ncta
THE INTERNET & TELEVISION ASSOCIATION

Discover all that we do at ncta.com

March 17, 2023

Ms. Cherilyn Pascoe
Senior Technology Policy Advisor & CSF Program Lead
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

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

Dear Ms. Pascoe:

NCTA - The Internet & Television Association (NCTA) submits this letter in response to the request for feedback from the National Institute of Standards and Technology (NIST) on its Concept Paper outlining potential changes to the Cybersecurity Framework (CSF or Framework) in advance of releasing a draft of CSF 2.0.[1/]

As providers of broadband service to millions of American households and commercial businesses, NCTA's member companies are highly motivated to secure and protect their networks. Ensuring that their customers are and feel safe and secure wherever they connect is a top business priority and customer satisfaction necessity for our members. Since its inception a decade ago, cable companies have employed the NIST Cybersecurity Framework as a key resource in their management of cybersecurity and assessment of their cyber defense protocols and practices. The Framework's central construct -- providing companies with the flexibility to tailor the CSF procedures, tools and resources to best comport with their network assets, business operations, and corporate structure – has been vital to enhancing the nation's cybersecurity posture.

Affirming the CSF's Core Principles. As NIST moves into the next stage of promoting and refining the Framework, the core drivers of its success – collaboration with industry, flexible adoption, and voluntary usage – remain critically important. The Framework has become the leading resource across all industry sectors, serving as a comprehensive guide for evaluating cyber readiness and as a compendium of effective cyber defense and risk management processes, techniques, and practices.

1/ *NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework,* National Institute for Standards and Technology, Jan. 19, 2023 ("Concept Paper").

The efficacy of the NIST Framework is grounded in its recognition that there is no "one size fits all" model for addressing cybersecurity risks. The Framework's flexibility, which allows companies to design and develop the best possible security solutions, and adapt them to the particular risk, network architecture, customer environment, and resources, is essential to the success of any cybersecurity program. In the Cybersecurity Enhancement Act (CEA), Congress identified NIST as the ongoing facilitator of the "voluntary, consensus-based, industry-led" Framework, and, in this role, NCTA encourages it to continue to ensure that the Framework provides guidance for organizations to manage cybersecurity risk in an effective and tailored way based on business needs and the evolving cybersecurity landscape.[2/] As NIST previously recognized in connection with the adoption of Version 1.1 of the CSF, the key principles of the CEA – voluntary, consensus-based, industry-led standards, guidelines, best practices and methodologies – formalized NIST's initial work in developing Version 1.0 and are intended to "provide guidance for future Framework evolution."[3/] NCTA encourages NIST to reaffirm these foundational principles - which have been instrumental to enhancing overall cyber readiness – as part of its iteration of Version 2.0 of the Framework.

Promising Elements of the Concept Paper. NCTA believes that some items set forth in Sections 1 and 2 hold significant promise and could enhance and improve Framework usage and adoption. Bolstering efforts to promote Framework adoption and usage across all sectors and regardless of organization size can strengthen our collective defense against cyber threats.[4/] As the Concept Paper correctly observes, "the Framework's key attributes – including its flexible, simple, and easy-to use nature – have been beneficial for implementation by organizations of varying sizes, types, and sectors."[5/] These characteristics, together with the Framework's scalability and capacity for being adapted to a variety of business models, threat environments, and network and information system configurations should enhance the success of any new or additional outreach initiatives promoting CSF usage.

NCTA agrees that greater "international use of the CSF would improve the efficiency and effectiveness of . . . cybersecurity efforts" within the U.S.[6/] Significant cyber threats and risks often arise from interdependent compromises or disruptions that not only cut across organizations but also transcend geographical boundaries. As we have noted previously,[7/] strengthening cybersecurity and resilience against malicious activity is an ecosystem-wide undertaking. Accordingly, the efficacy of policies aimed at bolstering our overall cyber defenses depends upon ecosystem-wide adoption and

---

2/ *See* Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274 § 101(a) (as codified in 15 U.S.C. § 272(c)(15)); *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, National Institute for Standards and Technology, April 16, 2018, at 1.

3/ 15 U.S.C. § 272(c)(15).

4/ Concept Paper at 4.

5/ *Id.* at 5.

