April 10, 2017

Via Electronic Submission to cyberframework@nist.gov

Mr. Edwin Games
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

RE: *Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity*

Dear Mr. Games:

The Financial Services Sector Coordinating Council ("the FSSCC")[1] appreciates the opportunity to provide comments in response to the notice and request for comment published in the *Federal Register*, Vol. 82, No. 15, on January 25, 2017, by the National Institute of Standards and Technology ("NIST") regarding views on the *Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity* (the "*Cybersecurity Framework*" or the "*Framework*").

As previously described in past comment letters[2], the FSSCC is supportive of the Congressionally approved[3] and multi-stakeholder developed *Cybersecurity Framework*. Both the process utilized and the resulting *Framework* should be lauded and used as an example to follow.

FSSCC is also largely supportive of the proposed *Framework* updates as described in the *Framework's Update*, *Version 1.1*. The added supply chain risk management and metrics concepts are welcome and needed evolutions. In this response, FSSCC will focus its comments on those added concepts.

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

[2] See: http://fsscc.morwebcms.com/files/galleries/NISTcommentletterSigned-0001.pdf; https://www.fsscc.org/fsscc/news/2014/FSSCC-PressRelease-NIST_CSF.pdf.

See also: https://www.fsscc.org/files/galleries/FSSCC_Cyber_ANPR_Comment_Letter_2-17-17-0001.pdf; https://www.fsscc.org/files/galleries/FSSCC_Cybersecurity_Recommendations_for_Administration_and_Congress_2017.pdf; https://www.fsscc.org/files/galleries/FSSCC_Submission_to_the_Presidential_Commission_on_Enhancing_National_Cybersecurity_Letter_vF.pdf; 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_2015-17907).pdf.

[3] See the Cybersecurity Enhancement Act of 2014: https://www.congress.gov/113/plaws/publ274/PLAW-113publ274.pdf.

The financial services sector exists in a complex web of regulatory entities, each with their own important role and mandate (please see Appendix 2). We believe that the NIST Cybersecurity *Framework* provides a critical opportunity for these disparate entities to leverage this industry-driven, consensus based approach as the foundation of cybersecurity regulation rather than continuing the current trend (please see Appendices 3 and 4). For this reason, FSSCC notes that the sector is currently developing a sector-specific profile ("Profile") that could serve as a template toward a more harmonized[4] regulatory approach, in contrast with the continuing proliferation of cybersecurity regulatory proposals and activities at both the federal and state level impacting the financial services industry (please see Appendix 4). In developing this Profile, the sector will be using the NIST *Cybersecurity Framework* organizational structure and incorporating key regulatory requirements and areas of oversight focus from across the various sub-sectors (e.g., banking, insurance, financial market utilities, finance, etc.), namely the more prominent placement of "Governance" and the newly added "Supply Chain Risk Management," which is often referred to as "Dependency Management" within the financial services sector. This Profile is also intended to be scalable and potentially usable as a diagnostic, taking into account the inherent risk and complexity of institutions. A preview of the Profile might be possible by the time of the NIST *Cybersecurity Framework* Workshop in May.

There is precedent for such a sector-specific profile approach. For example, late last year, the "Maritime Bulk Liquids Transfer Cybersecurity Framework Profile" was released.[5] The purpose of that profile was to "assist in cybersecurity risk assessments for those entities involved in [maritime bulk liquids transfer] operations as overseen by the [U.S. Coast Guard]." The telecommunications sector and electricity sub-sector each worked with their regulatory and sector specific agencies, respectively, to develop similarly tailored NIST Cybersecurity profiles as well.[6],[7] Most recently, NIST worked with industry stakeholders within the manufacturing sector to develop a "Cybersecurity Framework

---

[4] With the term "cybersecurity regulatory harmonization," FSSCC means the following:

1) An Unified Organizational Structure for Cyber Risk Management (i.e., a Dewey Decimal System or GAAP for cyber based on the *NIST Cybersecurity Framework*);
2) A common language and common taxonomy throughout the agencies and in their collateral documents, throughout industry, etc.;
3) A "common college application" approach to examination questionnaires with flexibility for each agency's unique statutory authorities and areas of focus;
4) If there is to be some type of compliance certification, it should be a more uniform "form" for certification so that a given firm does not have to reconcile differences between such forms.

