


July 7, 2023



To Whom It May Concern:

JPMorgan Chase & Co. appreciate the opportunity to comment on National Institute for Standards and Technology's (NIST's) Discussion Draft of the Cybersecurity Framework (CSF) Core 2.0. We believe NIST has made great strides to make the next version of the CSF forward-looking, clear, address developments in technology and risk, and improve alignment with national and international cybersecurity standards and practices. However, NIST has a missed opportunity in not recognizing Supply Chain risk as chief among threats to both public and private sector, thus warranting a distinct Supply Chain function.

We strongly applaud NIST for elevating Govern as a Function in CSF 2.0. This critical addition demonstrates acute awareness of the integral role governance plays in the realm of cybersecurity risk management. By instilling principles of good governance, organizations will enhance their cybersecurity posture and further ensure a secure and resilient global ecosystem.

Organizations of all sizes and sectors operate in an increasingly complex and interconnected global ecosystem and economy. The future threat landscape will include increased threats and attacks on cyber supply chain. This has brought urgency to both public and private sector to mitigate associated risks and have principles- and risk-based guidelines to do so. We commend NIST for addressing supply chain risk management in the CSF 2.0 Core, but we strongly believe the framework will be more effective and efficient by elevating supply chain considerations into a new and distinct Supply Chain Function.

This elevated distinction is imperative to progressing a comprehensive security baseline and ensuring alignment to jurisdictional and industry developments in a manner that is accessible and practical to organizations of all sizes. One of the tremendous values of the NIST CSF and, by extension, the Cyber Risk Institute (CRI) Profile, is its intuitive nature and its ability to absorb new controls to mitigate threats as the cybersecurity threat and technology landscape changes.

To reemphasize, supply chain risk management is a fundamental element of a holistic cybersecurity program. By reconfiguring the existing framework, NIST has the opportunity to help institutions substantially sharpen visibility into supply chain risk considerations and clarify key steps for managing supplier lifecycle. By delineating a separate function, NIST will simplify and enhance the user experience by offering a distinct, integrated resource for organizations to address and reduce supply chain risks. In light of these benefits, the question is not whether we can afford to implement this change, but rather if we can afford not to uplift the CSF to proactively address key threats and attacks in our multipolar and ever-

JPMORGAN CHASE & CO.

changing threat landscape that cybersecurity professionals are busy facing every day.

We urge NIST to create a separate Supply Chain Function to address the growing importance of supply chain risk management considerations, as called for by the CRI.

Sincerely,

Pat Opet
Chief Information Security Officer