February 17, 2017

Via electronic submission: regs.comments@federalreserve.gov; regs.comments@occ.treas.gov ; Comments@fdic.gov

Mr. Robert deV. Frierson
Secretary
Board of Governors of the Federal Reserve System
20th Street & Constitution Avenue, N.W.
Washington, DC 20551

Legislative and Regulatory Activities Division
Office of the Comptroller of the Currency
400 7th Street, SW., Suite 3E-218, Mail Stop 9W-11
Washington, DC 20219

Mr. Robert E. Feldman
Executive Secretary
Attention: Comments
Federal Deposit Insurance Corporation
550 17th Street, NW
Washington, DC 20429

Re: *Enhanced Cyber Risk Management Standards* (FRB Docket No. R-1550; RIN 7100-AE 61; Docket ID OCC-2016-0016; FDIC RIN 3064-AE45)

Dear Sirs and Madam;

The Financial Services Sector Coordinating Council (FSSCC)[1] appreciates the opportunity to provide comment on the advanced notice of proposed rulemaking (ANPR), *Enhanced Cyber Risk Management Standards*, jointly issued by the Board of Governors of the Federal Reserve System (Federal Reserve), the Office of the Comptroller of the Currency (OCC), and the Federal Deposit Insurance Corporation (FDIC) (the agencies).[2]

[1] Established in 2002 by the financial sector, FSSCC coordinates critical infrastructure and homeland security activities representing financial trade associations, financial utilities, and financial firms. FSSCC's mission is to strengthen critical infrastructure resiliency by identifying threats, promoting protection and preparedness, collaborating with the federal government, and coordinating crisis response for the benefit of the financial services sector, consumers and the nation. https://www.fsscc.org/About-FSSCC and charter https://www.dhs.gov/sites/default/files/publications/FSSCC-Charter-03-15-508.pdf.

[2] *Enhanced Cyber Risk Management Standards*, 81 Fed. Reg. 74315 (proposed Oct. 26, 2016), www.federalregister.gov/documents/2016/10/26/2016-25871/enhanced-cyber-risk-management-standards.

To develop these comments and recommendations, FSSCC facilitated a broad-based, cross-industry collaboration that included member financial firms, utilities and exchanges, and trade associations, representing a cross-section of the financial services industry.[3]

I. Convene a Collaborative Public-Private Sector Dialogue Before the ANPR Moves Forward.

The FSSCC recommends a robust public-private sector dialogue to address the critical infrastructure policy questions raised in the ANPR. A collaborative dialogue could address the complex questions, collective interest in enhancing the security and resiliency of the financial services sector, and potential regulatory burden. This stakeholder process could leverage existing venues, such as working through the Cybersecurity Profile Development Working Group of the Critical Infrastructure Partnership Advisory Council (CIPAC). This would allow confidential collaboration on shared objectives and identification of consensus-based cybersecurity standards that make the sector systemically more secure [See Appendix A for a detailed summary of CIPAC's creation and mission].[4] Therefore, FSSCC encourages the agencies to initiate an engagement with sector partners immediately to focus on the questions posed in the ANPR.

The dialogue could begin with a gap analysis to identify systemic security and management priorities with a long term goal of harmonizing the fragmented regime of cyber rules, regulations, guidance, and tools. Although the ANPR presents many questions for the sector, FSSCC urges an initial focus on:

1) adopting a multifactor approach to applicability,
2) addressing third party compliance and substitutability,
3) specifying scenarios for incident and recovery planning,
4) promoting flexible risk-based governance and reporting principles, and
5) building a consensus on methods to quantify cybersecurity risk.

---

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

[4] The Department of Homeland Security (DHS) established CIPAC in 2006 to facilitate interaction among the public sector and critical infrastructure owners and operators. The CIPAC is a forum for public and private sector entities to organize as coordinating councils and jointly support and coordinate critical infrastructure security and resilience efforts. It supports the implementation of the U.S. Department of Homeland Security's (DHS) *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security Resilience* prepared in response to the *Presidential Policy Directive 21, Critical Infrastructure Security and Resilience*. https://www.dhs.gov/financial-services-working-groups and FSSCC Charter (March 2015), *CIPAC Membership and Representation,* https://www.dhs.gov/financial-services-sector-council-charter-and-membership (last visited Feb. 13, 2017).

DHS provided that under the auspices of CIPAC, individual sectors could form CIPAC subgroups consisting of its respective sector coordinating council and government coordinating council to address sector-specific concerns. 71 Fed. Reg. at 14932 (March 24, 2006). Under this authority, subgroups are afforded the protections under the 2006 notice and the Homeland Security Act of 2002, Section 871, which together exempt them from Federal Advisory Committee Act constraints. 71 Fed. Reg. at 14933 (March 24, 2006). *See* Appendix A.

