



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 BITS², 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.

