November 6, 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 the Draft Cybersecurity Framework 2.0 (Draft) released on August 8, 2023.[1/]

Ensuring network safety and security via strong cybersecurity practices is a paramount responsibility of NCTA's members offering broadband services. Their business success is tied directly to maximizing customers' network usage and trust through such efforts as enhancing the security of cable modems, integrated access points, and home routers (collectively known as "gateway devices") against malicious activity and other cyber threats. The cable industry and its research and development consortium, CableLabs, are also driving increased Wi-Fi security, including security advances in device onboarding to better ensure that connected devices are added to the home network in a simple, seamless and secure manner[2] and the development of a stronger, PKI-based authentication approach for Wi-Fi device roaming.[3]

NIST's Cybersecurity Framework (CSF or Framework) has been an important tool and resource for our members in connection with their provision of a safe, trusted, and secure network environment.[4]

---

1 Public Draft: The *NIST Cybersecurity Framework 2.0,* National Institute for Standards and Technology, August 8, 2023, https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-20/ipd.

2 https://www.cablelabs.com/blog/nccoe-and-cablelabs-collaborate-to-develop-trusted-onboarding-solution.

3 https://www.cablelabs.com/blog/bringing-wi-fi-security-to-the-next-level.

4 The Framework provides valuable guidance for industry provision of secure connectivity services, and NCTA's members actively utilize it in their cybersecurity programs. In addition to the CSF itself, NIST has provided or is developing useful and effective security profiles and guidance in targeted areas of security in such areas as internet routing security, IoT device security and labeling, secure software development, and securing Wi-Fi routers and other gateway home devices.

In its comments on the Concept Paper outlining potential changes to the Framework,[5] NCTA highlighted promising elements of the updated Framework, emphasized the importance of continued fidelity to the foundational principles of the CSF, and provided input on the discussion of metrics and performance goals, the addition of a new Govern Function, and the treatment of cybersecurity supply chain risk management (C-SCRM).

Benefits of Updating the Framework. NCTA believes that a number of items proposed in the updated Framework hold significant promise and would likely enhance and improve broader usage and adoption of the CSF.

First, expanding the target users of the Framework from critical infrastructure owners and operators to all organizations is an important step that reflects the fact that cyber attacks originate and propagate from a myriad of points within a highly interdependent ecosystem.[6] The growth of cloud computing, the shift to conducting business from remote locations and mobile devices, the increasing interconnection between third-party software service providers and their clients, the exponential proliferation of Internet of Things (IoT) devices, the emergence of artificial intelligence (AI) as a key business operations tool, and the prevalence of cyber-physical systems, have all combined to multiply the breadth of attack surfaces that pose cyber risk threats, and intensified the potential magnitude and impact of such attacks. Holistic approaches to cybersecurity are essential to reduce the likelihood that cyber defense measures successfully implemented in some segments of the ecosystem will be negated by gaps and unaddressed vulnerabilities in others. Broadening the target users of the CSF from critical infrastructure owners and operators to all organizations within the digital ecosystem will appropriately expand the reach of the Framework's guidance, resources, and benefits.

Second, broadening the CSF's potential audience beyond U.S. organizations is another important measure that responds to the interdependent nature of the cybersecurity ecosytem.[7] Cyber attacks are a global problem that must be met with collective and coordinated action domestically and abroad. For example, most botnet attacks originate from outside the U.S., meaning that effective action to reduce such threats requires government leadership to foster globally-scaled solutions and international cooperation. The CSF has proven to be an effective and scalable blueprint for bolstering cyber defense awareness and readiness among businesses in the U.S., many of whom also operate globally or interface with a growing international cybersecurity supply chain and vendor base. Accordingly, it should be treated as a tool for strengthening collective cyber defense on a global scale and in international venues.

Third, NCTA agrees with the intention to more closely integrate the CSF Core and Informative References with other NIST Frameworks and resources. NIST has produced a considerable body of

---

5 Comments of NCTA – The Internet and Cable Association, Marcy 17, 2023, CSF 2.0 Concept Paper (NCTA Concept Paper Comments), https://www.nist.gov/system/files/documents/2023/04/26/2023-03-17%20NCTA_508_redacted.pdf

6 Public Draft, Summary of selected Framework changes from version 1.1 ("Scope of the Framework has been updated to reflect use by all organizations" and modifying the "original emphasis on critical infrastructure").