[5] See: http://mariners.coastguard.dodlive.mil/2016/11/10/release-maritime-bulk-liquids-transfer-cybersecurity-framework-profile/.

[6] See: https://energy.gov/sites/prod/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdf.

[7] See: https://energy.gov/sites/prod/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdf.

Manufacturing Profile." That particular profile was released on March 20, 2017, and is currently open for comment.[8]

I. Comments Regarding Update 1.1: Supply Chain Risk Management and Metrics

In the proposed Update, Version 1.1, NIST added a new Category of "Supply Chain Risk Management" under the "Identify" Function and a section of text on "Measuring and Demonstrating Cybersecurity." Regarding the addition of the "Supply Chain Risk Management" Category, FSSCC welcomes this addition. It is an appropriate progression of the *Framework* and it integrates an essential component to any thoughtful cyber risk management program. Supply chain risk management, often referred to as "Dependency Management" within the sector, is a programmatic focus for financial institutions, which will only increase in importance and attention with increased connectivity, specialization, and interdependencies. In fact, as mentioned, supply chain risk management/dependency management will be a key component of the financial services sector-specific profile, which is currently under development.

The added "Measuring and Demonstrating Cybersecurity" section is also is a much needed evolution, and NIST should be applauded. Nonetheless, NIST's description of its four-tier methodology as a metric, while accurate, the four-tier methodology, itself, has not been widely adopted by the financial services sector or its regulators. Rather, the financial services regulatory agencies have tended to utilize five-tier methodologies and sets of repeatable diagnostic questions answerable with a set of straightforward responses.[9] Accordingly, the FSSCC would like to work with NIST and the regulatory community to create a diagnostic embedded within a sector-specific cybersecurity profile that is risk-based and similar in format to past financial services diagnostics. Such a diagnostic should be scalable across sub-sectors and across firms of varying risk, allowing responses of "Not Applicable, Yes, No, Partial and Compensating" across various categories, subcategories, and control sets or requirements.

In terms of the quantification of cybersecurity risk and measuring its possible reduction, the FSSCC would be interested in engaging with NIST and the financial services regulatory community in developing methodologies and metrics to do so. 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.[10] 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*

[8] See: http://csrc.nist.gov/cyberframework/documents/csf-manufacturing-profile-draft2.pdf.

[9] For example, the FFIEC's "Cybersecurity Assessment Tool" uses a five-tier maturity model with levels of Baseline, Evolving, Intermediate, Advanced, and Innovative. See: https://www.ffiec.gov/cyberassessmenttool.htm.

[10] See: https://www.federalregister.gov/documents/2016/10/26/2016-25871/enhanced-cyber-risk-management-standards.

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 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.

II. The Financial Services Sector Reiterates Its Commitment to the Multi-Stakeholder NIST Process and Cybersecurity Advancement

The FSSCC would also like to again applaud NIST for the open and transparent process that it has used in creating and seeking to update the *Cybersecurity Framework*. The financial services sector has found value in this ongoing, multi-stakeholder collaborative process and has been one of its most ardent proponents. For the financial services sector, cybersecurity, collaboration, and cybersecurity maturation are an imperative.

Indeed, the financial services sector is investing time, talent, and resources into cybersecurity. Many of the world's largest financial institutions have made substantial investments in cybersecurity and are continuing unprecedented levels of spending. According to the report published by Homeland Security Research Corp., the financial services cybersecurity market in United States reached an estimated $9.5 billion in 2016, making it the largest non-government cybersecurity market.[11] Of that number, the top four U.S. banks have collectively spent nearly $1.5 billion.[12] In fact, according to a recent Kaspersky Lab Report, firms within the financial sector "spend more on IT security than any other sector, spending three times as much as comparably sized non-financial institutions."[13]

In fact, over the past two decades, the financial services sector has been at the forefront of cybersecurity innovation and collaboration. Together, the sector has:

