January 15, 2016

Via Electronic Submission to prainfo@occ.treas.gov and oira_submission@omb.eop.gov

Ms. Shaquita Merritt, OCC Clearance Officer
Legislative and Regulatory Activities Division
Office of the Comptroller of the Currency
Attention: 1557-0328
400 7th Street, NW, Suite 3E-218
Mail Stop 9W-11
Washington, D.C. 20219

RE: FFIEC Cybersecurity Assessment Tool

Dear Ms. Merritt:

The Financial Services Sector Coordinating Council ("FSSCC")[1] appreciates the opportunity to provide further comments in response to the Paperwork Reduction Act notice and request for comment, published in the *Federal Register*, Vol. 80, No. 241, on December 16, 2015, by the Office of the Comptroller of the Currency ("OCC"), the Board of Governors of the Federal Reserve ("Board"), the Federal Deposit Insurance Corporation ("FDIC"), and the National Credit Union Administration ("NCUA") (collectively, "the Agencies") with regard to the renewal of the information collection entitled "FFIEC Cybersecurity Assessment Tool" ("Assessment").

Together, the FSSCC and its members ("the sector") would like to thank the Federal Financial Institutions Examination Council ("FFIEC") and its member agencies for the time and effort that they have devoted to developing the *Assessment*. The sector would also like to thank the FFIEC and its member agencies for the opportunity to provide prior comment, for the in-person meeting the agencies granted upon the sector's request, and the response to the sector's and others' submissions embedded in this *Federal Register* request for further information.

[1] Established in 2002 by the financial sector, the FSSCC coordinates critical infrastructure and homeland security activities within the financial services industry. Its members consist of financial trade associations, financial utilities, and financial firms. FSSCC partners with the public sector on policy issues concerning the resilience of the sector.

FSSCC members are listed in an appendix, Appendix A. Firm members of each financial trade association can be found by visiting their respective websites.

To develop comments for this submission, the FSSCC used the same broad-based, cross-industry collaborative process that it used to develop its initial September 21, 2015 submission. Since the June 2015 release of the *Assessment*, the FSSCC member trade associations – which, together, represent the whole of the financial services sector – have held numerous teleconferences and meetings with their member institutions to discuss, evaluate, and synthesize the benefits and burdens of using the *Assessment*. This submission represents the input of the smallest financial institutions to the largest; from the front-line cybersecurity control implementers to the Chief Information Security Officers and the C-Suite (including Chief Executive Officers); and, from insurance companies to traditional depository institutions.

The sector incorporates its September 21, 2015 submission by this reference and additionally would like to highlight four key assertions and recommendations through this additional submission.

First, the sector requests that the FFIEC work in collaboration with the sector to develop an *Assessment* v2.0 that uses the NIST *Framework for Improving Critical Infrastructure Cybersecurity: Version 1.0* ("NIST Cybersecurity Framework")[2] as its visual base and foundation, but matures it to better incorporate the unique needs, threats, and products and services of the financial services industry. The current *Assessment*, while cross-referencing the requirements of the NIST *Cybersecurity Framework*, is not harmonized with the NIST *Cybersecurity Framework* such that a financial institution that completes the *Assessment* could understand its risk posture under the NIST *Cybersecurity Framework*. By using the NIST *Cybersecurity Framework* as the visual base and foundation for an *Assessment* v2.0, it would yield the following improvements:

- Use of a common and well-understood core framework would improve our industry's and regulators' collective understanding of the state of cybersecurity;
- Greater intra-business coordination and Boardroom engagement;
- More efficient resource allocation to address risks (including those that are inherent as well as residual);
- Enhanced oversight of a firm's cybersecurity, cybersecurity risk, and vendor management programs;
- Reduction in cybersecurity administrative burdens and regulatory compliance complexity; and
- Greater cross-sector and international cybersecurity understanding and collaboration.

