April 25, 2022

Via Electronic Mail

National Institute of Standards and Technology
100 Bureau Drive
Stop 2000
Gaithersburg, MD 20899
CSF-SCRM-RFI@nist.gov

Re: RFI: Evaluating and Improving Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

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 request for information issued by the National Institute of Standards and Technology ("NIST") regarding the proposed Cybersecurity Framework ("CSF") update.

When first published in 2014, NIST stated that the CSF would exist as a living document and go through ongoing updates based on industry stakeholder feedback. In the ensuing years, the CSF has helped create an effective common framework for cyber risk management and enabled cross-sector, public-private coordination. It has also spawned useful private sector enhancements such as the Cyber Risk Institute ("CRI") Profile, which extends the CSF in important areas such as governance and supply chain/dependency management and connects controls to both technical and financial industry regulatory guidance for firms to follow. However, both the day-to-day and strategic cybersecurity landscape of 2022 are vastly more complex than those of 2014. As a result of this more active and intense operating environment, it is imperative that the CSF continues to revise to meet these new challenges and remain a tool for users to identify, respond to, and if needed recover from threats. It is also important to ensure that future revisions do not add complexity and remain focused on technology and cybersecurity risk management.

We Support Maintaining the Incremental Adaptability and Agility of the NIST CSF to Reflect the Evolving Cybersecurity Landscape

[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.

The NIST CSF is valued for several reasons, including for providing firms an ability to catalog and characterize risk from front line personnel all the way up to the boardroom, as well as its adaptability and agility when identifying new threats and responding to a changing cybersecurity landscape. A cybersecurity framework, as intended by NIST, is meant to be incrementally modified and updated as its ability to successful identify and respond to risk changes. Therefore, we support NIST's willingness to evaluate the current state of the cyber threat environment and corresponding cyber risk management framework to ensure that industries can meet the evolving challenges they face since the CSF was first introduced.

As an example, whether SolarWinds, Microsoft Exchange, or Log4j, supply chain and third-party risks have grown in frequency and have been spread globally, particularly as we have migrated to more digital technologies and become more and more interconnected. Understandably so, practitioners and regulators have been increasingly concerned with supply chain relationships and the roles and responsibilities for those who manage cyber risk management processes. As NIST considers how to revise the CSF, we urge it to give priority to adapting to these new areas of concern.

Beyond addressing new challenges, continuously assessing governance is critical for cyber risk management, and it helps enable and ensure the success of an organization implementing critical functions and associated controls. Although the NIST CSF v1.0 discusses governance and dependency management activities, the discussion is only contained as supporting information in the text, and not elevated to reflect its growing importance. Additionally, the private sector is increasingly looking for standards that more closely tie aspects of business risk management like cybersecurity and enterprise risk management principles together to ensure that cyber risk is understood within the context of other business risks. NIST could better ensure that the CSF is adopted by the private sector through an integration of these principles. As a result, it is important for NIST to consider establishing functions that support the activities conducted, such as aligning cybersecurity and enterprise risk management[3]. This will provide firms with a model that helps ensure an organization understands supply chain dependencies and enhances its governance processes for cyber risk management.

Simplicity is Vital to Facilitating Future International Acceptance and Private Sector Adoption

In addition to ensuring that the CSF appropriately guides organizations to develop best practices internally, it is also important to update the CSF to maintain a high level of coordination and alignment between different domestic and foreign jurisdictions, with the goal of establishing a common understanding of key cyber risk management elements. As Congress, regulators, and other policymakers seek to strengthen cybersecurity through new requirements or guidelines, it would be exceedingly useful to coordinate these policies with the updated CSF to align and avoid unnecessary duplication, fragmentation, and complexity. Simple and appropriately scoped updates will help ensure cybersecurity personnel can utilize the CSF to focus on their core mission – protecting their organizations – rather than burdensome or duplicative regulatory compliance.

[3] https://csrc nist.gov/publications/detail/nistir/8286/final

Countries around the world have been interested in the CSF and some have adapted it into their own cybersecurity frameworks. NIST should continue to promote the CSF and sector-specific profiles internationally to facilitate acceptance among international government bodies and regulators. Likewise, it is important for NIST to balance new additions with the understanding that organizations around the world have already previously adopted the CSF into their risk management practices, and therefore new additions should be calibrated to reflect the evolving landscape but also be principle-based to ensure that organizations are implementing sound practices without chasing multiple new risk management requirements. A continued focus on simplicity will help to achieve this and we encourage NIST to make updates to the CSF in a manner consistent with the current CSF so that it remains easily understood and adaptable. This approach will have the concurrent benefit of supporting sector specific customizations, such as the CRI Profile, that capture the unique needs and subtleties of a sector and meaningfully connected to cybersecurity risk management.

Once again, BPI/BITS appreciates the opportunity to comment on this request for information. If you have questions or would like to discuss these comments further, please reach out to Brian Anderson at [redacted]

Sincerely,

Christopher Feeney
EVP and President, BITS
Bank Policy Institute