From: Andrea Flournoy
Sent: Thursday, January 18, 2018 11:14 AM
To: cyberframework <cyberframework@nist.gov>
Cc: Josh Magri
Subject: FSSCC Submission to NIST CSF Request for Comment

To Whom It May Concern:

The Financial Services Sector Coordinating Council appreciates the opportunity to respond to the National Institute of Standards and Technology's request for public comment on its second draft of version 1.1 ("Draft 2") of its *Framework for Improving Critical Infrastructure Cybersecurity.*

If you have any questions or concerns, please feel free to reach out. Thank you in advance for your time and attention.

Best Regards,
Andrea M. Flournoy
Deputy Director | FSSCC

[*Attachment copied below*]

January 19, 2018

Via Electronic Submission to cyberframework@nist.gov

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

RE: Request for Public Comment on NIST Cybersecurity Framework Version 1.1, Draft 2

To Whom It May Concern:

The Financial Services Sector Coordinating Council ("the FSSCC")[1] appreciates the opportunity to respond to the National Institute of Standards and Technology's (NIST's) request for public comment on its second draft of version 1.1 ("Draft 2") of its *Framework for Improving Critical Infrastructure Cybersecurity* ("NIST Cybersecurity Framework" or "Framework").

In Draft 2, NIST makes a number of enhancements, clarifications, and amendments to the previously issued NIST Cybersecurity Framework Version 1.1, Draft 1, a draft that the FSSCC largely supported.[2] More specifically, in Draft 2, NIST made the following substantive modifications –

[1] FSSCC members are listed in Appendix 1. Firm members of each financial trade association can be found by visiting their respective websites.

[2] To view the FSSCC's past letters of support for the NIST Cybersecurity Framework and the multi-stakeholder process that was so essential to its success and Framework effectiveness, please see the following –

FSSCC's submitted comments to the NIST Cybersecurity Framework Version 1.1, Draft 1 solicitation: https://www.fsscc.org/files/galleries/FSSCC_NIST_Response_04-07-2017_v3.pdf.

FSSCC February 9, 2016 response to NIST CSF RFI: https://www.nist.gov/sites/default/files/documents/2017/02/14/20160219_financial_services_sector_coordinating_council.pdf.

FSSCC October 10, 2014 response to NIST CSF RFI: https://www.nist.gov/sites/default/files/documents/2017/04/19/20141010_fsscc_garcia.pdf.

FSSCC April 8, 2013 response to NIST CSF RFI: https://www.nist.gov/sites/default/files/documents/2017/06/05/040813_fsscc.pdf.

See also –

FSSCC's submitted comments to the Federal Reserve Board, Office of the Comptroller of the Currency, and Federal Deposit Insurance Corporation advanced notice of proposed rulemaking on "Enhanced Cyber Risk Management Standards" solicitation: https://www.fsscc.org/files/galleries/FSSCC_Cyber_ANPR_Comment_Letter_2-17-17-0001.pdf.

- Additions of two subcategories to the NIST Cybersecurity Framework "Core": a subcategory under the "Protect" function, "Identity Management and Authentication and Access Control" category that recommends authentication at a level commensurate with a given transaction's [inherent] risk (PR.AC-7) and a subcategory under the "Respond" function, "Analysis" category that recommends the establishment of a process to receive, analyze, and respond to disclosed vulnerabilities (RS.AN-5).

- Clarification and enhancement of the subsection, entitled "Communicating Cybersecurity Requirements with Stakeholders" (Section 3.3), a subsection that now describes "cyber supply chain risk management" as identifying and managing "the cybersecurity effect an organization has on external parties and the cybersecurity effect external parties have on an organization," (i.e., what the financial services regulatory community has described as "dependency management") as well as its importance.

- Revision of a section (Section 4.0 and prior subsections) on the development and usage of NIST Cybersecurity Framework-based metrics for demonstrating desired business outcomes to a section that now describes how the NIST Cybersecurity Framework could be used for self-assessment.