Second, the sector again requests collaborating with the FFIEC and its member agencies to further develop the current *Assessment* into an *Assessment* v2.0 that can meet the jointly shared goals of increasing the cybersecurity posture of the financial services sector firms and the sector as a whole. In this regard, the sector proposes that the FFIEC develop a working group or other collaborative mechanism[3] for the purposes of enhancing the *Assessment's* overall effectiveness in

[2] National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity: Version 1.0.* 12 February 2014. <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>.
[3] The sector invites the FFIEC to a conversation about potential collaborative mechanisms.

evaluating a firm's cybersecurity program and providing a better roadmap to action in addressing its inherent and residual cybersecurity risk.

Third, the sector would like to thank the FFIEC for clarifying in its *Federal Register* renewal of information collection notice and request for comment that firm use of the *Assessment* is voluntary. However, the sector seeks further clarification from the Conference of State Bank Supervisors and its State members in light of recent State issued bulletins.

Fourth, the sector seeks to reaffirm the burden the financial sector will face to complete the current *Assessment*.

The sector appreciates your consideration of our recommendations.

I. The *Assessment* Would be Improved if it Used the NIST *Cybersecurity Framework* as its Visual Base and Foundation.

The sector would like to stress that it shares the FFIEC member agencies' goals of improving the cybersecurity posture of not only the financial sector as a whole, but at the individual firm level as well. As such, the sector requests that the FFIEC and its member agencies establish a working group or other collaborative mechanism in the near term to help improve the utility of the information collected by the *Assessment*. As examiners have begun to use the *Assessment* in examinations, the sector suggests a near-term (12 months) integration of an *Assessment* v2.0 into the NIST *Cybersecurity Framework* as the visual base and for foundational language. This can be accomplished in a working group comprised of the sector, the FFIEC, and its member agencies. Such an *Assessment* would yield numerous benefits to individual firms, the sector as a whole, agencies involved in regulatory oversight, the vendor community, and the other critical infrastructure sectors.

In using the NIST *Cybersecurity Framework* as the visual base and foundation for an *Assessment* v2.0, it would provide a uniform, extensible, and shared risk management vocabulary that is used and accessible across risk management disciplines, such as operations, audit, legal, new product development, etc. The NIST *Cybersecurity Framework* taxonomy and lexicon is language that is understood from the front-line cybersecurity control implementers up through the C-Suite to the Chief Executive Office and Boardroom. Usage of it in an *Assessment* v2.0 would enable greater intra-business coordination, more efficient resource allocation to address risks (including those that are inherent as well as residual), and enhanced oversight of a firm's cybersecurity, cybersecurity risk, and vendor management programs. It would also reduce cybersecurity administrative burdens and regulatory compliance complexity and foster greater cross-sector and international cybersecurity understanding and collaboration.

Indeed, in the approximately two years since the NIST *Cybersecurity Framework's* release, many Board Directors of financial services firms have embraced the NIST *Cybersecurity Framework,* its taxonomy and approach due to media coverage, endorsement by the National Association of Corporate Directors and the proliferation of outside materials and ongoing board educational sessions hosted by third-party audit firms. Moreover, as mentioned in our prior

submission, most of these Board Directors are native to other sectors wherein adoption of the NIST *Cybersecurity Framework* is widespread. As a result, firm management and many of these Directors are required to expend extensive time reconciling the current *Assessment* with the prior NIST *Cybersecurity Framework*, and it is impacting their ability to contextualize key issues and make appropriate decisions on the effectiveness of cybersecurity programs. Such an outcome is contrary to the FFIEC goal of enhanced board understanding and oversight, but is easily correctible if an *Assessment* v2.0 uses as a foundation the more universally adopted NIST *Cybersecurity Framework.*