- Established the ***Financial Services Information Sharing and Analysis Center (FS-ISAC)*** in 1999 to facilitate information sharing and analysis of cyber and physical threats facing the financial services sector. Today, the FS-ISAC has about 7,000 member financial institutions and trade associations in 38 countries.
- Established the ***Financial Services Sector Coordinating Council (FSSCC)*** in 2002; the FSSCC consists of private sector owners, operators, utilities and trade associations, representing a cross-section of the financial services industry. It partners with the financial services government coordinating council – the Financial and Banking Information Infrastructure

[11] See: http://homelandsecurityresearch.com/2014/10/u-s-banking-financial-services-retail-payment-cybersecurity-market-2015-2020/.
[12] See: https://www.forbes.com/sites/stevemorgan/2015/12/13/j-p-morgan-boa-citi-and-wells-spending-1-5-billion-to-battle-cyber-crime/#7204cf13116d.
[13] See: https://go.kaspersky.com/rs/802-IJN-240/images/Financial_Survey_Report_eng_final.pdf.

Committee (FBIIC) – to address critical infrastructure policy issues and strengthen industry resiliency and preparedness.

- Developed and convened 13 ***"Hamilton Series"*** cyber exercises in 2014-16 in collaboration with the various U.S. Government agencies to better prepare the financial sector in addressing the risks and challenges presented by significant cybersecurity incidents. The exercises ranged from regionally-focused events among small and medium sized companies to exercises hosted by the U.S. Treasury Department and Federal Reserve Bank of New York involving large, systemically important financial sector companies. Additionally, these scenarios examined impacts to different segments of the financial sector, including impacts to equities markets, large, regional, and medium-sized depository institutions, payments systems and liquidity, and futures exchanges.
- Coordinated extensively with Treasury, DHS, and the White House on the development of ***Presidential Policy Directive (PPD) 41***, July 2016, which outlines the U.S. Government's response protocols for a cyber security incident.
- Improved and expanded ***cross-sector and public-private information sharing and collaboration***, including providing subject matter expertise and advocacy to support the ***Cybersecurity Act of 2015***; investing in technologies and standards to automate cyber threat/attack information sharing; embedding a financial sector expert in DHS's National Cybersecurity and Communications Integration Center; expanding membership in the FS-ISAC and working with the Electricity Subsector and Communications Sector to foster integrated responses to cybersecurity.
- ***Fostered sector-wide cybersecurity collaboration*** through nine ***Joint Financial Associations Cybersecurity Summits***. Since 2013, the Summits have brought together key financial sector and government executives to discuss Sector resiliency, address cyber threats and capability gaps, and enhance coordination and collaboration.
- Created ***Sheltered Harbor*** to help firms further protect consumer's and their accounts, balances and assets. Firms can use Sheltered Harbor developed architecture standards and assurance model to create their own distributed data vault, adding an extra layer of protection against a potential significant cyber risk and loss of critical processing capability.
- Created the ***Financial Systemic Resilience and Analysis Center (FSARC)***, a subsidiary of the FS-ISAC. The mission of the FSARC is to proactively identify, assess, and coordinate efforts to mitigate systemic risk from cyber security threats. FSARC membership is limited to those entities within the financial sector designated as "critical infrastructure" under Executive Order 13636.
- Updated and tested ***cyber response plans***, including the ***All-Hazards Crisis Response Playbook***, to assign responsibilities for collaboration, communication, and decision-making within the financial sector and key partners in other sectors and the Federal Government.

Because the overwhelming majority of financial services and critical infrastructure information systems are owned or operated by the private sector, in order to advance cybersecurity, collaboration between the private sector and the government is essential. NIST's open and transparent process, with multiple engagements with the variety of interested stakeholders is a model that should be continued. Further, it is one that should be adopted by those agencies with oversight authority over cybersecurity related risk and matters.