7 *See id.* ("Original emphasis on securing U.S. critical infrastructure has been modified to focus on organizations all around the world").

work on a wide range of key cybersecurity issues since publication of the original Framework, and integrating those resources and guidance into the updated Framework will benefit all users. Likewise, the addition of Implementation Examples will help provide practical guidance on achieving outcomes described in the Framework, while at the same time preserving the Framework's sector- and technology-neutral approach that "provides organizations with the flexibility needed to address their unique risk, technology, and mission considerations."[8/]

Fourth, the Public Draft's emphasis on continuous improvement,[9/] together with its characterization of metrics as a tool for assessing internal progress are useful practical tweaks that should help promote adoption of the updated Framework. Metrics are best employed to help Framework users assess their internal progress in enhancing cyber readiness and improving risk management strategies, tools, and protocols. They are less useful as a maturity model or as benchmarks for comparison within or across sectors. As the Public Draft recognizes, organizations should customize metrics and use them to help assess and prioritize "progress from Current to Target Profiles."[10/]

Affirming the CSF's Core Principles. Flexible, voluntary standards forged via industry-driven best practices and initiatives have been the cornerstone of successful cyber policy efforts, including the CSF. The Framework has become the leading resource across all industry sectors because of its recognition that there is no "one size fits all" model for addressing cybersecurity risks and its emphasis on voluntary usage and flexible implementation, 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.

The Executive Summary of v 1.1 contextualized the emergence of the CSF against the backdrop of the Cybersecurity Enhancement Act of 2014 (CEA) and the directive to identify "a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks."[11/]

While the Public Draft notes that the CEA established NIST as the ongoing facilitator of the "voluntary, consensus-based, industry-led" Framework,[12/] other references to the voluntary nature of the Framework and its reliance on "business drivers" and objective of managing cybersecurity risk "without placing additional regulatory requirements on businesses" have been curtailed or dropped.[13/] NIST should consider reinstating discussion of these key guideposts, since they have helped drive the

---

8 Public Draft at 1.

9 Public Draft, Summary of selected Framework changes from version 1.1 ("Importance of continuous improvement is emphasized through a new Improvement Category in the Identify Function"); *see also* Public Draft at 10, 21, 32.

10 Public Draft at 12.

11 *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, National Institute for Standards and Technology, April 16, 2018, at 1 (NIST CSF v.1.1).

12 Public Draft at 4.

13 *See e.g.,* NIST CSF v.1.1 at v, 2, 4.

proliferation of the Framework's use across a wide variety of organizations. It should also consider revising this sentence, in lines 89-90 of the Executive Summary to reflect the evolution of the Framework's adoption since its release in 2014:

> "The CSF is a foundational resource that is adopted voluntarily by private entities and through governmental policies and mandates applicable to Federal agencies, contractors, and grant recipients."[14/]

Adoption of a Govern Function. NCTA concurs with the key objectives of the newly proposed Govern function, which is to ensure a holistic, organization-wide approach to cyber risk management and ensure oversight and engagement by senior management in such activities. In establishing this Function, however, NIST should consider the utility of proffering it as the first Function and describing it in the Framework text as the "center of the wheel [that] informs how an organization will implement the other five Functions."[15/]

For nearly a decade, adoption and utilization of the Framework has taken place without a Govern function. To describe this new Function as the foundation for an organization's implementation of the other 5 functions, and to suggest that the effectuation of other functions (e.g., Identify) should be dependent upon the Govern function,[16/] may unwittingly prompt organizations that have already adopted the Framework effectively to engage in an overhaul of their cyber risk management structure and operations. Further, the Govern function is necessarily process-oriented, and does not in and of itself implicate the core cybersecurity enhancing activities of identifying gaps and vulnerabilities and targeting safeguards, tools, and protocols to address them. An effective cyber risk management strategy should emerge from the results of these activities – at least as much as it may from the mission needs and planning processes orientation of the Govern function.