Additionally, by using the NIST *Cybersecurity Framework* as the visual base and foundation for a collaboratively developed *Assessment* v2.0, it would substantially reduce the administrative burdens and cybersecurity regulatory, examination, and oversight complexity that is only growing. Indeed, Chief Information Security executives are reporting that this complex regulatory environment is distracting its top cybersecurity professionals from assessing the threat environment, designing cybersecurity strategies and leading teams in control implementation. Aside from the NIST *Cybersecurity Framework* and the *Assessment*, in the past two years alone, financial services regulatory and oversight organizations have announced the following regarding cybersecurity risk management and controls, testing and evaluation, business continuity planning and disaster recovery, and reporting and disclosure:

	Issuing Org	Date	Description
1	CFTC	12/23/2015	*Federal Register* notice of proposed rulemaking, "System Safeguards Testing Requirements for Derivatives Clearing Organizations"
2	OCC	12/17/2015	*Federal Register* notice of proposed enforceable guidelines, "Guidelines Establishing Standards for Recovery Planning by Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches," with reference to cyber stress testing
3	NAIC	12/17/2015	NAIC adoption of "Roadmap for Cybersecurity Consumer Protections," which include requirement that privacy policies include a statement on how consumer data is stored and protected and that insurance companies "take reasonable steps to keep unauthorized persons from seeing, stealing or using your personal information"
4	OFR	12/15/2015	OFR "2015 Financial Stability Report," which suggests that regulatory agencies consider further regulatory disclosure requirements regarding cyber incidents
5	NIST	12/1/2015	The NIST-led initiative to "pursue the development and use of international standards for cybersecurity," as detailed in the "Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity" and required by Cybersecurity Enhancement Act of 2014, Section 502
6	BIS CPMI-IOSCO	11/24/2015	Consultative white paper entitled, "Guidance on cyber resilience for financial market infrastructures," proposing principle-based cybersecurity requirements
7	FFIEC	11/10/2015	Revised "IT Examination Handbook: Management Booklet" issued
8	New York	11/9/2015	NYDFS' "Letter to Federal and State Financial Regulators on Potential New NYDFS Cyber Security Regulation Requirements for Financial Institutions"
9	NFA	10/23/2015	Adoption of interpretive notice, "9070 - NFA COMPLIANCE RULES 2-9, 2-36 AND 2-49: INFORMATION SYSTEMS SECURITY PROGRAMS," effective March 1, 2016 and requiring adoption and enforcement of a written information systems security program
10	Maine	10/16/2015	Bureau of Financial Institutions' Bulletin #80 regarding "Cybersecurity Assessments & the FFIEC Cybersecurity Assessment Tool," requesting completed FFIEC CAT Assessments starting 11/1/2015
11	Massachusetts	9/30/2015	Division of Banking's Bulletin regarding "Cybersecurity Assessments & the FFIEC Cybersecurity Assessment Tool," requiring measurement of "inherent cyber risks" and "cybersecurity maturity" using the FFIEC CAT by 3/31/2016 or to call Division staff to discuss whether use of an alternative framework would be acceptable
12	Texas	9/15/2015	Department of Banking's "Industry Notice 2015-8" requiring banks to measure "inherent cyber risks" and "cybersecurity maturity" using the FFIEC CAT by 12/31/2015 or to call Department of Banking staff to discuss whether use of an alternative framework would be acceptable
13	SEC	9/15/2015	Office of Compliance Inspections and Examinations' "Risk Alert" announcing further cyber exams of broker/dealers and investment advisors with new focus areas
14	NAIC	8/16/2015	Meeting minutes indicating NAIC Cybersecurity Task Force review and update of NAIC model laws