III. Conclusion

In conclusion, the FSSCC commends NIST for its update. As it has been throughout the Framework's development, the FSSCC will continue its collaboration with NIST and other stakeholders in the Framework's evolution. FSSCC expects that the Profile it is currently developing will be a critical resource to drive regulatory harmonization. We look forward to engaging NIST, and the financial services regulatory community, as this Profile work continues, which the FSSCC expects to complete just prior to the May workshop.

Please contact me, or FSSCC's Executive Director Brian Tishuk at (312) 342-1308 or brian.tishuk@fsscc.org, with questions or comments.

Sincerely,

Rich Baich
Chair, Financial Services Sector Coordinating Council
Tel: (704) 715-8018
Fax: (704) 383-8129
rich.baich@wellsfargo.com

APPENDIX 1. FSSCC Members

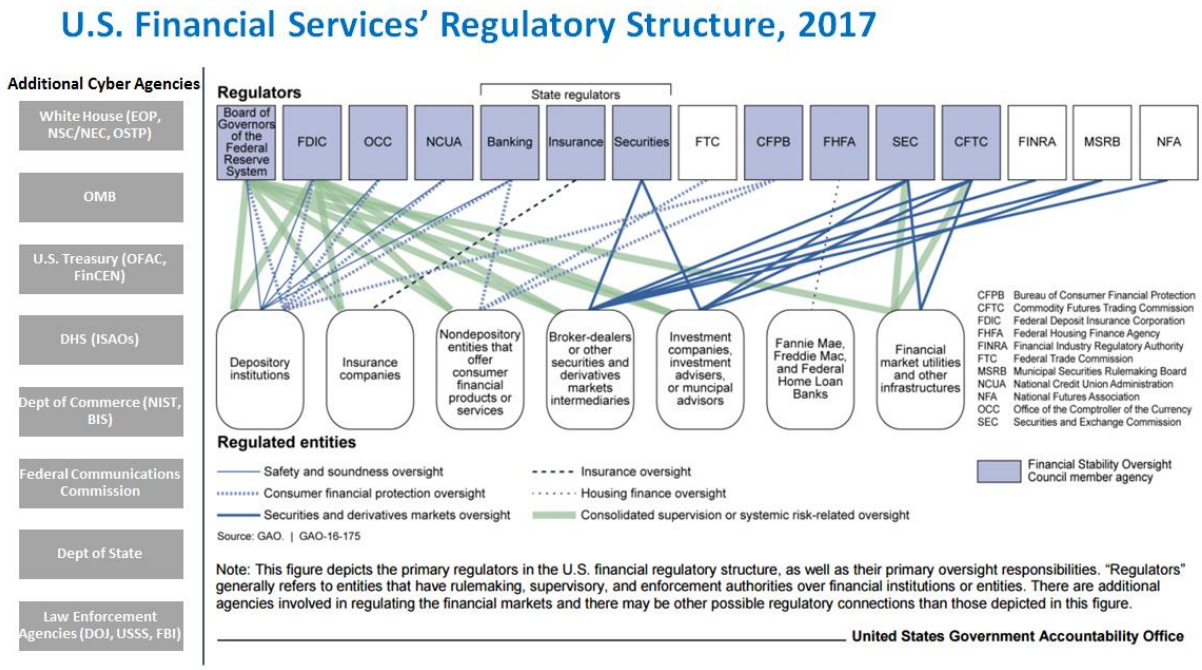
Associations	Operators	Utilities and Exchanges
American Bankers Association (ABA) American Council of Life Insurers (ACLI) American Insurance Association (AIA) American Society for Industrial Security International (ASIS) Bank Administration Institute (BAI) BITS/The Financial Services Roundtable ChicagoFIRST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

*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.