FSSCC will focus its comments on these modifications, how the modifications might increase usage of the Framework, and how the financial services sector's request of NIST to hold a financial services sector-only workshop to further develop a risk tiering methodology and attendant criteria for the "Financial Services Sector Specific Cybersecurity Profile"[3] will increase usage of the Framework.

A. FSSCC Supports the Addition of the Two Subcategories to the NIST Cybersecurity Framework Core

As described above, in Draft 2, NIST added the following two subcategories to the NIST Cybersecurity Framework core:

FSSCC's submitted cybersecurity recommendations for the Trump Administration and 115th Congress: https://www.fsscc.org/files/galleries/FSSCC_Cybersecurity_Recommendations_for_Administration_and_Congress_2017.pdf.

FSSCC's submitted "Recommendations to the Commission on Enhancing National Cybersecurity": https://www.fsscc.org/files/galleries/FSSCC_Submission_to_the_Presidential_Commission_on_Enhancing_National_Cybersecurity_Letter_vF.pdf.

FSSCC's submissions to the FFIEC regarding its published Cybersecurity Assessment Tool: https://www.fsscc.org/files/galleries/FFIEC_Letter_1-15-16_FINAL.pdf; https://www.fsscc.org/files/galleries/FSSCC_FFIEC_Cybersecurity_Assessment_Comment_Letter_(FR_201 5-17907).pdf.

[3] The "Profile" significantly leverages the NIST Cybersecurity Framework with appropriate customizations for the financial services sector by blending the NIST Cybersecurity Framework architecture and categorization system with current regulatory expectations.

PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).

RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers).

These two new subcategories are a welcome evolution of the NIST Cybersecurity Framework core and correspond with the maturation of cybersecurity programs generally and the Framework, itself, to meet those advancements in thinking and practice.

With respect to PR.AC-7 - designing authentication practices to meet the risk of transaction, financial institutions have taken such a risk-based approach since the creation of financial institutions themselves, whenever transacting in financial instruments. With the advent of online and mobile banking to meet customer demand, financial institutions and those that oversee them have adapted by creating and adopting a series of authentication practices similar to the one expressed in PR.AC-7 (e.g., Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6809, the *Interagency Guidelines Establishing Information Security Standards* jointly issued by the Board, the FDIC, the OCC, and now subsumed OTS, 12 C.F.R. Part 208, app. D-2 and Part 225, app. F, PCI-DSS, and the Profile). As such, FSSCC endorses its addition and believes it an approach that should be followed across all sectors.

Regarding the addition of RS.AN-5, the FSSCC supports its addition to the NIST Cybersecurity Framework core. By adding this subcategory, NIST is acknowledging a process that enables institutions to make risk-informed decisions to mitigate, avoid, accept, or transfer the risks that flow from identified vulnerabilities. Such practices are incorporated within financial institution security programs and underlie the risk assessment process that these firms must implement pursuant to Gramm-Leach-Bliley and the implementing guidelines referenced above.

Lastly, FSSCC interprets the plain text of RS.AN-5 as suggesting that organizations develop processes to address inbound disclosures to the organization itself. To the extent that the FSSCC's interpretation of the language is correct, FSSCC supports its addition to the NIST Cybersecurity Framework core. If, however, RS.AN-5 is to be interpreted as directing an organization to participate in coordinated vulnerability disclosure (CVD) programs as some may suggest, FSSCC would not support RS.AN-5's addition in this update. Rather, FSSCC would suggest clarification and further study, analysis, and maturation of such programs before ensconcing them within the NIST Cybersecurity Framework core.

B. FSSCC Supports the Modifications Made to Section 3.3 "Communicating Cybersecurity Requirements with Stakeholders"

In its response to Draft 1, FSSCC described supply chain risk management as an "essential component to any thoughtful cyber risk management program" in reference to its support of NIST's addition of a "Supply Chain Risk Management" category to the NIST Cybersecurity Framework core. This Draft 1 addition remained in Draft 2 and continues to receive the FSSCC's support.