			and regulations to further advance cybersecurity, including potential updates to "NAIC Insurance Information and Privacy Protection Model Act (#670)"; "the Privacy of Consumer Financial and Health Information Regulation (#672)"; the "Standards for Safeguarding Consumer Information Model Regulation (#673)"; and the "Insurance Fraud Prevention Model Act (#680)"
15	SEC	7/8/2015	Request for comment on "Possible Revisions To Audit Committee Disclosures," including whether a publicly traded company's Audit Committee should oversee "treatment" of "cyber risks"
16	SEC	4/28/2015	Division of Investment Mgmt's "Guidance Update: Cybersecurity Guidance" for investment advisors
17	FFIEC	2/6/2015	Revised "Information Technology Examination Handbook: Business Continuity Planning Booklet" issued, which included the addition of a new appendix, "Appendix J: Strengthening the Resilience of Outsourced Technology Services"
18	FINRA	2/3/2015	Summary of cybersecurity principles and effective practices as reported in its February 3, 2015 Report on Cybersecurity Practice
19	FTC	8/24/2014	FTC's application of cybersecurity standards in UDAP enforcement actions post Federal Trade Commission v. Wyndham Worldwide Corporation, (3d Cir. 2015)
20	SEC	4/15/2014	Office of Compliance Inspections and Examinations' "Risk Alert" announcing cyber exams of broker/dealers and investment advisors

As mentioned in our prior submission, these separate regulatory initiatives and proposed requirements are having an effect on firm cybersecurity experts in that they are being increasingly asked to answer questionnaires and become involved in other compliance related work at the expense of engaging in protective cybersecurity activity. Firms cannot address this problem by simply hiring more cybersecurity personnel as they are becoming an increasingly scarce resource.[4] Thus, a reduction in redundant, multiplicative, and, at times, inconsistent approaches is essential. Using the NIST *Cybersecurity Framework* as the foundation for an *Assessment* v2.0 would greatly assist in reducing compliance complexity and enable cybersecurity professionals and their institutions to mature their cybersecurity programs.

Furthermore, by using the NIST *Cybersecurity Framework* as the foundation for an *Assessment* v2.0, it would allow sectors' institutions to continue using the NIST *Cybersecurity Framework* to communicate expectations and requirements to non-sector vendors and third parties, a stated area of focus for FFIEC member agencies.[5] Indeed, having an *Assessment* v2.0 that is more synchronous with the NIST *Cybersecurity Framework* can only assist in further cross-sector collaboration and understanding of key interdependencies as well as in the sector's collaboration with the government as a whole. According to PwC's recent "Global State of Information Security Survey for 2016," 91% of those surveyed either use this NIST *Cybersecurity Framework* or the ISO standards for cybersecurity risk management. In a similarly recent survey conducted by Dell Corp. of federal IT personnel, 82% of respondents reported that their agencies used the NIST *Cybersecurity Framework*, with 53% stating that it was "fully" used within their organization. The Office of Financial Research remarked in its 2015 Financial Stability Report that "the NIST *Cybersecurity Framework* is emerging as a de facto standard for firms seeking guidance in their

[4] According to the 2015 (ISC)2 "Global Information Security Workforce Study," the projected shortfall in cybersecurity professionals is expected to be 621,000 people worldwide in 2016 (271,000 people for the Americas); 901,000 people worldwide in 2017 (389,000 people for the Americas); 1,172,000 people worldwide in 2018 (516,000 people for the Americas); and 1,536,000 people worldwide in 2019 (649,000 people for the Americas).

[5] Please see: Office of the Comptroller of the Currency – OCC Bulletin 2013-29 "Third-Party Relationships"; FFIEC IT Examination Handbook InfoBase, Business Continuity Planning, Appendix J – "Strengthening the Resilience of Outsourced Technology Services"; Federal Deposit Insurance Corporation – Financial Institution Letter 44-2008, "Guidance for Managing Third Party Risk"; Federal Reserve, "Guidance on Managing Outsourcing Risk"; and National Credit Union Administration – Supervisory Letter 07-01, "Evaluating Third Party Relationships".

efforts to counter cyber threats." These findings echo the sector's experiences. As detailed in prior meetings with FFIEC member agencies, the sector has even developed a third-party, vendor management program to streamline the third-party assessment processes for financial services firms by "increasing the coverage of the AICPA [Service Organization Control Reports, version 2 (SOC 2)] to encompass the needs of the sector, incorporate the content of the NIST *Cybersecurity Framework* and align the risk that is evaluated to other assessment methods."