6/ *Id.*

7/ *See e.g.*, *Experience With the Framework for Improving Critical Infrastructure Cybersecurity,* Docket No. 140721609-4609-01, National Institute for Standards and Technology, Comments of NCTA, October 10, 2014, at 13; *Promoting Stakeholder Action Botnets and Other Automated Threats*, Docket No. 170602536-7536-01, National Telecommunications and Information Administration, Comments of NCTA, July 28, 2017, at 1-2, 23.

implementation of the risk management processes and tools embodied in the Framework. NIST's intention to increase international engagement and prioritize exchanges with foreign governments as part of CSF 2.0 development, including participating actively in international standards activities that leverage the Framework, are important steps that can help strengthen overall ecosystem security.

NCTA also concurs with the utility of relating the CSF to other NIST Frameworks while keeping them separate and undertaking an ongoing review and update of the CSF's Informative References,[8/] given the rapidity with which new security tools, practices, and protocols can emerge and the continuous evolution of key standards and best practices. The Framework's flexibility and adaptability enables its use in connection with management of a diverse array of risk profiles, including those associated with emerging technologies such as artificial intelligence (AI) and the Internet of Things (IoT). We also agree that the Framework's technology and vendor-neutral approach has been crucial to its success and adoption by a diverse variety of organizations and enhances the likelihood that the CSF's "broad outcomes can continue to be leveraged by organizations regardless of the technology or services they employ."[9/]

Developing a Common Taxonomy for Measurement and Assessment. As noted in the Concept Paper, having a common measurement taxonomy is essential for effective communication of measurement and assessment objectives and outcomes, regardless of the underlying risk management process.[10/] A shared lexicon helps to ensure that the same language is used across different domains, which enables effective collaboration and sharing of knowledge, insights, and lessons learned. An agreed upon methodology for measurements is also key for comparison and assessment purposes. Without identifying means and point of measurement, normalization and comparison can be difficult, regardless of how consistent and well-crafted the measurement lexicon.

NIST can leverage the CSF to support measurement and assessment of cybersecurity programs by not only encouraging a common taxonomy and lexicon but providing definitions for measurement taxonomy. The taxonomy should include but not be limited to terms such as the following:

- Binary
- Continuous
- Dichotomous
- Effectiveness
- Efficiency
- Interval
- Mean
- Median
- Mode
- Nominal

8/ Concept Paper at 6.

9/ *Id.* at 7.

10/ *Id.* at 12.

- Ordinal
- Ordinal-categorical
- Ordinal interval ratio
- Precision
- Range
- Ratio
- Continuous ratio

A common understanding of key measurement lexicon terms that may otherwise vary across different organizations, sectors, countries, and domains can be beneficial for analysts and decision-makers, as it allows them to select the most appropriate type of measurement indicator for their specific need. It also helps to ensure that the data is collected and analyzed accurately, which can lead to better decision-making and outcomes.

It is also important to have a shared understanding of not only the utility of key metrics being employed, but also their limits. For example, ordinal metrics can convey whether one thing is greater than another, but they cannot reliably quantify or convey how much better – or in this instance, how much more secure – one thing might be in relation to another.[11/] There are similar limitations associated with nominal metrics, interval metrics, and ratio metrics – as well as qualitative metrics and range compression probability categories such as low, medium and high.[12/] Further, even a shared understanding of the meaning and limitations of key lexicon terms cannot address the risks associated with misinterpreting or drawing the wrong conclusions from the items or occurrences being measured. For example, if the number of cyber attacks detected by an organization's intrusion detection systems (IDS) rises, that does not necessarily imply that the organization is under attack. The IDS vendor may have a new capability for identifying threats that were there all along but previously went undetected; or when adversaries have changed tactics and are seeking to use the organization's IDS to divert attention from a new vector of attack that more readily evades detection.[13/]

NCTA encourages NIST to continue to use metrics to help Framework users assess their internal progress in managing cyber risks, enhancing cyber readiness, and improving decision-making about security investments, protocols, and operational practices. Metrics should be employed as a tool to support a company's specific performance goals and objectives and improving security and risk management outcomes. As the Concept Paper correctly observes:

11/ M. Carothers, "Why Most People Are Bad at Metrics and How You Can Be Less Bad," Society of Cable Telecommunications Engineers, https://broadbandlibrary.com/why-most-people-are-bad-at-metrics-and-how-you-can-be-less-bad/