* * * * *

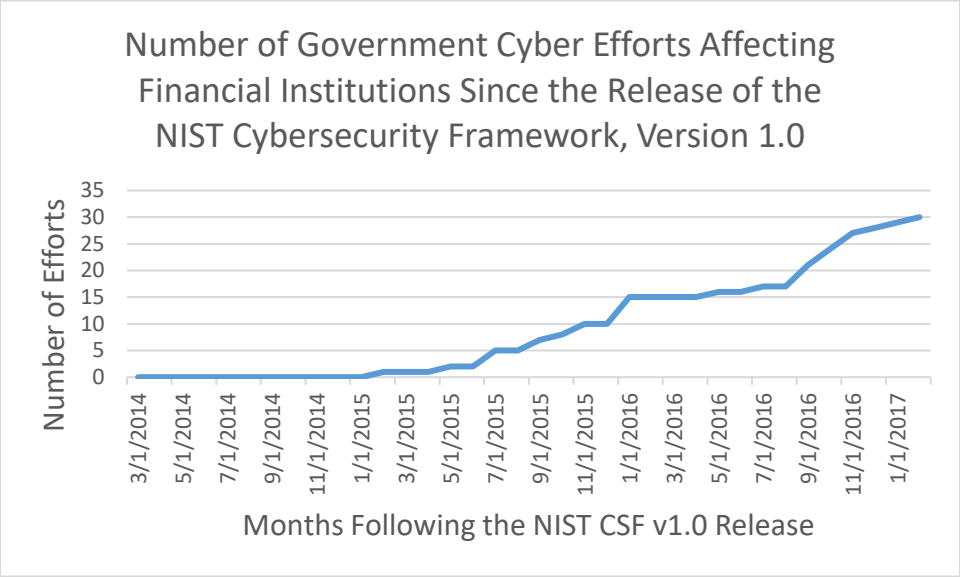
The following Appendices, Appendices 2-5, identify the current state of cyber frameworks, tools and regulatory guidance and requirements. The use of the NIST *Cybersecurity Framework* plus the Financial Services Sector Cybersecurity Profile is intended to simplify terminology, minimize duplication, provide consistent descriptions and terminology and improve industries ability to enhance Cybersecurity capabilities

APPENDIX 2. Regulatory Chart



APPENDIX 3. Regulatory Trend

In the past three years, we tracked nearly 30 different cybersecurity proposals/compliance regimes from more than a dozen regulatory agencies.



APPENDIX 4. Catalogue

Excerpted from the Financial Services Sector Coordinating Council's February 17, 2017, response to the solicitation on the jointly issued "Enhanced Cyber Risk Management Standards": https://www.fsscc.org/files/galleries/FSSCC_Cyber_ANPR_Comment_Letter_2-17-17-0001.pdf -

> **Cybersecurity-related Regulations, Requirements, Examination Expectations, and Other Government Cyber Efforts Affecting financial institutions since the release of the NIST Cybersecurity Framework, Version 1.0 in February 2014.**
>
> These lists may not be exhaustive, and inclusion does not represent a judgment of the relative benefits or burdens of each singular issuance. Rather, this catalogue is meant to illustrate the complexity of the cyber landscape for financial institutions.
>
> For a list of statutory and regulatory requirements that predate the NIST Cybersecurity Framework and which apply solely to banking firms, please refer to the FSSCC's September 21, 2015, submission on the "FFIEC Cybersecurity Assessment Tool,"[14] as well as the Center for

[14] See FSSCC's September 21, 2015, submission on the "FFIEC Cybersecurity Assessment Tool," p.4, found here: https://www.fsscc.org/files/galleries/FSSCC_FFIEC_Cybersecurity_Assessment_Comment_Letter_(FR_2015-17907).pdf

Strategic and International Studies' (CSIS) July 2015 report, entitled, "The Evolution of Cybersecurity Requirements for the U.S. Financial Industry"[15].

Table A. Regulatory Requirements, Issuances, and Proposals affecting financial institutions' cybersecurity programs directly.[16]