Because of the value and unprecedented adoption of the NIST *Cybersecurity Framework*, it is unlikely that such non-sector firms or third parties will grant financial institution requests, to report its cybersecurity risk management conformity to the *Assessment*. Accordingly, if the *Assessment* is not more fully aligned with the NIST *Cybersecurity Framework*, financial sector firms will find it increasingly difficult to evaluate third parties in the context of FFIEC *Assessment* expectations. As such, the sector requests the opportunity to collaborate with the FFIEC and its member agencies in a working group or other collaborative vehicle to develop an *Assessment* v2.0 that uses the NIST *Cybersecurity Framework* as its visual base and taxonomy foundation and incorporates key elements of the *Assessment* that are industry specific, complementary and additive, further advancing the financial industry's cybersecurity capabilities.

In the FFIEC's *Federal Register* notice and request for comment,[6] the FFIEC states that "[u]nlike other frameworks, the *Assessment* is specifically tailored to the products and services offered by financial institutions and the control and risk mitigation techniques used by the industry." The FFIEC further stated that its member agencies "also agree that the NIST *Framework* provides a mechanism for cross-sector coordination. However, because of the unique cyber risks facing the financial industry, the [FFIEC member agencies] identified a need to develop a more granular framework that is more specific to the financial services industry to assist financial institutions in evaluating themselves." While the sector agrees that its composition differs from other sectors (much as other sectors' compositions differ from each other), the *Assessment*, as currently constructed, consists of general cybersecurity controls that could be applied at any organization, in any sector. More specifically, in reviewing the declarative statements, none of the suggested controls are uniquely applicable to financial data and transactions, automated teller machines (ATMs), mobile banking, etc. Nor are the Maturity Level Domains unique. Indeed, Domain 1: Cyber Risk Management and Oversight, Domain 2: Threat Intelligence and Collaboration, Domain 3: Cybersecurity Controls, Domain 4: External Dependency Management, and Domain 5: Cyber Incident Management and Resilience are just as applicable and essential to other critical infrastructure sectors, sectors which are covered by the NIST *Cybersecurity Framework.*

In reviewing the Inherent Risk Profile Categories and their corresponding questions, it is much the same. Aside from the Online/Mobile Products and Technology Services Category and Automated Teller Machine service described in the Delivery Channel Category, the remainder of the Inherent Risk Profile Categories could be applied to non-financial sector firms. However, even though the above described category and service are unique to financial services, this particularization is lost at the control level because they are not considered or embedded within the cybersecurity Maturity Level Domains or Declarative Statements.

---

[6] *Federal Register*. Vol. 80, No. 241. 16 December 2015. 78287-8.

In designing the NIST *Cybersecurity Framework*, *Executive Order 13636*[7] directed the National Institute of Standards and Technology to "focus on identifying cross-sector standards and guidelines applicable to critical infrastructure."[8] The NIST *Cybersecurity Framework* has achieved that objective, and as described above, it is also applicable at the sector level for each critical infrastructure sector.

Recently, National Cybersecurity Coordinator Michael Daniel announced a NIST-led White House strategy for engaging the international community on cybersecurity standards standardization. In a blog describing the strategy, Mr. Daniel stated "[n]ot only do common standards make it easier for product development and sales, companies can more easily maintain and enhance network defense and resilience, which are vital in today's world of diverse cyber threats."[9] This rationale is equally applicable domestically, and, as such, greater synchronization domestically can only assist financial services firms in protecting themselves and the data that they are entrusted with.

