VIA ELECTRONIC SUBMISSION

November 6, 2023

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

Re: Comments on NIST Cybersecurity Framework 2.0 Public Draft & Implementation Examples Discussion Draft

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 Public Draft and Implementation Examples Discussion Draft. 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.

Given the broad composition of our membership, the i2Coalition recognizes 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 releasing the next-level CSF 2.0 in 2024, building on years of practical and technical experience and essential input from a diverse range of stakeholders.

II. Discussion

The i2Coalition appreciates NIST's affirmative decision declaring that the CSF 2.0 is explicitly designed to be used by organizations of all sizes and sectors, not just critical infrastructure. We provide comments below on several aspects of CSF 2.0 as currently proposed.

Govern Function is a Fundamental Improvement. The i2Coalition commends NIST's addition of the Govern function to the CSF 2.0 Core in the Public Draft, and applauds NIST's clear visual representation of this new element in the CSF Functions "wheel." Inclusion of a Govern function in the Core sends the clear message that risk management is a holistic and continuous process requiring key leadership involvement inside organizations. Ultimately, the value of adding the Govern function will be understood from future experience in the various ways that the public and private sectors choose to implement it according to their needs and resources. NIST's intentional placement of the Govern function in the CSF 2.0 Core promises to deliver a cross-cutting catalyst for all the other Core functions, resulting in minimizing or eliminating risk-ridden internal silos, and reaching better levels of organizational responsibility and communications that will lead to improved cybersecurity outcomes.

Further Engagement on Cloud Services. The growing use of cloud services by the public and private sector, the different models by which they are provided (e.g., public, private, hybrid, and multi cloud), and the ranges and degrees of associated first- and third-party roles and risks, present unique and complex CSF 2.0 implementation challenges. For cloud services, further engagement on the application of the CSF 2.0 functions, especially the Govern function and its supply chain risk management sub-elements, would be helpful. In addition, cloud

providers and users would benefit from opportunities to assess additional practical examples of how shared responsibility models for cloud services can work in alignment with the CSF 2.0, as well as a further description of the shared responsibility model within the framework itself.

The i2Coalition appreciates NIST's commitment to engage in further work with stakeholders to encourage and enable the production of mappings which support the CSF 2.0. Because of their complexity and growing importance in the digital ecosystem and economy, cloud services are an ideal candidate for this deeper collaborative work. This additional engagement is fundamental to building the broad customer trust required to enable cloud computing technologies to achieve their full potential.

Proper Scope of "Continuous Monitoring" for External Service Providers.

Another area that would benefit from further refinement by NIST involves the practical application of the "continuous monitoring" of "external service providers" (e.g., "cloud-based services, internet service providers, and other service providers") in the Implementation Examples DE.CM-06 (Discussion Draft at 30-31). Continuous monitoring is fundamental to risk management, but it is important to clarify what "monitoring" means in varying contexts. Organizations have different levels of monitoring capabilities when it comes to their own systems and those systems of external service providers. Use of the term "monitor" in relation to external service providers, without more elucidation, could create an unsound expectation of precision, visibility, and internal systems access that is not technically feasible, realistic, or secure. The i2Coalition recommends modifying the language for the external service provider

Example 2 in DE.CM-06 to emphasize the need to be situationally aware, instead of using the word “monitor” because that term could be misinterpreted.

Future Challenges for the CSF 2.0. The impact of rapidly emerging digital technologies, combined with the potential for even broader adoption of the CSF 2.0 within the U.S. and globally, underline the importance of maintaining the CSF’s hallmarks. These include its voluntary, non-prescriptive, risk-based and technology-neutral underpinnings, and its adaptability to address the needs of all organizations regardless of their sector type, size, or technological sophistication.

As NIST works to release the final CSF 2.0 in 2024, it is not too early to consider planning for future updates arising from new circumstances on the horizon, such as the impact on cybersecurity of more extensive, sophisticated uses of AI. The pace of technological change driven by AI and potentially other future developments (such as quantum computing) may demand that supplemental revisions to CSF 2.0 occur earlier and more often in comparison with the timing of the revision processes undertaken for version 1.0.

In addition, as NIST and stakeholders gain practical experience from implementing the CSF 2.0, it is crucial to hold true to its voluntary, non-prescriptive foundation for the private sector, which has been a key part of the CSF’s success. This commitment is especially vital for small and medium sized enterprises (SMEs). If “voluntary” uses of the CSF 2.0 in the real world begin to wear the cloak of “mandates,” then the innovation and adaptability of the CSF tradition will be thwarted. The CSF 2.0 could become a barrier to entry for many SMEs and disincentivize valuable information sharing through implementation case examples across various sectors. The i2Coalition commends NIST for underscoring the voluntary, non-prescriptive, risk-based and technology-neutral intent of the CSF 2.0 numerous times in the Public Draft. Going forward, businesses and other stakeholders depending on and benefitting from the voluntary,

non-prescriptive flexibility and agility offered in the CSF 2.0, together with NIST, should remain vigilant in upholding those essential principles and values as they implement the CSF 2.0 in the marketplace.

Further, as the representative of Internet infrastructure providers operating globally, the i2Coalition agrees with NIST that the CSF's "enduring and flexible nature transcends sectors, technologies, and national borders" (CSF 2.0 Public Draft at 1). We thus urge NIST to commit to fostering continued international adoption of the CSF 2.0.

III. Conclusion

The release of the final CSF 2.0 will be a watershed moment for which NIST and all collaborating stakeholders deserve credit. NIST's continuing outreach to stakeholders of all sizes around the development of the CSF 2.0 is 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. This open communication has helped to improve and modernize the CSF model over time. To that end, the i2Coalition urges NIST in particular to conduct additional engagement with cloud services providers and users to consider some of their unique implementation challenges and concerns. The i2Coalition also looks forward not only to the release of the final CSF 2.0, but to supporting NIST as it creates a future vision for continuing the resilience of the voluntary CSF tradition as digital technologies emerge, develop, and mature, and as the cybersecurity landscape evolves.

Respectfully submitted,

Christian Dawson
Executive Director
Internet Infrastructure Coalition
[redacted]
www.i2Coalition.com