A. *Enhance National Cybersecurity through Sector Collaboration and Coordination*

Financial services sector collaboration is proven by its history of demonstrable achievements. Through the FSSCC, and other financial services coordination processes, the sector has worked diligently for two decades to enhance cyber defenses in collaboration with U.S. government, including the agencies and other critical infrastructure sectors. In addition to the detailed list in Appendix B, the key cyber accomplishments and initiatives of financial sector cyber collaboration include establishing the Financial Services Information Sharing and Analysis Center (FS-ISAC),[5] launching the Financial Services Sector Coordinating Council (FSSCC),[6] robustly engaging in the joint private-public sector development of the National Institute of Standards and Technology *Framework for Improving Critical Infrastructure Cybersecurity* (NIST Framework),[7] developing and expanding 'Hamilton Series' of thirteen cybersecurity tabletop exercises,[8] and building the Sheltered Harbor initiative to improve cyber incident restoration capabilities.[9]

B. *Improve National Cybersecurity and Reduce Private Sector Costs by Harmonizing Fragmented Regulation*

The FSSCC encourages all federal and state agencies to adhere to a common cybersecurity approach developed in collaboration with industry, as was done with the NIST Framework, when pursuing cybersecurity regulatory endeavors. The current web of cybersecurity regulation is complex and marked by overlapping requirements, guidance, and issuances from agencies and self-regulatory organizations with varying oversight and responsibility. A focused effort to harmonize these regulations and other requirements would improve the ability of the financial industry and regulators to meet current needs and to adapt quickly to future cyber threats.

---

[5] Launched in 1999, FS-ISAC was established by the financial services sector in response to *Presidential Directive No. 63*, 63 Fed. Reg. 41804 (May 23, 1998). www.gpo.gov/fdsys/pkg/FR-1998-08-05/pdf/98-20865.pdf and *Homeland Security Presidential Directive No. 7*, 39 Weekly Compilation of Presidential Documents 51, 1816 – 1822 (December 22, 2003) www.hsdl.org/?abstract&did=441950 mandated that the public and private sectors share information about physical and cyber security threats and vulnerabilities to help protect the U.S. critical infrastructure. *See infra* Appendix B, 17.

[6] *See supra* at note 1.

[7] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity Version 1.0* (Feb 12, 2014). www.nist.gov/cyberframework

[8] *See infra* Appendix B, 17.

[9] *See infra* Part II(D)(ii) *Accommodate Sheltered Harbor Enabled Recovery Planning and Preservation of Record Requirements*, 10, and Appendix B, 17.

As the ANPR recognizes, financial institutions and financial services companies comply with a broad array of cyber obligations, including the Gramm-Leach-Bliley Act (GLBA)[10] and the subsequent *Interagency Guidelines Establishing Information Security Standards*;[11] Federal Financial Institutions Examination Council (FFIEC)[12] *Information Technology (IT) Examination Handbook*,[13] and *Cybersecurity Assessment Tool (CAT)*,[14] and the Federal Reserve, OCC, and the Securities and Exchange Commission (SEC) *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System.*[15] In addition to federal efforts, states increasingly are interested in pursuing their own approaches. In February 2017, the New York Department of Financial Services released a financial services-specific cybersecurity rule, which is seen as a harbinger of further state attempts to regulate the cybersecurity of financial services.[16]

Since 2014, federal and state agencies, self-regulatory organizations, and international regulatory bodies have issued or proposed 43 differing cybersecurity frameworks, questionnaires, rules, and requirements applicable to the financial services sector. [See Appendix C for list of cybersecurity regulatory actions]. In addition to these directly applicable regulatory activities, the sector also is impacted significantly by a variety of sector-relevant government actions. Although some of these initiatives incorporate a common lexicon and well-regarded cybersecurity frameworks, such as the NIST Framework or the International Organization for Standardization,[17] others are rooted in differing frameworks, standards, structures offering idiosyncratic terminology, approaches, and language.

---

[10] Financial Services Modernization Act of 1999 (the Gramm-Leach-Bliley Act), 15 U.S.C. § 6801 *et seq*., 16 C.F.R. § 313.1 *et seq.* (privacy), 16 C.F.R. §314.1 *et seq.* (safeguarding).

[11] 66 Fed. Reg. 8633, Feb. 1, 2001, *as amended at* 69 Fed. Reg. 77616, Dec. 28, 2004; 70 Fed. Reg. 15751, 15753, Mar. 29, 2005; 71 Fed. Reg. 5780, Feb. 3, 2006.

