June 23, 2023

Via Electronic Mail

National Institute of Standards and Technology
10 Bureau Drive
Gaithersburg, MD 20899

Re: Discussion Draft of the NIST Cybersecurity Framework 2.0 Core

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) *Discussion Draft of the Cybersecurity Framework 2.0 Core*.

The Cybersecurity Framework (CSF) has supported both public and private sector efforts to inform and prioritize cyber risk management strategies. The CSF also serves as the foundation for the Cyber Risk Institute's (CRI) Financial Sector Profile (Profile), which leverages the CSF's controls, but also integrates regulatory requirements unique to the financial sector. Since the CSF was last updated in 2018, threat actors have increasingly targeted vulnerabilities in software supply chains to maximize the breadth and impact of their attacks. To ensure the CSF's continued adaptability to evolving cyber risks, we recommend that NIST: (1) elevate supply chain risk management; and (2) align CSF version 2.0 with current cyber policies and requirements.

Importance of Elevating Supply Chain Risk Management

We commend NIST for elevating governance to a new function in its latest CSF Framework Core 2.0 discussion draft. Implementing effective cyber risk management practices requires CEOs and boards of directors to be aware of the vulnerabilities facing their organizations and engaged in overseeing risk

[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.

management strategies. Developing sound risk management policies in the current cyber threat environment is imperative, but it is equally important to develop appropriate oversight structures to ensure those policies are adhered to. The new "govern" function will help generate the executive level buy-in and support needed to drive enterprise-wide improvements.

We also appreciate NIST including considerations for supply chain risk management throughout its CSF 2.0 Core. Expanding supply chain risk management controls in this way will help organizations better assess and account for third-party risk. Nevertheless, and due to the increased prominence of supply chain vulnerabilities in our interconnected economy, we encourage NIST to add an additional supply chain function. Creating this new function would allow organizations to efficiently reference and implement supply chain controls without having to search for each discrete control dispersed throughout the framework. We noted from other comment letters that most organizations agree supply chain risk management is important, but commenters also believe it does not need its own function because supply chain controls span across existing functions. While supply chain risk management controls are accounted for within various functions, a single, unified view of those controls would decrease complexity and better equip organizations to implement supply chain risk management programs. Additionally, as noted in CRI's response, if NIST does not establish a supply chain function, it should create some mechanism to make those controls readily accessible for organizations as they consult the CSF.[3]

Alignment with New Cyber Policies and Requirements

Recent incidents like the MOVEit breach, and the attacks against SolarWinds and Kaseya forced regulators and policymakers to appreciate the far-ranging impact of supply chain attacks. Establishing a supply chain risk management function would mirror the current attention dedicated to this issue. For instance, the Biden Administration's recent National Cybersecurity Strategy identified securing global supply chains as a strategic objective saying, the "dependency on critical foreign products and services from untrusted suppliers introduces multiple sources of systemic risk to our digital ecosystem."[4] The prudential banking regulators also recently issued guidance on the topic emphasizing "a banking organization can be exposed to adverse impacts, including substantial financial loss and operational disruption, if it fails to appropriately manage the risks associated with third-party relationships."[5] This focus on supply chain considerations will continue for the foreseeable future and updates to the CSF should reflect that reality.

BPI/BITS appreciates the opportunity to comment on NIST's Cybersecurity Framework 2.0 Core discussion draft. The CSF has been a valuable resource to organizations striving to better address cyber risk. To preserve this value, we recommend that NIST adopt a forward-looking approach that fully considers the dynamic cyber threat environment. If you have questions or would like to discuss these comments further, please contact Heather Hogsett [redacted]

[3] Cyber Risk Institute, Comment Letter on NIST Cybersecurity Framework Core 2.0 Discussion Draft (Jun. 15, 2023).
[4] EXEC. OFFICE OF THE PRESIDENT, NATIONAL CYBERSECURITY STRATEGY 32 (2023).
[5] Interagency Guidance on Third-Party Relationships: Risk Management, 88 Fed. Reg. 37927 (Jun. 9, 2023).

Sincerely,

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