, CTIA REITERATES ITS CALLS FOR THE FRAMEWORK TO PRESERVE THE KEY FEATURES THAT HAVE DRIVEN ITS SUCCESS TO DATE.

The Draft 2.0 Core addresses only a portion of the updated CSF; it does not include any proposed updates to Informative References, Tiers, or measurement and assessment, among other things. Accordingly, there are important issues remaining for NIST to consider as it prepares to release the full Draft CSF 2.0.

A. NIST Should Emphasize the CSF’s Voluntary Nature and Make Clear that It Is Not Designed To Be a Template for Regulation.

Consistent with previous iterations of the CSF, NIST should continue to emphasize that the CSF is purely voluntary for the private sector and should not be used as a template by regulators. Unfortunately, some government efforts have recently expressed interest in doing just that. For example, the National Cybersecurity Strategy cites the CSF as a source document that proposed cybersecurity regulations should “leverage.”[37]

NIST should make clear that any changes it makes to the CSF are not intended to turn the document into a template for regulation and it should continue to highlight that the CSF’s voluntary nature has been an important part of its success.[38] In the full CSF 2.0 draft, NIST should state clearly that CSF 2.0 is not intended to be a used as a basis for regulations.

[36] Draft 2.0 Core at 9.

[37] The White House, National Cybersecurity Strategy, at 8 (Mar. 1, 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

[38] *See* CTIA Concept Paper Comments at 16-17.

B. NIST Should Follow Through with Its Proposal To Provide Substantive Measurement Guidance in 800-55 Rev. 2, Not in the CSF.

In the Concept Paper, NIST states that "[t]he underlying fundamentals of cybersecurity measurement process and implementation will not be included in the CSF, but rather in [SP 800-55 Rev. 2, *Performance Measurement Guide for Information Security* ("800-55 Rev. 2")]."[39] CTIA continues to support NIST's proposed approach in the Concept Paper,[40] and accordingly, has concerns about NIST's statement in the Draft 2.0 Core that it is developing guidance for "the use of the CSF for assessment and measurement."[41]

Rather than develop assessment and measurement guidance under its CSF 2.0 efforts, NIST should continue its plans to deal with the complex issue of measurement in 800-55 Rev. 2. CSF 1.1 already provides general guidance on the purpose of cyber measurement and the ways in which "the cybersecurity outcomes of the [CSF] Core support self-assessment of investment effectiveness and cybersecurity activities[.]"[42] Attempting to update the CSF 2.0 with more substantive measurement guidance than is already provided in CSF 1.1 would overly complicate the CSF. At the same time, providing substantive cyber measurement guidance in 800-55 Rev. 2 will streamline NIST's cyber measurement guidance and avoid the fragmentation that would result if NIST provides substantive measurement guidance in both documents. Keeping measurement guidance in 800-55 Rev. 2—and not in the CSF 2.0—will facilitate ease of use for stakeholders and reduce the risk of confusing the community.

[39] Concept Paper at 14.

[40] *See* CTIA Concept Paper Comments at 31.

[41] Draft 2.0 Core at 2.

[42] CSF 1.1 at 20.

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

Consistent with stakeholder calls for more clarity about the CSF Tiers, [43] NIST should further develop its discussion of Tiers, which serve as a practical framework for implementing the CSF across diverse settings. NIST should consider adding an additional Tier in between the current Tier 3 (Repeatable) and Tier 4 (Adaptive). Adding a Tier between Tier 3 and Tier 4 would facilitate greater adoption of CSF practices by small- or medium-sized organizations. It would also help NIST meet its Congressional mandates.[44] Some of these organizations may not have the resources or expertise to meet the full Tier 4 definition but have the experience and capabilities to evolve beyond Tier 3. This limited update to the CSF 2.0 structure would benefit the target audience—which includes organizations of all sizes—but would not cause negative downstream effects that could result from more expansive changes to the CSF Core.

As NIST updates the Tiers, it should clarify that they are not intended to be used as a proxy for a maturity model. In the Concept Paper, NIST writes that it plans to "better describe the relationship between Tiers and maturity model concepts," but makes clear that "CSF 2.0 will not provide a distinct maturity model to meet CSF outcomes at the Function, Category, or Subcategory" levels.[45] To address this, NIST could provide notional implementation examples of how the CSF can be leveraged to assist an organization with benchmarking its implementation of the CSF across the Tiers. Doing so would help stakeholders better understand how to compare their own practices with others, without making disruptive changes to the Core.

[43] *See* Concept Paper at 14.

[44] *See* Concept Paper at 4.

[45] *Id.* at 14.

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

Given the constantly changing cybersecurity landscape, it is important that NIST continue to establish and support efforts to keep the CSF current, even between formal updates. NIST has recognized that the CSF "is intended to be a living document that is refined and improved over time."[46] There are multiple ways for NIST to achieve this without disrupting the CSF Core. For example, NIST should continue to leverage and promote the Online Informative References ("OLIR") Program.[47] NIST should also work to bolster mappings between the CSF and the documents that are built from or reference the CSF, including international standards. As noted above, this will be especially important to the extent there are key changes made to the CSF Core in CSF 2.0. Finally, NIST should continue to engage with domestic and international stakeholders—with a priority focus on standards organizations—who are developing and deploying cybersecurity standards and best practices.

V. CONCLUSION.

NIST's Draft 2.0 Core keeps what is helpful about the CSF: it is flexible, voluntary, and threat- and technology-neutral. That said, CTIA continues to have concerns about the disruption that will result from adding a sixth function, Govern, and encourages NIST to bolster efforts to limit negative downstream impacts of wholesale substantive and structural changes to this foundational document. Additionally, as NIST builds out CSF 2.0, CTIA encourages it to: reemphasize the voluntary nature of the CSF; reject calls to provide significant new measurement in assessment guidance in CSF 2.0 and instead do so in SP 800-55 Rev. 2; consider

[46] Concept Paper at 3.

[47] *See* NISTIR 8278 Rev. 1 (Draft), National Online Informative References (OLIR) Program: Overview, Benefits, and Use, NIST (Dec. 2022), https://csrc nist.gov/publications/detail/nistir/8278/rev-1/draft.

adding an additional Tier and clarifying the relationship between Tiers and maturity models; and expand and update engagement of the CSF with other guidance and standards.

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

May 31, 2023