In Draft 2, however, NIST notably revised its description of the interplay between the NIST Cybersecurity Framework and cyber supply chain risk management in Section 3.3 "Communicating Cybersecurity Requirements with Stakeholders." More specifically, NIST expanded the subject of cyber supply chain risk management from third parties to more broadly defined "external parties." This broadening is consistent with the financial services sector's approach that financial institutions should not only consider those that they have contractual relationships with and how a cyber incident might impact them, but also consider those that they do not have a direct relationship with, but, nonetheless, may impact the institution in the event that those non-contractual fourth and fifth parties are impacted by a cyber incident. As NIST aptly described it in Draft 2, "cyber [supply chain risk management addresses both the cybersecurity effect an organization has on external parties and cybersecurity effect external parties have on an organization." This is an approach that the financial services regulatory community refers to as "dependency management." With this adjustment by NIST, both the NIST Cybersecurity Framework and the Financial Services Sector Specific Cybersecurity Profile with its addition of a dependency management function are now more conceptually aligned. As such, FSSCC supports NIST's modifications of this section: Section 3.3.

C. FSSCC Supports the Revision of Section 4.0 (and Prior Subsections) So That It Describes the Benefits of the NIST Cybersecurity Framework as a Self-Assessment Tool

In Draft 1, NIST's Section 4.0 and subsections described how the NIST Cybersecurity Framework could be used to develop a set of metrics that correlate the Framework tiers and security control usage with desired business outcomes. While the FSSCC applauded NIST's introduction of the concept, FSSCC noted that the Framework's four-tier methodology was not a methodology used by the financial services sector or the regulatory community that oversees it. Rather, the financial services sector had traditionally used a five-tier methodology and asked NIST and the regulatory community to assist the sector in the development of its Cybersecurity Profile.

The FSSCC also cautioned NIST to avoid selecting any one methodology in measuring cybersecurity risk and its potential reduction. The FSSCC noted that in the jointly issued advance notice of proposed rulemaking on "Enhanced Cyber Risk Management Standards," the Federal Reserve Board, the Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corporation similarly raised the topic of cybersecurity measurement, stating:

In the recent jointly issued FRB-OCC-FDIC proposal, the agencies inquired about quantitative cyber risk methodologies, such as the FAIR Institute's Factor Analysis of Information Risk standard. In its response, the FSSCC eschewed favoring any one methodology, but indicated the need to develop consensus based quantification metrics. FSSCC members still believe that it is premature to pick any one methodology; time and experience with various methodologies is still needed and should be explored in order to allow for evidence based calibrations to them. Respondents also cautioned that until the items to be measured are agreed upon and consistently described, measurement will not be reliable. However, by using the NIST Cybersecurity Framework's widely embraced descriptions and terminology, the possibility for such measurement and methodology development is greater. Additionally, FSSCC counsels that in considering metrics, NIST's intent is clear: metrics should be used to benchmark and drive improvements within a firm and not as a basis to suggest and enact prescriptive regulatory requirements. Lastly, until a methodology for calibrating risk metrics across firms is developed and validated, metrics should be used [to] measure improvement by comparing a single firm's current performance to its past performance, but should not be used to compare firms with one another.

With NIST's revision of Section 4.0 to focus on self-assessment, it is clear that NIST heeded this cautionary note. As such, the FSSCC is appreciative and supports the revisions.

D. NIST's Modifications and Updates to the NIST Cybersecurity Framework Coupled with NIST's Facilitation of a Financial Services Sector Only Workshop to Further Develop the Financial Services Sector Specific Cybersecurity Profile Will Only Serve to Increase Usage of the NIST Cybersecurity Framework.