	Issuing Org	Date	Description
1	NAIC	2/27/2017	Issuance of proposed "Insurance Data Security Model Law," Version 3. Once finalized, NAIC will move for the model law to be passed by its state constituents via the accreditation process. http://www.naic.org/documents/cmte_ex_cybersecurity_tf_170307_data_security_model_law_clean.pdf
2	NYDFS	2/16/2017	NYDFS issues financial services specific cybersecurity regulations, entitled, "Cybersecurity Requirements for Financial Services Companies," 23 NYCRR 500 http://www.dfs.ny.gov/legal/regulations/adoptions/rf23-nycrr-500_cybersecurity.pdf, which takes effect on 3/1/2017.
3	OCC	1/24/2017	OCC Bulletin 2017-7 "Supplemental Examination Procedures for Risk Management of Third-Party Relationships," which "expand on the cores assessment contained in the 'Community Bank Supervision,' 'Large Bank Supervision,' and 'Federal Branches and Agencies Supervision' booklets of the *Comptroller's Handbook*," by providing "additional guidance" on, among other things, examination of third party selection and due diligence vis a vis cyber resiliency and contractual clause adequacy in addressing cyber incident notification. https://www.occ.gov/publications/publications-by-type/comptrollers-handbook/pub-third-party-exam-supplemental-procedures.pdf
4	SEC	11/15/2016	Order approving the "National Market System Plan Governing the Consolidated Audit Trail," which codifies certain cybersecurity requirements for "Plan Processors." https://www.sec.gov/rules/sro/nms/2016/34-79318.pdf
5	FRB, OCC, FDIC	10/26/2016	*Federal Register* notice of advanced notice of proposed rulemaking (ANPRM), entitled, "Enhanced Cyber Risk Management Standards," which imposes new cybersecurity regulatory requirements on financial institutions with asset sizes of $50B+ and which is not directly aligned with past regulatory regimes. https://www.federalregister.gov/documents/2016/10/26/2016-25871/enhanced-cyber-risk-management-standards
6	OCC	9/29/2016	*Federal Register* notice of finalized 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. https://www.gpo.gov/fdsys/pkg/FR-2016-09-29/pdf/2016-23366.pdf
7	SEC	9/28/2016	*Federal Register* notice of adoption of a final rule of the "Enhanced Regulatory Framework for Covered Clearing Agencies"; the rule includes cybersecurity related requirements. https://www.federalregister.gov/documents/2016/10/13/2016-23891/standards-for-covered-clearing-agencies
8	CFTC	9/19/2016	Federal Register notice of final rule for "System Safeguards Testing Requirements," which promulgates new cybersecurity testing requirements. http://www.cftc.gov/idc/groups/public/@lrfederalregister/documents/file/2016-22174a.pdf

[15] See: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/150717_Carter_CybersecurityRequirements_Web.pdf

[16] California State Assembly member Ed Chau filed "AB-1186 Cybersecurity" on February 21, 2017, which declares his intent "to enact legislation relating to cybersecurity." See: http://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB1186

	Issuing Org	Date	Description
9	FTC	9/12/2016	*Federal Register* solicitation concerning update to the "Disposal of Consumer Information and Records Rule," which requires properly dispose of consumer report information and reasonable measures to protect it from unauthorized access; solicitation poses question whether disposal requirements should be more prescriptive and/or reference other information destruction frameworks. https://www.ftc.gov/system/files/documents/federal_register_notices/2016/09/160915frn.pdf
10	FFIEC	9/9/2016	Revised "Information Security Booklet" issued for the "FFIEC IT Examination Handbook." https://www.ffiec.gov/press/PDF/FFIEC_IT_Handbook_Information_Security_Booklet.pdf
11	FTC	8/29/2016	*Federal Register* solicitation concerning update to the "Standards for Safeguarding Customer Information" (the Safeguards Rule), which requires financial institutions to develop, implement and maintain a comprehensive information security program for handling customer information; solicitation proposes incorporation of the NIST Cybersecurity Framework and expansion of certain key definitions. https://www.ftc.gov/system/files/documents/federal_register_notices/2016/09/frn_standards_for_safeguarding_customer_information.pdf
12	FFIEC	4/29/2016	"Appendix E: Mobile Financial Services" issued as an appendix to the "Retail Payments Booklet" of the "FFIEC IT Examination Handbook." https://www.ffiec.gov/press/PDF/FFIEC_CCR_System_Federal_Register_Notice.pdf
13	NCUA	1/11/2016	Letter No.: 16-CU-01, "Supervisory Priorities for 2016", which states "NCUA encourages all credit unions to use the FFIEC tool to manage cybersecurity risks. NCUA also plans to begin incorporating the Cybersecurity Assessment Tool into our examination process in the second half of 2016." https://www.ncua.gov/regulation-supervision/pages/policy-compliance/communications/letters-to-credit-unions/2016/01.aspx
14	CFTC	12/23/2015	*Federal Register* notice of proposed rulemaking, "System Safeguards Testing Requirements for Derivatives Clearing Organizations." http://www.cftc.gov/idc/groups/public/@newsroom/documents/file/federalregister121615b.pdf
15	CFTC	12/23/2015	*Federal Register* notice of proposed rulemaking, "System Safeguards Testing Requirements." http://www.cftc.gov/LawRegulation/FederalRegister/ProposedRules/2015-32143
16	FFIEC	11/10/2015	Revised "IT Examination Handbook: Management Booklet" issued. http://ithandbook.ffiec.gov/it-booklets/management.aspx
17	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. https://www.nfa.futures.org/nfamanual/NFAManual.aspx?RuleID=9070&Section=9
18	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 http://www.maine.gov/pfr/financialinstitutions/bulletins/bull80.htm
19	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 http://www.mass.gov/ocabr/docs/dob/industry-letter-cyber-09302015.pdf

