October 10, 2014

Via Electronic Submission to *cyberframework@nist.gov*

Ms. Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899.

RE: Experience With the Framework for Improving Critical Infrastructure Cybersecurity

Dear Ms. Honeycutt:

The Financial Services Sector Coordinating Council (FSSCC) appreciates the opportunity to provide comments in response to the request for information by the National Institute of Standards and Technology ("NIST") about the level of awareness throughout critical infrastructure organizations, and initial experiences with the Framework for Improving Critical Infrastructure Cybersecurity (the "Framework" or "Cybersecurity Framework").

Established in 2002, the FSSCC is the sector coordinator for financial services for the protection of critical infrastructure, focused on operational risks. Its membership is composed of 64 or the largest financial institutions and their industry associations. The FSSCC's mission is to strengthen the resiliency of the financial services sector against attacks and other threats to the nation's critical infrastructure by proactively identifying threats and promoting protection, driving preparedness, collaborating with the federal government, and coordinating crisis response for the benefit of the financial services sector, consumers and the nation.

FSSCC is submitting this response as a continuation of the financial sector's deep commitment to the public-private partnership process of the Cybersecurity Framework and its principle of voluntary, not mandatory, usage. We share the Administration's concerns regarding cyber threats and, since the FSSCC's establishment in 2002, we have engaged collectively in close partnerships within the sector, with government, and across other critical sectors to address this ongoing challenge. Accordingly, many members of the financial sector participated extensively in the development of the Framework since it was announced via Executive Order 13636 in February 2013, leading to "Version 1.0's" release in February of this year.[1] The end result is a set of consensus-based voluntary guidelines intended to align with existing regulatory authorities and regulations, enable technical innovation and, thus, avoid prescriptive technological solutions or specifications. We also agree with NIST that an important objective of its efforts should be to encourage widespread voluntary usage of the Cybersecurity

[1] **See FSSCC April 8, 2013 Submission to NIST RFI, February 26, 2013 – "Developing a Framework to Improve Infrastructure Cybersecurity"**

Framework across critical industries, as the financial industry's cybersecurity is contingent on the safety and security of other critical sectors, such as telecommunications and energy.

As we considered NIST's RFI questions related to "Awareness," "Experience" and "Roadmap for the Future of the Cybersecurity Framework," two observations guided our approach to providing NIST a useful snapshot of the degree to which the Framework, in these early stages of its circulation, is represented in the financial sector's enterprise risk management programs:

1) The FSSCC membership is composed of most of the largest critical financial infrastructure enterprises that by regulation and sound business practices – already employ cybersecurity controls that map closely to NIST and other standards included in the Cybersecurity Framework; and
2) Many small and mid-sized financial institutions as a category have far fewer resources than their larger counterparts, in addition to a lower risk profile by not being designated as a critical financial infrastructure firms, and thus may be at a more basic or early stage level when it comes to using the Framework.

To account for these differing subsectors, the FSSCC generated two separate surveys: The first, targeting the large, "critical infrastructure" FSSCC members which could provide a more detailed response based on their sophistication, involvement in the Framework's development and their position as critical infrastructure within the sector; and the second, focusing on the rest of the sector in order to gauge wide spread usage and feedback at a more basic level.

Survey questions directed to smaller institutions in the financial sector were posed in a questionnaire by the Financial Services Information Sharing and Analysis Center (FS-ISAC), a member association of the FSSCC and the primary operational collaboration center for the sector. Almost 75% of the FS-ISAC survey respondents, whose survey results are summarized after the FSSCC member results, are institutions of fewer than 500 employees.

FSSCC MEMBER SURVEY RESULTS FOR NIST CYBER FRAMEWORK

The following summary of FSSCC survey results are organized according to the structure of the NIST RFI, which evaluates in turn: "Awareness," "Experience," and "Roadmap for the Future."

AWARENESS

Many of NIST's questions focused on basic levels of awareness of the Framework. As has been heavily documented, FSSCC and its member organizations have moved beyond awareness to active engagement in the development of the Framework, and, in many cases, have begun the process of mapping the Framework to their existing practices. Within the FSSCC membership there is a high-level of awareness.

At a broader level, most FSSCC members operate globally or rely on the interconnectedness of the global digital infrastructure; hence, as with the NIST RFI, the FSSCC survey explored members' perception of the level of international awareness of the Framework.

