[redacted] [redacted]

Subject: Proposed Changes to the CSF v2.0 Core
Date: Friday, June 16, 2023 8:04:16 AM
Attachments: image001.png

To Whom It May Concern:

I appreciate the opportunity to provide comments to the National Institute for Standards and Technology's (NIST) Discussion Draft of the Cybersecurity Framework Core 2.0. I commend the continued efforts of NIST to ensure that the next version of the CSF is forward-looking, clear, addresses developments in technology and risk, and improves alignment with national and international cybersecurity standards and practices.

I appreciate that NIST included a "Govern" Function in the next version of the NIST CSF. I know that good governance is critical for cyber risk management, and it helps enable and ensure the success of an organization implementing the other critical functions and associated controls.

Additionally, I commend NIST for addressing supply chain risk management in the CSF 2.0 Core, but we believe NIST could do so more effectively and efficiently for organizations by creating a new Supply Chain Function. One of the tremendous values of the NIST CSF and, by extension, the Cyber Risk Institute (CRI) Profile, is its ability to absorb new controls to mitigate threats as the cybersecurity threat and technology landscape changes. However, without a Supply Chain Function, the CSF risks not keeping pace with the ever-evolving cybersecurity landscape that practitioners are busy facing every day.

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

Thank you,

James Maxwell
Chief Information Security Officer
Amalgamated Bank of Chicago
[redacted]
www.aboc.com

AMALGAMATED
Bank of Chicago

[redacted]