	Issuing Org	Date	Description
20	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 http://www.dob.texas.gov/public/uploads/files/news/Industrynotices/in2015-08.pdf
21	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 https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf
22	FFIEC	6/30/2015	FFIEC Cybersecurity Assessment Tool https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_June_2015_PDF2.pdf
23	FTC	6/30/2015	FTC Issues "Start with Security, A Guide for Business: Lessons Learned from FTC Cases," which details cybersecurity expectations to avoid UDAP enforcement action. The FTC regulates through rulemaking as well as through enforcement actions. https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf
24	SEC	4/28/2015	Division of Investment Mgmt's "Guidance Update: Cybersecurity Guidance" for investment advisors https://www.sec.gov/investment/im-guidance-2015-02.pdf
25	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." http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/appendix-j-strengthening-the-resilience-of-outsourced-technology-services.aspx

Table B. Regulatory Requirements and Proposals affecting financial institutions' cybersecurity programs generally.

	Issuing Org	Date	Description
26	CFPB	11/22/2016	*Federal Register* notice and "Request for Information Regarding Consumer Access to Financial Records," seeking comment on whether to undertake a rulemaking subject to Dodd-Frank Section 1033 and with what requirements; as described in comments by Director Cordray and in the RFI, a subsequent rule could conflict with "safety and soundness" information security requirements https://www.federalregister.gov/documents/2016/11/22/2016-28086/request-for-information-regarding-consumer-access-to-financial-records
27	FinCEN	10/25/2016	Advisory FIN-2016-A005 issued, entitled "Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime," which directs financial institutions to file Suspicious Activity Reports (SARs) for certain enumerated "cyber-events" https://www.fincen.gov/sites/default/files/advisory/2016-10-25/Cyber%20Threats%20Advisory%20-%20FINAL%20508_2.pdf
28	SWIFT	9/27/2016	Launched "Customer Security Programme" (CSP), which consists of five strategic initiatives: (1) Improve information sharing; (2) Enhance SWIFT-related tools for customers; (3) Enhance guidelines and provide audit frameworks; (4) Support increased transaction pattern detection; and (5) Enhance support by third party providers. SWIFT members will have to comply with the SWIFT