12/ *Id.*

13/ *See id.*

> Each organization's risks, priorities, and systems are unique, so the methods and actions used to achieve the outcomes described by the Framework Core vary. As such, measurement and assessment of outcomes vary depending on the context.[14/]

The success or failure of particular cyber undertakings within an organization – such as security training, access controls, new security tools, intelligence capabilities, or modified protocols and practices – may be difficult to quantify because of the challenges associated with pinpointing cause and effect. NCTA agrees that NIST should be wary of endorsing metrics that are susceptible to generating out-of-context conclusions or that would divert attention and resources toward producing expensive, time-consuming reports that offer little insight into the quality and agility of a company's cyber defense posture. Instead, consistent with the fundamental risk management objectives of the Framework, metrics should help each organization user assess the efficacy of its cybersecurity program in relation to its underlying security objectives and business environment.

Performance Goals. NCTA also believes that guidance on a common taxonomy and lexicon for outcome-based cybersecurity performance goals will help an organization's risk management program and use of the Framework. Based upon its current structure, some organizations may misread the Framework as prompting them to focus on moving from their current risk profile toward the Framework tier level that represents their optimal state of cyber readiness. Among many organizations, particularly those that are small, this approach can lead to difficulties in gauging their progress toward that objective or in adapting to – and incorporating – new risk factors as they arise.

Guidance from NIST on how to establish and track internal performance goals would provide better granularity for organizations to assess their progress and success through the use of the Framework and improving their overall cybersecurity posture. A Framework primer on how an organization should develop and articulate its internal, outcome-based cybersecurity performance goals is just as important as having a common measurement taxonomy in terms of promoting effective communication of measurement and assessment objectives. We recommend NIST include this component as it develops the ideas set forth in Section 6 of the Concept Paper.

Moving Cautiously on Governance. NIST should carefully consider the potential for unintended consequences arising from the possible introduction of a new "Govern" Function.[15/] While NCTA appreciates the imperative to align risk management decisions with accountability and authority among organizational leadership and understands the role NIST would like a Govern Function to play within CSF 2.0, there is no one-size-fits-all approach to governance as it applies to cybersecurity risk management. Further, there is inherent friction between the elements of the Framework that have been instrumental in driving its adoption and efficacy – i.e., its flexibility, adaptability to diverse business models and organizational operations, and its orientation around outcomes – and any internal process prescriptions that might become elements of a Govern Function.

14/ Concept Paper at 12.

15/ *Id.* at 10.

To avoid this outcome, NIST should include appropriate qualifying language in any discussion of a Govern Function. For example, the CSF 2.0 should make clear that organizations have a wide array of governamce structures and operational processes, with roles and responsibilities determined by their unique missions and needs. Likewise, risk management decisions may sometimes be forged by key technical and subject matter experts, while at other times may warrant collaboration with a range of organizational leaders with skills and experiences that may cut across all facets of the organization. Flexibility and agility are at the heart of all of the Framework's key Functions, and they should be core elements of any Govern Function to avoid rigid or under-developed risk management decision-making processes. NIST also should ensure that the addition of a Govern Function does not inadvertently lead to counterproductive metrics, particularly among regulators or enforcement bodies that look to NIST's Cybersecurity Framework as an articulation of cybersecurity best practices.

Lastly, to the extent that NIST considers expanding the guidance it offers on cybersecurity supply chain risk management (CSCRM), it should incorporate any such guidance into existing Functions and Categories that already address CSCRM, rather than create an entirely new CSCRM Function or Category. Revamping the CSF to move existing references to CSCRM guidance into its own Function or Category would break the backwards compatibility of the Framework and undermine its agility by unnecessarily burdening those entities that have already successfully adopted the Framework with undue costs to update their cybersecurity programs to align with the revised Framework.

* * * * *

NCTA appreciates NIST's continued efforts to update the structure and content of the Cybersecurity Framework to improve cybersecurity outcomes. We look forward to continuing to collaborate with NIST on refining and improving this important resource for managing cybersecurity risk.

Sincerely,

/s/ Loretta Polk

Loretta Polk
Vice President, Deputy General Counsel
Legal & Regulatory Affairs

/s/ Matthew J. Tooley

Matthew J. Tooley
Vice President, Broadband Technology
Science & Technology

NCTA – The Internet & Television Association

[redacted]