II. A Collaborative Effort Will Improve the Effectiveness and Quality of the *Assessment*

Through a collaborative development of an *Assessment* v2.0 using the NIST *Cybersecurity Framework* as foundation and visual base, sector firms could more easily select their own risk tolerance based on their own business and security factors, such as the line of business that they are in, the business functions that they undertake, the information that they handle, and the cybersecurity program that they have in place. As mentioned in our prior submission, under the current *Assessment*, the focus is on "Inherent Risk" as determined by the FFIEC's *Assessment* categories and questions, but not on the residual risk following the selection and deployment of appropriate compensating controls. Because firms cannot answer "Yes, No, Partial, Compensating Controls Used, or Not Applicable," but rather, "Yes, No," it effectively chooses risk tolerance for that firm for that particular control. Either it is 100 percent or zero percent. For example, a certain product or service offering may have a certain risk profile of and by itself. However, in order to account for that risk, institutions will put into place certain mitigating controls by which the inherent risk is controlled. As such, the binary responses for the various maturity levels, either at 100 percent or zero percent, do not accurately reflect the steps an institution has already taken to control the risk for which the institution has specifically selected for their own business model.[10]

---

[7] Obama, Barack. *Executive Order 13636, Improving Critical Infrastructure Cybersecurity*. The White House, 12 Feb. 2013. <https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-criticalinfrastructure-cybersecurity>.

[8] Ibid.

[9] Daniel, J. Michael. The White House. "Engaging the International Community on Cybersecurity Standards." <https://www.whitehouse.gov/blog/2015/12/23/engaging-international-community-cybersecurity-standards>. Published 23 December 2015.

[10] For a more detailed discussion of the concept of residual risk and the sector's concerns, which are reaffirmed here, please refer to the sector's initial September 21, 2015 submission.

Collaborative models have been used to much effect in other sectors, generating faster adoption rates and calls to action. Since the NIST *Cybersecurity Framework's* release, the Federal Communications Commission, the Department of Energy, and the Department of Health and Human Services, as directed by Section 405 of the Cybersecurity Act of 2015, have been or are currently working with their private sector counterparts to customize the NIST *Cybersecurity Framework* for sector specific needs. The sector requests that the FFIEC collaboratively work with the sector to do the same for an *Assessment* v2.0.

III. Clarifying Statements of the Voluntary Nature of the *Assessment* by the Conference of State Bank Supervisors and Its Member States Will Ease Confusion Concerning Use

As an initial matter, the sector would like to thank the FFIEC for clarifying in its *Federal Register* renewal of information collection notice and request for comment that the member agencies' examiner's "will not require a financial institution to complete the *Assessment*," and that the member agencies "are educating examiners on the voluntary nature of the *Assessment* and including statements about its voluntary nature....".[11]

Since the FFIEC clarification, the states of Texas, Massachusetts, and Maine have all issued notifications to state-chartered banks that it is either the implicit or explicit expectation that state-chartered banks will utilize the *Assessment*. All three agencies are members of the FFIEC through their membership in the Conference of State Bank Supervisors. The sector requests clarifying statements from the Conference of State Bank Supervisors and its member States that usage of the *Assessment* will remain voluntary.[12]

IV. The FFIEC's Burden Estimates Remain Significantly Understated for Firms That Intend to Perform More Than a Perfunctory *Assessment*

Lastly, regarding the FFIEC's solicitation regarding the accuracy of the burden, we note that the notice and request for comment states that "[t]he Agencies' revised burden estimates do not include the amount of time associated with reporting to management and internal committees, developing and implementing action plans, and preparing for examination as such time and resources are outside the scope of the PRA."[13]

However, as institutions reported at the in-person meeting, an essential component of preparing for an examination is to provide auditable and defensible information for examiners. Bankers view preparation of the *Assessment* in the same manner and therefore suggest that the document preparation and completion of the *Assessment* cannot be separated.

---

[11] *Federal Register*. Vol. 80, No. 241. 16 December 2015. 78288.

[12] See Texas Department of Banking, "Industry Notice 2015-8." 15 September 2015; the Commonwealth of Massachusetts Division of Banks, "Industry Letter on FFIEC Cyber Security Tool, 30 September 2015"; State of Maine Bureau of Financial Institutions, "Bulletin #80" 16 October 2015.