	Issuing Org	Date	Description
			compliance framework by January 2018. Non-compliant members will be reported to their regulators. https://www.swift.com/myswift/customer-security-programme-csp_#topic-tabs-menu
29	CPMI-IOSCO	6/29/2016	Publication of "Guidance on cyber resilience for financial market infrastructures," which provides guidance for financial market infrastructures to enhance cyber resilience. IOSCO member agencies regulate "more than 95% of the world's securities markets in more than 115 jurisdictions." https://www.iosco.org/library/pubdocs/pdf/IOSCOPD535.pdf
30	PCI	4/28/2016	Issuance of the "Payment Card Industry Data Security Standard" (PCI-DSS), version 3.2, which is required for those that accept or process payment cards. https://www.pcisecuritystandards.org/document_library
31	SEC	12/31/2015	*Federal Register* notice of advance notice of proposed rulemaking, concept release, and request for comment on "Transfer Agent Regulations," which poses 21 questions related to potential cybersecurity regulation of transfer agents. https://www.gpo.gov/fdsys/pkg/FR-2015-12-31/pdf/2015-32755.pdf
32	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" http://www.naic.org/documents/committees_ex_cybersecurity_tf_related_roadmap_cybersecurity_consumer_protections.pdf
33	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." https://www.sec.gov/rules/concept/2015/33-9862.pdf
34	FINRA	2/3/2015	Summary of cybersecurity principles and effective practices as reported in its February 3, 2015 Report on Cybersecurity Practice https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf

Table C. Government-led Cybersecurity Initiatives affecting financial institution cybersecurity programs.

	Issuing Org	Date	Description
35	DHS	1/18/2017	Issuance of an updated "National Cyber Incident Response Plan." NCIRP builds upon PPD-41 and outlines the roles and responsibilities of federal, state, local, tribal, territorial, private sector, and international stakeholders during a cyber incident; identifies the core capabilities required in the event of a cyber incident; and describes the coordination structure the Federal Government will use to coordinate its activities with affected stakeholders. https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf
36	NIST	1/10/2017	Issuance of an updated NIST Cybersecurity Framework – a version 1.1 – that expands the original Framework to include "supply chain risk management," with a solicitation for comment. https://www.nist.gov/sites/default/files/documents/2017/01/30/draft-cybersecurity-framework-v1.1-with-markup.pdf

	Issuing Org	Date	Description
37	Treasury as part of G-7	10/11/2016	Publication of the Group of 7 (G-7) "Fundamental Elements of Cybersecurity for the Financial Sector," which are described as a concise set of principles on best practices in cybersecurity for public and private entities in the financial sector. While these fundamental elements are described as principles, outside the United States (Treasury is not a regulatory agency), these principles as described and arranged could form the basis for downstream regulations in the other G-7 countries where regulatory oversight and jurisdiction is less complex than in the United States. https://www.treasury.gov/resource-center/international/g7-g20/Documents/G7%20Fundamental%20Elements%20Oct%202016.pdf
38	White House	7/26/2016	Presidential Policy Directive/PPD-41, entitled "United States Cyber Incident Coordination," which sets forth principles governing the Federal Government's response to any cyber incident, whether involving government or private sector entities. https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident
39	CPMI-IOSCO	6/29/2016	Publication of "Guidance on cyber resilience for financial market infrastructures," which provides guidance for financial market infrastructures to enhance cyber resilience. IOSCO member agencies regulate "more than 95% of the world's securities markets in more than 115 jurisdictions." https://www.iosco.org/library/pubdocs/pdf/IOSCOPD535.pdf
40	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" http://www.naic.org/documents/committees_ex_cybersecurity_tf_related_roadmap_cybersecurity_consumer_protections.pdf
41	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 http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8074v1.pdf
42	FCC	7/10/2015	Issuance of "TCPA Omnibus Declaratory Ruling and Order," which placed impediments on financial institutions and businesses generally in notifying customer of potential security breaches via mobile/cellular channels. https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-72A1_Rcd.pdf
43	Commerce, BIS	5/20/2015	Department of Commerce, Bureau of Industry and Security proposed rulemaking to implement Wassenaar Arrangement agreement to limit the import/export (or deemed "export") of intrusion software (e.g., penetration testing software). While the United States is unlikely to implement the rule, those other 40 countries that are part of the Wassenaar arrangement may well do so, as limited revisions were accepted at the December 2016 plenary. https://www.bis.doc.gov/index.php/forms-documents/doc_download/1236-80-fr-28853

APPENDIX 5. Complexity in Reconciliation (Select Proposals Graphically Mapped to the NIST *Cybersecurity Framework*)