Responding members' characterizations of awareness about the Cybersecurity Framework in Europe, Latin America and Asia ranged from "limited" to "general." Further, respondents noted that usage of the Cybersecurity Framework abroad could be complicated by differing cybersecurity standards and

regulations in other countries. One news report quoted international regulators as "looking at producing a global 'toolbox' next year…," and that "[t]he starting point is to look at what the Americans have done…and look at those risk-management principles and see how they could translate globally," an apparent reference to NIST's Cybersecurity Framework.

Similarly, appropriate and uniform application of the Framework's elements depends in part on the regulator community's awareness of the Framework and how each regulator maps it to their own control requirements for their regulated entities. FSSCC members were asked how they would characterize their regulator's awareness and use of the Framework in their assessments of cybersecurity risk management. Analysis of member responses indicates that financial regulators appear to be aware of the Framework and are still determining if, and how, to incorporate the Framework into their examinations. Some respondents reported that regulators have referenced the Framework in their communications with companies. Still, respondents have taken notice of some regulators' public statements about the Framework, and some have indicated that they are preparing their teams to appropriately respond to potential examination inquiries.

EXPERIENCE

FSSCC members' experience with cyber risk management is among the most advanced of any of the critical sectors. How that experience will integrate elements of the Framework, in whole or in part, will be determined over time. The first step is a mapping process, and FSSCC members indicated that they have mapped their internal information security practices to the NIST controls and generally found close alignment. Where there was not full alignment, the majority of respondents indicated that their enterprise policies and control standards are more comprehensive than what is outlined in the Framework.

Members are also mapping the Framework objectives to other control standards, such as ISO and SANS. One respondent indicated that the alignment with the NIST Framework can be reconciled using the "Alternative View" provided by NIST as a supplement to the Cybersecurity Framework. In addition, FSSCC members have been working on mapping the Framework to the AICPA SOC2 and Shared Assessments AUP in order to develop a method by which the outcomes can be linked to controls and test criteria in order to determine how firms are achieving the Framework's outcomes.

One sector innovation launched in September 2014 that leverages the financial sector's collaborative imperative and maps to the Cybersecurity Framework's "Detect (DE)" function is an automated threat intelligence capability called "Soltra Edge™." This capability employs software automation and services that detect, collect, distill and speed the transfer of threat intelligence from a myriad of sources to help safeguard against cyber attacks. It leverages the open-standard Structured Threat Information eXpression (STIX™) and Trusted Automated eXchange of Indicator Information (TAXII™). The solution will provide the platform, infrastructure and ecosystem to help individual organizations of all sizes, including Information Sharing and Analysis Centers (ISACs), Computer Emergency Response Teams (CERTs), industry bodies and private sector vendors, to come together to streamline threat information sharing using STIX and TAXII.

This capability will help companies achieve Framework Tier 4 Adaptive implementation aligned to:

- DE.AE-2: Detected events are analyzed to understand attack targets and methods
- DE.CM-1: The network is monitored to detect potential cybersecurity events
- DE.DP-4: Event detection information is communicated to appropriate parties.

An important part of generating awareness of the NIST Cyber Framework is the extent to which security and risk executives communicate to the company's key internal and external stakeholders (e.g., boards, investors, auditors, insurers, vendors, small and mid-sized financial institutions, and the general public) about the relationship between the company's cybersecurity risk management and the Framework.

FSSCC members indicated that they are using the Cybersecurity Framework as a reference for communications with key internal stakeholders at a level commensurate with their intentions to integrate it into their risk management programs. In practice, that means that some organizations are communicating about the Cyber Framework to their Boards and C-suites as part of their normal reporting process, while others continue to use reporting methods linked to others standards of practice they already have in place.

At a sector-wide level, many of our member associations have invested substantial human and financial resources not only to help develop the Cyber Framework in partnership with NIST and sector specific agencies, but also to educate member companies about the utility of the Framework as a viable reference for cyber risk management and how it maps to the existing cybersecurity and data breach regulations that firms currently adhere to.

Sector organizations have used member meetings and conferences to discuss the Cybersecurity Framework with members at all levels, from analysts to CEOs. Financial services sector organizations have also leveraged NIST's willingness to engage directly with Sector Coordinating Councils and other groups to raise awareness of the details and goals of the Framework.

Member companies have also reported that since the Framework's release, their Boards have increasingly requested presentations on cybersecurity risk management issues facing the organization, and have enrolled Board members in all-day seminars on cybersecurity risk for a particular institution.

