March 3, 2023

Via Electronic Mail

National Institute of Standards and Technology
10 Bureau Drive
Gaithersburg, MD 20899
cyberframework@nist.gov

Re: Concept Paper: Potential Significant Updates to the Cybersecurity Framework

Ladies and Gentlemen:

The Bank Policy Institute ("BPI")[1], through its technology policy division known as BITS[2], appreciates the opportunity to comment on the National Institute of Standards and Technology's (NIST) *Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework*.

Since its inception, the Cybersecurity Framework (CSF) has served as a foundation for organizations of various shapes and sizes to better understand, prioritize, manage, and communicate cyber risks. Beginning in 2015, more than 300 financial institutions, trade associations and academic experts began working together to leverage the CSF as the base for what is now known as the Cyber Risk Institute (CRI) Financial Sector Profile, which consolidates existing financial sector regulatory requirements and other standards such as ISO into a unified approach for assessing cyber risk.

Elevating Governance and Supply Chain Risk Management
We are pleased to see that NIST plans on elevating governance to a new function and also plans on emphasizing the importance of supply chain risk management. The CRI Profile uses the CSF as its base and elevates "Governance" and "Supply Chain/Dependency Management" to functions in recognition of the important role they play. Governance is foundational to cyber risk management and helps establish organizational structures, policies, and oversight that support an effective cyber risk management program and a continuous cycle of improvement. Cyber risk management requires an enterprise-wide approach and a culture of awareness that starts at the top and must be cultivated throughout the organization. Active engagement by CEOs and boards of directors with appropriate policies and procedures, regular testing and evaluation, investment and improvement are critical elements.

---

[1] The Bank Policy Institute is a nonpartisan public policy, research, and advocacy group, representing the nation's leading banks and their customers. Our members include universal banks, regional banks and the major foreign banks doing business in the United States. Collectively, they employ almost 2 million Americans, make nearly half of the nation's small business loans and are an engine for financial innovation and economic growth.
[2] BITS – Business, Innovation, Technology, and Security – is BPI's technology policy division that provides an executive level forum to discuss and promote current and emerging technology, foster innovation, reduce fraud, and improve cybersecurity and risk management practices for the nation's financial sector.

Similarly, given the interconnected nature of our economy, cyber risk management must extend beyond the perimeter of a company or an organization to include critical third-party or vendor relationships. The complex nature of third-party relationships often requires assessment and oversight by separate teams within an organization. The importance of third-party risk management and the need for greater efficiency and clarity in roles and responsibilities is a key focus of financial institutions and regulators around the globe. We believe elevating supply chain risk management to a function is appropriate and would highlight its importance and impact on cybersecurity risk management. On this point, we encourage NIST to leverage the work being done by CRI as it updates the Profile. For instance, the next version of the Profile will incorporate supply chain related elements such as procurement planning, due diligence, contract negotiations, ongoing monitoring, and relationship termination in a separate function, address governance of supply chain risks in the Governance function and cover software acquisition, integrity and authenticity in the systems development life cycle-related categories under the Protect function.

Supporting Measurement and Assessment

Measuring and assessing the effectiveness of cyber risk management programs is a continued area of interest among financial institutions. It would be beneficial if NIST would provide various examples of how organizations have used the CSF to (1) communicate their cyber risk management program capabilities and effectiveness to internal and external partners, and (2) develop scalable methodologies to ingest various supplier (and their Nth parties) measurements and assessments into an enterprise program. It would also be valuable if NIST could develop a set of characteristics or attributes upon which sound assessment and maturity approaches could be further developed.

Continue to Encourage Alignment with the CSF in the Development of New or Updated Cyber Polices

Policymakers at federal, state, and international levels are continuing to mature and expand a variety of cyber-related guidance, rules, and policies. Since its inception in 2014, the CSF has helped create a common framework for cyber risk management and enabled cross-sector, public-private coordination on cyber risks. We applaud NIST's extensive collaboration with other agencies, including internationally, and encourage other government agencies to leverage and align their work to the CSF to avoid unnecessary duplication, fragmentation, or confusion. Many organizations have adopted the CSF and the CRI Profile, in some cases using it to help brief senior management and the board of directors. The addition of new performance goals or guidelines that are similar but use a different approach risks confusion or delay and diverts attention away from addressing cyber threats and achieving desired outcomes.

BPI/BITS appreciates the opportunity to comment on the Concept Paper and NIST's ongoing collaborative efforts to update the CSF. The continued evolution of the CSF including efforts to make it easier to use through linkages to other frameworks and the use of online informative references that can be updated more readily will contribute to the value the CSF provides to organizations. If you have questions or would like to discuss these comments further, please contact Heather Hogsett at heather.hogsett@bpi.com.

Sincerely,

/s/Heather Hogsett
Heather Hogsett
SVP, Technology & Risk Strategy, BITS
Bank Policy Institute