NIST should consider re-framing the Govern function as an operational mechanism for, among other things, promoting a holistic cyber risk management strategy, integrating the effectuation of the five Functions on an organization-wide basis, ensuring that lessons learned are effectively incorporated into its approach to managing cyber risks, and ensuring accountability and engagement of senior management. As NCTA has previously noted,[17/] organizations have a wide array of governance structures and operational processes and a Govern function should not be misconstrued as promoting top-down, risk management operational processes – particularly in connection with a cross disciplinary matter like cybersecurity which benefits considerably from organizational agility and flexibility.[18/]

---

14 Public Draft at 1.

15 *See* Public Draft at 5-6.

16 Public Draft at 5 (Identify Function helps "determine the current cybersecurity risk to the organization. Understanding its assets (e.g., data, hardware, software, systems, facilities, services, people) and the related cybersecurity risks enables an organization to focus and prioritize its efforts in a manner consistent with its risk management strategy and the mission needs identified under Govern").

17 NCTA Concept Paper Comments at 5-6.

18 At other points, the Public Draft appears to contemplate greater horizontal interdependence between each of the Functions in connection with the effectuation of an organization's risk management activities – such that governance

C-SCRM. NCTA appreciates the additional focus and explication of cybersecurity supply chain risk management (C-SCRM) in Section 3.5. We agree that "the primary objective of C-SCRM" should be to "extend appropriate first-party cybersecurity risk management considerations to third parties, supply chains, and products and services an organization acquires, based on supplier criticality and risk assessment."[19/] Framing C-SCRM as an extension of first-party protections to encompass activities of third-party suppliers ensures that activities undertaken to carry out Framework Functions that bolster protection of the first-party organization, will also be extended to third-party suppliers in a seamless fashion – thereby avoiding the creation of two separate review and implementation processes for the organization and its suppliers. In addition, as NCTA noted in comments on the Concept Paper, [20/] restricting the Framework to pull current C-SCRM guidance into its own Function would create backwards compatibility issues for organizations that have already successfully adopted the Framework – on top of a similar, albeit less drastic, dynamic at work in connection with elements of the new Govern Function.

For these reasons, we believe that NIST should refrain from adopting suggestions to establish a separate Extend/C-SCRM Function,[21/] and instead encourage organizations to utilize the additional guidance in Section 3 and gain experience with an incorporation of some C-SCRM activities into the new Govern function.

Internet Routing Security Profile. NCTA members, through CableLabs, have been working to jointly develop a risk-based secure routing profile to provide guidance for addressing the most prominent Internet routing risks faced by Internet service providers (ISPs) and other Autonomous Systems networks (ASes).[22/] The profile is designed to serve both as a benchmark and a tool for ISPs and ASes to advance the security of internet routing. CableLabs will publicly release the profile before the end of this calendar year. A risk-based secure routing profile associated with the CSF would be helpful in raising awareness of the importance of detecting and deterring route hijacks.[23/] Leveraging

---

processes established under the Govern Function can and should be informed by risk assessment activities and priorities that emerge from Identify and Protect activities:

> "For organizations that already assess their cybersecurity risk management practices on a regular basis, the results from recent self-assessments or third-party assessments may provide much of the data needed to create Current Profiles, which capture the as-implemented state of Framework outcomes. Organizations that use the Framework are encouraged to begin with their existing cybersecurity risk assessments and risk management processes."

Public Draft at 12.

19 Public Draft at 17.

20 NCTA Concept Paper Comments at 6.

21 *Cf.* Comments of Cyber Risk Institute, Discussion Draft of the NIST CSF 2.0 Core, June 15, 2023, https://www.nist.gov/system/files/documents/2023/08/04/Cyber%20Risk%20Institute%2006152023%20Discussion%20Draft_Redacted.pdf

22 NIST invites Framework users to submit example profiles designed to provide a roadmap for addressing cybersecurity risk associated with a particular business or organizational activity or operation. https://www.nist.gov/cyberframework/examples-framework-profiles.

the prominence, flexibility, and efficacy of the CSF to address routing security issues could be an effective means of bolstering our collective defense against cyber incidents caused by route hijacks.

* * * * *

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

[23] *See* "Cable Leads the Way in Advancing Secure Internet Routing," July 31, 2023, https://www.ncta.com/whats-new/cable-leads-the-way-in-advancing-secure-internet-routing