[13] *Federal Register*. Vol. 80, No. 241. 16 December 2015. 78288.

Based on the sampling mentioned in the prior submission and follow-up inquiries of sector firms, the revised burden estimates remain significantly understated. As such, the sector refers the FFIEC to its original submission with regard to its burden estimates. Accordingly, the sector requests that the FFIEC revisit the criteria by which it determined the revised estimates as well as the estimates themselves.[14]

Finally, as mentioned above, several states have mandated the use of the *Assessment* despite the FFIEC's insistence on the voluntary nature of the *Assessment*. The sector contends that this echo affect will ultimately affect the burden estimates by the FFIEC member agencies' not only today but into the future. Certainly, a harmonization between the states and Federal regulators on the intent of the *Assessment*, whether it is voluntary or otherwise should be clarified. As the burden may differ for state chartered banks versus those with federal charters and this, too, could affect the final burden estimates.

V. Conclusion

In conclusion, the sector commends the FFIEC and its member agencies for their focus on cybersecurity and cybersecurity risk management and the effects on financial services at both the sector and institutional level, and we share a common goal to improve our collective capabilities. In addition, the sector asks that the FFIEC and its member agencies grant the sector's request to engage in a collaborative process to develop a refined *Assessment* v2.0, such as through a working group or other coordinative mechanism, that addresses the above suggested improvements and further aligns the *Assessment*, the NIST *Cybersecurity Framework* and our industry's capabilities in protecting the nation's consumers and economic platforms and critical infrastructure.

Sincerely,

Russell Fitzgibbons
Chairman

Attachment

[14] The sector contends that its estimates are in accord with the strictures set forth in 44 U.S.C. §§ 3501(4), 3502(2).

Appendix A

Financial Services Sector Coordinating Council Membership

The Financial Services Sector Coordinating Council (FSSCC) fosters and facilitates financial services sector-wide activities and initiatives designed to improve Critical Infrastructure Protection and Homeland Security. The Council was created in June 2002 by the private sector to coordinate critical infrastructure and homeland security activities in the financial services industry.

Associations (24)	Operators (32)	Utilities and Exchanges (14)
American Bankers Association (ABA)	AIG	BATS Exchange
American Council of Life Insurers (ACLI)	American Express	CLS Services
American Insurance Association (AIA)	Aetna	The Clearing House
American Society for Industrial Security International (ASIS)	Bank of America	CME Group
Bank Administration Institute (BAI)	BB&T	Direct Edge
BITS/The Financial Services Roundtable	BNY Mellon	Depository Trust & Clearing Corporation (DTCC)
ChicagoFIRST	Charles Schwab	First Data
Consumer Bankers Associations (CBA)	Citi	Intercontinental Exchange (ICE) / NYSE
Credit Union National Association (CUNA)	Comerica	International Securities Exchange (ISE)
Financial Information Forum (FIF)	Convergex	LCH Clearnet
Financial Services Information Sharing and Analysis Center (FS-ISAC)	Equifax	NASDAQ
Futures Industry Association (FIA)	Fannie Mae	National Stock Exchange
Independent Community Bankers of America (ICBA)	Fidelity Investments	Omgeo
Institute of International Bankers (IIB)	FIS	Options Clearing Corporation
Investment Company Institute (ICI)	Freddie Mac	
Managed Funds Association (MFA)	Goldman Sachs	
National Automated Clearing House Association (NACHA)	JPMorgan Chase	
National Association of Federal Credit Unions (NAFCU)	Manulife Financial	
National Armored Car Association	MasterCard	
National Futures Association	Morgan Stanley	
Property Casualty Insurers Association of America (PCI)	Navy Federal	
Securities Industry and Financial Markets Association (SIFMA)	Northern Trust	
	PNC	
	RBS	
	Sallie Mae	
	State Farm	
	State Street	
	Sun Trust	
	Synchrony Financial	
	US Bank	
	Visa	
	Wells Fargo	