INTERNET
INFRASTRUCTURE
COALITION

VIA ELECTRONIC SUBMISSION

March 3, 2023

National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, Maryland 20899

Re: Comments on NIST Cybersecurity Framework 2.0 Concept Paper

I. Introduction

The Internet Infrastructure Coalition (i2Coalition) appreciates the opportunity to submit comments in response to the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0 Concept Paper. Founded in 2012 by a diverse group of Internet infrastructure companies, the i2Coalition is a global organization that supports and represents the companies that build and maintain the Internet's infrastructure. Our members include cloud providers, data centers, web hosting companies, domain registries and registrars, IXPs, CDNs, network protection services, and other foundational Internet enterprises.

The broad composition of our membership empowers the i2Coalition to recognize that cybersecurity awareness, threat assessment, and collective responsibility and action on the part of all public and private Internet stakeholders are vital to maintaining a safe and secure Internet ecosystem. The Cybersecurity Framework (CSF) is an outstanding example of public-private collaboration on an issue crucial to the digital economy and national security. The i2Coalition commends NIST’s drive toward the next-level CSF 2.0 in 2024, building on years of experience and vital input from all stakeholders. We applaud and appreciate NIST’s thoughtful and phased development of the final version of CSF 2.0, initially through an RFI and workshops, now with the Concept Paper public comment cycle, and later with additional public comment and workshop opportunities planned for 2023.

II. Specific Comments

Title, Scope, and International Collaboration (1.1-1.3). The i2Coalition fully supports NIST's proposal in 1.1. to change the official title of the CSF. Through this sensible change, NIST will ensure understanding that the CSF is useful and addressed to all organizations across government, industry and academia, not only "critical infrastructure." Clarity in the name and the text is important not only for U.S.-based entities, but also for the many global organizations and other nations modeling the CSF 2.0 as they work to improve their own cybersecurity practices and policies.

As a trade association representing mostly small- and medium-sized Internet infrastructure providers, the i2Coalition applauds NIST's commitment in 1.2 to increase its efforts and collaboration with stakeholders to ensure that CSF 2.0 is helpful to "organizations–regardless of sector, type, or size–in addressing cybersecurity challenges." (Concept Paper 1.2 at 4). Our members and their small and medium-sized customers will benefit directly from NIST's renewed focus and responsiveness to Congress' directive to consider small business concerns in the CSF. When considering the concerns of small businesses, the CSF 2.0 should account for differences in sector, type, and context, avoiding "one size fits all" approaches. The 1.3 proposal to increase international collaboration and engagement is especially welcome. The digital economy is global and interconnected, and cybersecurity efforts must reflect that reality to be resilient and effective. NIST's commitment to international collaboration and engagement to promote adoption of the CSF by our trading partners will help to keep global market opportunities open and safe for businesses of all sizes. Companies and organizations doing business in other countries can do their part to highlight the CSF 2.0 in those markets and encourage its adoption. Taken together, adoption of the changes outlined in 1.1, 1.2 and 1.3 will clarify, strengthen, and broaden the CSF. These changes will further broadcast a key theme emanating from the valuable stakeholder discussions at NIST's recent (February 2023) Concept Paper workshops: cybersecurity is a *global* team sport.

Details, Tools, and Resources (2.1-2.6). Section 2 proposes balanced changes that do not impair core benefits that the CSF has provided since its inception–most notably its "flexible, simple, and easy-to-use nature." (Concept Paper 2.1 at 5). Preserving those valued attributes bolsters the CSF's utility in helping entities get organized in the most efficient way about their own cybersecurity tools and practices in a world in which "[t]here is no shortage of cybersecurity standards, best practices, checklists, goals, and resources." (Concept Paper 2.1 at 5). We appreciate NIST's Section 2 proposals to help make the CSF 2.0 more accessible to organizations of all sizes. A flexible structure that can include the most current and tailored mappings for specific sectors and technologies will well serve the needs of diverse organizations. Further, maintaining a technology- and vendor-neutral approach in the CSF 2.0, as detailed in 2.6, is vital to its integrity, relevance, and broad long-term adoption.

