INTERNET
INFRASTRUCTURE
COALITION

COMMENTS ON NIST CYBERSECURITY FRAMEWORK

The Internet Infrastructure Coalition ("i2Coalition") submits these comments in response to the February 22, 2022, Federal Register notice Docket Number: 220210-0045 requesting public input on Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management.

The National Institute of Standards and Technology (NIST) is seeking information to assist in evaluating and improving its cybersecurity resources, including the "Framework for Improving Critical Infrastructure Cybersecurity" (the "NIST Cybersecurity Framework," "CSF" or "Framework") and a variety of existing and potential standards, guidelines, and other information, including those relating to improving cybersecurity in supply chains.

i2Coalition Background

The i2Coalition provides a global voice for the people and companies building the infrastructure of the Internet. We believe that policies supporting an environment of innovation are vital to the continued growth and success of the Internet and Internet infrastructure industry.

The i2Coalition represents a large swath of Internet infrastructure companies and related technology firms. Our membership is a collection of well over one hundred companies that have generated the infrastructure on which the digital economy sits. Members of the i2Coalition, including small and medium-sized enterprises, are key contributors to the growth of U.S. exports of digitally enabled services, which has produced beneficial trade surpluses. As an organization, we believe that the full innovative potential of the Internet can only be harnessed if its inherent openness is preserved and made available to all, not just the giants of the industry.

Collaboration Principles

i2Coalition recognizes that government has an important role to play in cybersecurity. The government's part must, however, continue to work in tandem with the processes and procedures that have led to the most powerful engine for economic growth, and communication, seen in many generations. Security need not come with decreased innovation, less business activity, or limits on the exercise of fundamental human rights. Nor need it curtail the ability of small businesses to enter Internet marketplaces.

In general, this is something that the NIST CSF has historically gotten right. We wish to note that i2Coalition has frequently pointed to the NIST CSF as an example of government standards-setting done right because it is:

a. Done in collaboration with industry
b. Technology agnostic
c. Voluntary
d. Not “one size fits all”

These principles should persist as the NIST CSF continues.

Additionally, we propose the following general principles to guide continued work on NIST’s successful framework.

1. Technology has created a platform for a truly global marketplace. Non-collaborative decision-making and regulation carry with them a high risk of exclusion.
2. Strong regard for the security and privacy of end users builds trust in the companies with whom those end users choose to do business.
3. Private companies and organizations have a passionate and vested interest in solving the growing threat of cyberattacks. They should be encouraged and supported in this goal.
4. Encouraging innovation and economic potential should be at the center of decisions made about cybersecurity.

Conclusion

i2Coalition views the continued evolution of the NIST Cybersecurity Framework as beneficial. Governments should look to the way that NIST has created this framework as a model for collaborating with industry to solve complex problems at a number of different scales.

Cybersecurity risk management practices are still in their infancy, and we expect that the NIST Cybersecurity Framework will continue to adapt and change. i2Coalition looks forward to an ongoing dialogue that can help the NIST Cybersecurity Framework continue to mature and improve.