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

The Financial Services Sector Coordinating Council (FSSCC) is pleased to comment on the National Institute of Standards and Technology's (NIST) Request for Information on the Cybersecurity Framework (CSF). The FSSCC is a strong supporter of the CSF —having developed a sector-specific CSF-based risk assessment model— and offers the following comments to further strengthen its usefulness and reflect today's threat environment.

The FSSCC was established in 2002 by financial institutions to work collaboratively with key government agencies while coordinating critical infrastructure and homeland security activities within the financial services industry. The FSSCC works across the financial services sector to strengthen resiliency against attacks and other threats to the nation's critical infrastructure by proactively identifying threats, promoting protection, driving preparedness, collaborating with the U.S. Federal government, and coordinating crisis response – for the benefit of the financial services sector, consumers, and the USA. The FSSCC and its members were actively engaged in the formation of the CSF and have promoted its use and adoption across the financial sector.

Beginning in 2016, more than 300 financial institutions, trade associations and academic experts began collaborating to develop the Financial Sector Profile, now known as the Cyber Risk Institute Profile (CRI Profile), to consolidate existing regulatory requirements and standards such as ISO, into a unified approach for assessing cybersecurity risk. The CRI Profile uses the NIST CSF as the base and elevates certain categories from the "Identify" function to a new "Supply Chain/Dependency Management" function and a "Governance" function, both of which have been focus areas for financial regulatory agencies. In this regard, the NIST CSF, the CRI Profile, and other similar risk based tools have been useful to help financial institutions of all shapes and sizes assess their cyber risk and manage the myriad of financial regulatory requirements through a unified approach.

In light of recent cybersecurity events such as the SolarWinds, Microsoft Exchange server, and Log4j incidents and the rise of ransomware attacks, as well as increased focus by U.S. and international regulators and policymakers on strengthening cybersecurity, we offer the following recommendations to strengthen the CSF and its applicability to today's threat environment:

- **The CSF should elevate governance and dependency management to functions to better reflect their importance.**
  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.

  Similarly, recent cyber events have highlighted the importance of organizations understanding their use of and dependency on third parties. Given the interconnected nature of our economy, cyber risk management must extend beyond the perimeter of a company or an organization to include critical third party or vendor relationships. While both of these concepts are included in the CSF, elevating them to functions would highlight their importance and more appropriately reflect their relevance to the current threat environment.

- **NIST should work across the U.S. Government and with state authorities to encourage the alignment of new and emerging cybersecurity requirements with the CSF.**
  By creating a common framework and definitions for cyber risk management across all types of organizations, the CSF helps establish a common understanding of key elements for effective cyber risk management which supports coordination and communication across critical infrastructure sectors and with government partners – something that is critically important when planning for or responding to significant cyber events.

  As Congress, regulators, and other policymakers seek to strengthen cybersecurity through new requirements or guidelines, it is vital that these policies leverage and align to the CSF to avoid unnecessary duplication or fragmentation and ensure cybersecurity personnel can focus on protecting their organizations rather than filling out compliance questionnaires. For example, the FSSCC has encouraged the Cybersecurity and Infrastructure Security Agency (CISA) to align the new Common Baseline Cybersecurity Performance Goals and the Sector Specific Cybersecurity Performance Goals to the CSF and the CRI Profile, respectively. Many organizations have adopted the CSF and the CRI Profile, in some cases using it to help brief senior management and the board of directors. Adding a similar set of guidelines or requirements that use a different approach, risks creating confusion and diverts attention away from addressing cyber threats rather than promoting desired outcomes.

- **NIST should continue efforts to encourage international adoption of the CSF.**
  For global companies, the ability to take an enterprise-wide approach and adopt a common cyber risk management assessment improves communication across the firm and with international regulatory authorities. A consistent and aligned approach to supervision of cyber risk enhances the stability of the global financial system and improves regulators' ability to understand cross-border risks.

  Several countries have incorporated the CSF into their own cybersecurity frameworks or expressed interest in doing so. It would be helpful if NIST and other U.S. agencies would encourage adoption of the CSF through the G-7 and with other foreign partners. Other

jurisdictions may benefit from greater engagement with NIST during development of CSF 2.0. Workshops aimed at sectoral regulatory agencies and industry may be useful in building capacity for cyber risk management, as well as enhancing NIST's understanding of how cyber risk management principles are translated into sectoral regulation. FSSCC members are happy to support such efforts through member company presence across different global regions.

When the CSF was first published in 2014, NIST stated that it was intended to be a living document that would be updated based on feedback from stakeholders. The CSF has helped create an effective common framework for cyber risk management and enabled cross-sector, public-private coordination on cyber risks. As those risks have continued to grow, they have underscored the importance of key elements such as governance and dependency management. An update to the CSF to better reflect these elements would be timely.

On behalf of the FSSCC, thank you for your consideration of these recommendations and for your leadership in developing and maintaining the CSF.

Sincerely,

Ron Green, Chair
Financial Services Sector Coordinating Council (FSSCC)
[redacted]