Further, the FSSCC is partnering with its member associations, the Treasury Department and other agencies to raise awareness about the Framework to small and mid-sized community institutions across the country. FSSCC member associations continue to communicate about many cyber risk management activities to small and mid-sized institutions, with the Cybersecurity Framework as a prominent element in the messaging and resources offered. These activities include:

- Distributing information on cyber-attacks and threats, and mitigation strategies to small financial institutions, and encouraging them to join and actively participate in the FS-ISAC and regional information sharing organizations.

- Providing limited technical assistance to small financial institutions that FS-ISAC members detect are targets of cyber-attacks.

- Engaging smaller financial institutions in cyber exercises and simulations, and expanding participation by financial institutions of all sizes in the Cyber Attack against Payment Processes (CAPP) exercise.[2]

- Developing and disseminating industry best practices, such as security "toolkits" to assist small financial institutions with developing security strategies, risk management, intelligence

[2] https://www.fsisac.com/fs-isac-cyber-attack-against-payment-processes-capp-exercise

programs, and incident response and escalation programs. These toolkits also cover security, fraud reduction, vendor management, and emerging technologies available to financial institutions of all sizes by creating a mentoring program that will bring information security practitioners together, matching small financial institutions with larger financial institutions.[3]

- Developing a $4 million security automation project (see "Soltra Edge" above) that will enhance the sharing of threat information by making the process faster and more efficient across the sector (including with third party providers that service small financial institution).[4]

- Applying the structure of the Framework to similar and overlapping risk areas like insider threats, by mapping existing best practices within the private and public sector so the two areas can be more closely aligned.[5]

Members were also asked whether they are using the Framework to express cybersecurity requirements to their partners, suppliers, and other third parties. They uniformly indicated that it is too early in the Cyber Framework's arc for it to be applied to third party risk management requirements in place of existing assessments, but some have said that they are considering doing so. Many of the larger institutions already have sophisticated and mature vendor and third party requirements in place, and converting those systems would be time consuming and costly, absent a predictable and measurable improvement in security assurance outcomes.

While FSSCC members are still assessing how the rollout of the Framework will penetrate across the financial ecosystem and the broader economy, they were asked to discuss how expectations have or have not been met by the Framework.

This question elicited many thoughtful answers that are better compiled as individual responses rather than generalized into a consolidated FSSCC statement. The perspectives illustrate that the Cyber Framework has generated various expectations weighed against the anticipated costs, complexity and uniformity of adoption. As practitioners and executives of our critical financial infrastructure seek collectively to raise the bar toward a more resilient ecosystem, their views are paraphrased below as a cross-section of the hopes and apprehensions about the Framework's utilization.

Areas where the Framework is hitting the mark:

- In discussing the NIST Cybersecurity Framework, members have stated that the Framework is helpful in that it provides a common lexicon that is accessible not only to various functions within a given organization, but across sectors as well. It has also been helpful in that it has raised the profile and importance of cybersecurity risk management across sectors and many more C-suites.

- We believe no significant areas have been left out of the Framework, including the organization and hierarchy of categories and subcategories, along with the specific references.

[3] http://www.sifma.org/issues/operations-and-technology/cybersecurity/guidance-for-small-firms/
[4] http://avalanche.fsisac.com/soltra/about
[5] http://www.sifma.org/uploadedfiles/issues/technology_and_operations/cyber_security/insider-threat-best-practices-guide.pdf?n=92084

- The opportunity to have one standard for all sectors with minor modifications is a key selling point for further use in the third-party risk management space. It is our hope that NIST will continue to own the Framework and improve upon, and enhance, it. This leadership and participation has been critical to its success.

- Expectations were met; however, implementation or adoption of the Framework, and incorporating Framework parlance into our lexicon, does present potential challenges. These may include inconsistent application by regulators relative to preexisting frameworks. (This was noted in prior feedback to NIST specifically citing the existence of NIST SP 800-53 and the ISO/IEC 27000 series).

- The Framework is helpful by creating a common lexicon regarding cybersecurity risk management, particularly among those entities whose cybersecurity risk management practices are in the early phases of development and implementation. The Framework could be a useful tool among regulators, provided there is agreement among them to use the Framework within existing regulatory regimes. It could also be helpful to harmonize cybersecurity regulations among regulators, particularly for those firms who are regulated by more than one regulatory agency and/or type of regulator (i.e. sector specific or non-sector specific).

