Cherilyn Pascoe
Senior Technology Policy Advisor
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Via e-mail to cyberframework@nist.gov

March 3, 2023

Ms. Pascoe,

BSA | The Software Alliance appreciates the opportunity to continue to engage with the National Institute of Standards and Technology (NIST) on its forthcoming updates to the NIST Cybersecurity Framework. BSA appreciates your deep and ongoing engagement with industry to ensure that the NIST Cybersecurity Framework continues to deliver value to the cybersecurity community by helping organizations manage cybersecurity risk.

BSA is the leading advocate for the enterprise technology sector. Our members are among the world's most innovative companies and help to drive digital transformation by providing the solutions that make businesses and governments more competitive and effective, including cybersecurity, cloud computing, customer relationship management, human resources management, data analytics, manufacturing, infrastructure, and identity and access management tools and services.

As we shared in our April 25, 2022, response to NIST's Request for Information (Docket Number 220210-0045), "Too often documents increase in volume but decline in value." We continue to urge NIST to include only those outcomes and activities that NIST and its stakeholders identify as the most important. BSA understands that limiting the length of the NIST Cybersecurity Framework will be a challenge, but in meeting that challenge, NIST will create value for its stakeholders.

Within that context, BSA is generally supportive of the changes identified in the NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework and provides the following more detailed responses.

[redacted]

1.3 Increase international collaboration and engagement
BSA agrees that it is important for NIST to increase its international collaboration and engagement, particularly surrounding the NIST Cybersecurity Framework. This effort should, of course, include ongoing work in standards development organizations.

More broadly, NIST should prioritize encouraging laws and policies that recognize cybersecurity is an ongoing risk management activity. As BSA noted in our 2023 Global Cyber Agenda, “Returning to the prescriptive, compliance-based checklists of the 20th century will provide malicious actors more opportunities to launch successful cyber attacks.”

2.6 Remain technology- and vendor-neutral, but reflect changes in cybersecurity practices
BSA agrees that the NIST Cybersecurity Framework should remain technology- and vendor neutral. As BSA noted in our 2023 Global Cyber Agenda, outcome-based laws and policies incentivize companies to develop new, better, and more cost-effective cybersecurity solutions.

As NIST notes in its concept paper, identity management is a critical topic. It is particularly important that NIST aligns the Cybersecurity Framework, and the documents it references. For example, NIST Special Publication 800-63, Digital Identity Guidelines, should, like the NIST Cybersecurity Framework, continue to support technology- and vendor- neutral approaches.

4.1 Add a new Govern Function
BSA supports NIST adding this new function. Adding a govern function will support NIST, the US Government, and the entire cybersecurity community’s long-running efforts to elevate and maintain cybersecurity risk management as a function undertaken by an organization’s leaders. Too often, an organization’s leaders do not see their roles reflected in the identify, detect, protect, respond, or recover functions. Adding a govern function would more clearly indicate the activities an organization’s leaders should undertake.

5.1 Expand Coverage of supply chain
BSA agrees that NIST should highlight the importance (and challenge) of managing cybersecurity supply chain risks but cautions that this effort risks overwhelming the NIST Cybersecurity Framework. For example, NIST Special Publication 800-161, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, is more than three hundred pages. As discussed above, it is NIST’s ability to limit the Cybersecurity Framework to the most important outcomes and activities that creates value.

[redacted]

As a practical matter, NIST should consider simply highlighting that an organization should, in the words of Special Publication 800-161, have “a systematic process for managing exposure to cybersecurity risks throughout the supply chain and developing appropriate response strategies, policies, processes, and procedures.” NIST can point to other documents, like Special Publication 800-161, to provide guidance on how to manage those risks.

6.1 Clarify how leveraging the CSF can support the measurement and assessment of cybersecurity programs

BSA supports NIST clarifying how the Cybersecurity Framework can support the measurement and assessment of cybersecurity programs. As a national metrology institute, advancing measurement is a particularly valuable role for NIST to play. Measuring cybersecurity is extremely challenging because organizations undertake cybersecurity activities in a complex ecosystem in which multiple, diverse actors interact and adapt. NIST should explicitly communicate the challenges and limitations of measuring complex systems.

Conclusion

BSA generally supports the changes NIST identified in its concept paper. We look forward to continuing to work with NIST as it develops version 2.0 of the NIST Cybersecurity Framework.

Sincerely,

Henry Young
Director, Policy

[redacted]