Implementation Guidance and Website Enhancement (3.1-3.3). In Section 3, NIST's proposals rightly seek to meet the challenge of offering implementation guidance without being prescriptive. They also aptly call out the need to keep in mind "the evolving nature of cybersecurity technologies and techniques." (Concept Paper 3.1 at 8). The guidance offered will be especially valuable to smaller organizations with limited resources as well as entities of every size that have elevated risks. NIST's commitment to flexibility and "notional" implementation examples gives the added advantage of encouraging creative approaches and avoiding closed thinking within the broad stakeholder community. The i2Coalition welcomes NIST's emphasis on templates for CSF Profiles, and on improving its website, including the addition of success stories and use cases. In recognition of the differing implementation guidance needs and risks of organizations, NIST could consider, after reviewing the Concept Paper comments, whether to hold breakout portions at one or more future CSF 2.0 development events to engage with some categories of organizations at a more granular level.

Governance (4.1-4.2). The i2Coalition supports the addition of a Govern Function to the CSF 2.0. A Govern Function can act as a bonding catalyst supporting the other existing Functions of the CSF 2.0 while preventing the creation of risk-ridden silos. With an express and separate Govern Function, the CSF 2.0 should connect with greater impact to optimal cybersecurity practices and outcomes, including accommodating technological evolution, maturation of practices and approaches, consistency, transparency, and accountability. A Govern Function injects a unifying force into the CSF 2.0, and, as NIST noted in 4.1, would allow separation and improved organization within it of certain subcategories of governance-related categories.

Cybersecurity Supply Chain Risk Management (5.1). Supply chain risk management (C-SCRM) poses significant challenges for all organizations, particularly small- and medium-sized enterprises with fewer resources. We support NIST's emphasis on organizations' examination of the similarities and differences between first- and third-party risks and on ensuring that if separate teams perform those reviews, then those teams should share information and coordinate with each other. For technologies such as cloud computing to reach their full potential and offer maximum efficiencies, customers must have trust in their cybersecurity features. In recognition of increased focus on C-SCRM, the i2Coalition agrees that NIST should include additional C-SCRM outcomes to provide more guidance to organizations facing these distinct risks, and Option 1 (further integrating C-SCRM outcomes throughout the CSF Core across Functions) would be an appropriate way to meet that need at this time.

Measurement and Assessment (6.1-6.4). The i2Coalition supports the proposal for NIST to provide more guidance and resources for organizations to use in measuring and assessing their use of the CSF. We appreciate NIST's attention to measurement and assessment tools, as cybersecurity risks are not static, and it would be nearly impossible to improve safety without them.

Within their environments, organizations need to know what is and is not working in their cybersecurity risk management programs. We welcome and applaud the continued flexibility that NIST builds into the CSF for assessment methods by various organizations. Improving communications within organizations between cybersecurity personnel and non-cybersecurity audiences, and setting overall cybersecurity improvement goals that all personnel in an organization will work to internalize and achieve, are core objectives. Clear communications and terminology among and within all levels of an organization go hand-in-hand with implementing the practices, systems, and technology to protect an organization from cyber threats. Concerning the Implementation Tiers, we agree with the suggestion in 6.4 to shift the focus of the Tiers to goals and objectives and to a qualitative assessment incorporated into or based on the outcomes of the new proposed Govern Function.

III. Conclusion

The i2Coalition thanks NIST for its thorough outreach seeking stakeholders' input around the development of the CSF 2.0 and commends NIST's fealty to, among other elements, clarity, flexibility, technological- and vendor-neutrality, and continuous improvement in the process. We look forward to NIST's next steps for the positive evolution to version 2.0 of the CSF, a model of excellence in public-private collaboration that has helped scores of organizations in the U.S. and around the world improve their cybersecurity.

Respectfully submitted,

Christian Dawson
Executive Director
Internet Infrastructure Coalition
[redacted]