As described in prior submissions, the FSSCC and the sector's financial institutions have been among the earliest proponents and users of the NIST Cybersecurity Framework. NIST's modifications to the Framework only enhance the sector's support. However, also as described in previous submissions, the financial services sector is among the most highly regulated sectors both in the quantity of oversight agencies at the federal, state, and self-regulatory organization level as well as the number of regulatory expectations issued therefrom. In an attempt to synthesize these expectations around a common cybersecurity risk management framework, the financial services sector chose the NIST Cybersecurity Framework as its base. Upon analysis, it became clear that some customizations to the Framework would have to be made to address certain regulatory areas of focus and to extend the Framework to be more of a firm diagnostic. These customizations as referenced above are known as the Financial Services Sector Specific Cybersecurity Profile.

At the May 2017 NIST Cybersecurity Framework workshop, the sector previewed the Cybersecurity Profile as a "proof of concept." Since that time, further refinements have been made to the Profile based on sector and regulatory community feedback. The Profile is now ready for its next phase: the development of a risk-tiering methodology specific to the financial services sector that

seamlessly overlays with the Profile, and which is accessible and implementable for financial institutions of all cyber complexity. The FSSCC requests that NIST or one of its components, such as the National Cybersecurity Center of Excellence (NCCoE), host a workshop of financial institutions, financial services related trade associations, and the financial services regulatory community to develop and refine such a risk-tiering methodology. With the development of such a methodology, FSSCC expects that the NIST Cybersecurity Framework via the Profile would be more widely adopted by financial sector institution and would be more widely accepted by government agencies. Additionally, by hosting such a workshop, NIST would be more able to fulfill its requirement under Cybersecurity Enhancement Act of 2014 to "prevent duplication of regulatory processes and prevent conflict with or superseding of regulatory requirements, mandatory standards, and related processes" (15 U.S.C. § 272[e][1][A][vii]).

Sincerely,

Rich Baich
Chair, Financial Services Sector Coordinating Council

Appendix 1. FSSCC Members

- Aetna
- AIG
- American Bankers Association (ABA)
- American Council of Life Insurers (ACLI)
- American Express
- American Insurance Association (AIA)
- American Society for Industrial Security International (ASIS)
- Bank Administration Institute (BAI)
- Bank of America
- BATS Exchange
- BB&T
- BCG Partners
- BITS/The Financial Services Roundtable
- BMO Financial Group
- BNY Mellon
- Capital One
- Charles Schwab
- ChicagoFIRST
- Citigroup
- The Clearing House
- CLS Bank International
- CME Group
- Comerica
- Consumer Bankers Associations (CBA)
- Credit Union National Association (CUNA)
- Credit Suisse
- Depository Trust & Clearing Corporation (DTCC)
- Discover Financial Services
- Equifax
- Fannie Mae
- Fidelity Investments
- Financial Information Forum (FIF)
- Financial Services Information Sharing and Analysis Center (FS-ISAC)
- First Data
- FIS
- Freddie Mac
- Futures Industry Association (FIA)
- Goldman Sachs
- Independent Community Bankers of America (ICBA)
- Institute of International Bankers (IIB)
- Intercontinental Exchange (ICE)/NYSE
- Investment Company Institute (ICI)
- John Hancock/Manulife Financial
- JPMorgan Chase
- LCH Clearnet
- Managed Funds Association (MFA)
- MasterCard
- Money Management Institute (MMI)
- Morgan Stanley
- NASDAQ
- National Armored Car Association
- National Association of Federal Credit Unions (NAFCU)
- National Automated Clearing House Association (NACHA)
- *National Futures Association
- Navient
- Navy Federal Credit Union
- Northern Trust
- The Options Clearing Corporation
- PNC
- Property Casualty Insurers Association of America (PCI)
- RBS
- Securities Industry and Financial Markets Association (SIFMA)
- State Farm
- State Street
- Sun Trust
- Synchrony Financial
- USAA
- U.S. Bank
- Visa
- Wells Fargo

*While the National Futures Association is a member of the FSSCC, it is a self-regulatory organization and did not participate in the drafting of this submission.