- We expected that the Framework addresses all industries equally. This expectation was met, and the Framework now helps us communicate the need for strong cybersecurity risk management requirements to our business partners, as well as the need for incident and vulnerability information sharing.

Areas where the Framework needs additional work:

- The integration of policies, and specifically control standards, with specific practices is labor intensive and might not be as valuable for mature programs.

- It is not clear why the framework doesn't include several of the NIST 800-53 Controls.

- The Framework and its components are not directly measurable. This should be a more measurable framework.

- The lack of metrics surrounding adherence or "compliance" to the Framework is a gap that should be addressed.

- There is no one-size-fits-all answer for cybersecurity, and we're skeptical that governments can provide comprehensive, prescriptive guidelines for all entities across industries.

- While the core structure of the Framework is solid, having been built using various existing standards and models, the "hype" associated with the Framework may have set expectations of something more groundbreaking than it may turn out to be. Furthermore, while the notion of implementation tiers provides for a more flexible approach in the application of the Framework, the lack of practical examples or reference models through sample profiles either at a broad or sector level make it difficult to understand the expectations of external entities such as regulators.

Future Roadmap

As with the above discussion of expectations about the Framework, members were asked to consider, even in these early stages of the Framework's process, what might be appropriate next steps. The recommendations, as with the answers above, are better compiled as expressed than generalized into a consolidated FSSCC statement.

- Build in implementation guidance, outcome metrics and measurements.
- Provide illustrative examples that aid in tiering self-assessment.
- Add risk and threat analysis and prioritization.
- Integrate with existing governance, risk and compliance (GRC) solutions.
- Target small institution education and adoption.
- Give it time to "steep" in enterprise systems before embarking on the next version.
- Provide guidance that takes into account organizations at various levels of maturity along the cybersecurity spectrum. NIST should continue to encourage consistency through ongoing awareness, practical examples and collaborative opportunities.
- Include cross-references to selected transnational frameworks – such as Information Security Forum – as a foundation for harmonization across global firms.
- To the extent it becomes used as regulatory guidance, the Framework should provide training and assessment standards for the regulator/auditor to recognize compliance with the Framework. The Framework provides an important opportunity to drive harmonization across the regulatory environment, particularly as regulatory agencies expand their examination programs to assist smaller financial institutions manage risk assurances from third party service providers on whom they depend.
- Although every institution has differing systems and threat profiles, NIST should provide examples of security controls that would provide the most benefit for the least cost. Doing so would serve the needs of smaller institutions who are challenged to allocate resources and elevate their security posture.
- NIST could help improve usage by developing a way for institutions to benchmark within and across sectors.

FS-ISAC BROAD SECTOR SURVEY

As discussed in the summary of this submission, many small and mid-sized financial institutions as a category have less awareness than their larger counterparts about available cybersecurity tools and procedures available to them – including the Framework – and thus might not be able to provide useful answers to many of the NIST RFI questions.

Thus, survey questions directed to smaller institutions in the financial sector were posed in a questionnaire by the Financial Services Information Sharing and Analysis Center (FS-ISAC), a member association of the FSSCC and the primary operational collaboration center for the sector. Almost 75% of the FS-ISAC respondents, whose survey results are summarized after the FSSCC member results, are institutions of fewer than 500 employees.

Below is a brief summary for the Cybersecurity Framework RFI survey that was distributed via the FS-ISAC.

- The survey primarily reflects the responses of small firms (<500 employees) in the sector.
- They are by and large aware of the NIST-CF and have been informed via the trade associations and other sector agencies like FS-ISAC and FSSCC.
- The Information Security teams of the responding firms are typically 1 FTE or less.
- For the most part they are currently using the FFIEC as their primary standard and guidance for security measures and controls which maps to the large number of community banks responding.
- 45% of the firms have evaluated the NIST-CF and within the next 6 months we expect approximately 78% of responding firms will evaluate it.
- As of today 55% have used it to drive an assessment, 54% to drive improvement and 36% to facilitate communication.
- Regulators by and large seem not to be contacting smaller firms regarding the NIST-CF.
- Firms are not using it externally to drive security requirements with third parties.

This concludes the FSSCC submission to this RFI. We will be happy to answer questions you may have.

Sincerely,

Russell Fitzgibbons
Chairman, Financial Services Sector Coordinating Council
Executive Vice President and Chief Risk Officer, The Clearing House