[12] The FFIEC "is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions…and to make recommendations to promote uniformity in the supervision of financial institutions." It was established on March 10, 1979 under the *Financial Institutions Regulatory and Interest Rate Control Act of 1978*, Pub L No. 95-630. https://www.ffiec.gov/about.htm

[13] The FFIEC IT Examination HandBook InfoBase is an online compendium of the eleven booklets and nearly 1000 pages of the FFIEC IT Handbook, and the association Resources, Reference Materials, and Glossary. http://ithandbook.ffiec.gov/

[14] Federal Financial Institutions Examination Council, *Cybersecurity Assessment Tool* (June 30, 2015). www.ffiec.gov/cyberassessmenttool.htm

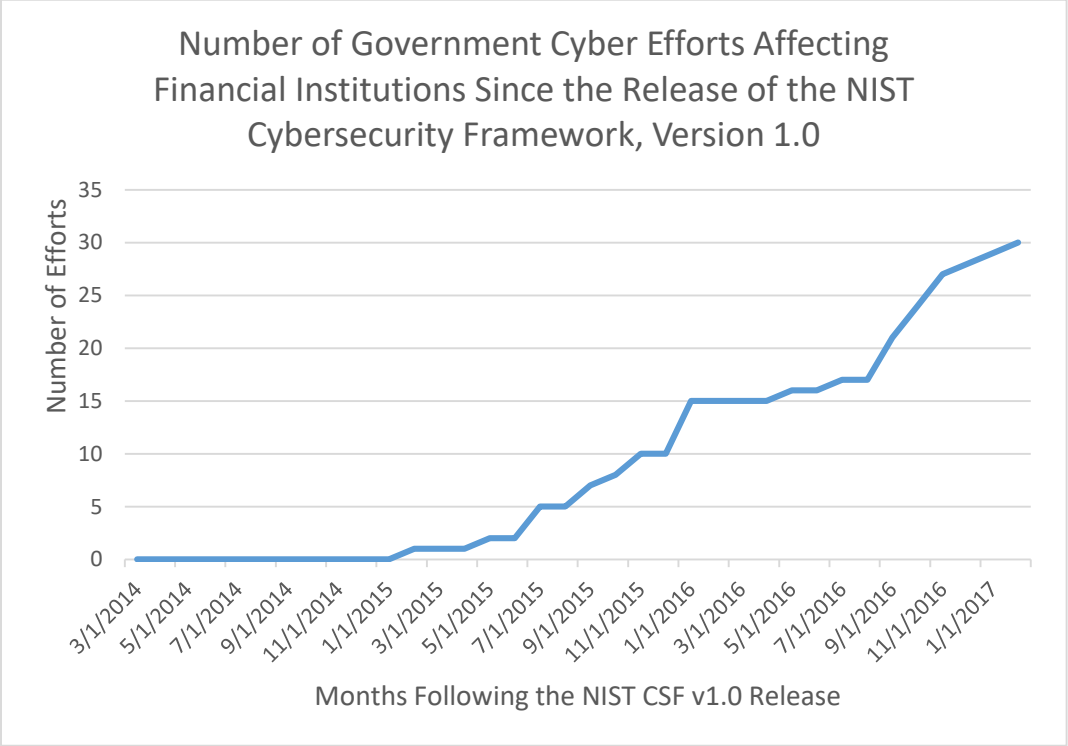
[15] 68 Fed. Reg. 70, 17809 (April 11, 2003).

[16] *Cybersecurity Requirements for Financial Services Companies*, (website published Feb. 16, 2017) to be codified at N.Y. Comp. Codes R. & Regs. tit. 23, § 500. http://www.dfs.ny.gov/legal/regulations/adoptions/rf23-nycrr-500_cybersecurity.pdf (last visited Feb. 17, 2017). The regulation will be become effective upon publication in the New York State Register on March 1, 2017.

[17] "ISO is an independent, non-governmental international organization with a membership of 161 national standards bodies. …[I]t brings together experts to share knowledge and develop voluntary, consensus-based, market relevant International Standards that support innovation and provide solutions to global challenges….ISO has published more than 21000 International Standards and related documents, covering almost every industry, from technology, to food safety, to agriculture and healthcare. ISO International Standards impact everyone, everywhere." http://www.iso.org

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.

See Appendix C for detailed catalogue.



As currently drafted, the ANPR would further complicate this environment, as it includes 84 proposed standards addressing eight risk categories. These new standards, added to the current lack of regulatory harmonization and alignment, would require firms to expend more of their cyber resources reconciling differing approaches. Disparate requirements in structure, language, exam questionnaires, frameworks, and tools hinder the ability of firms to identify key issues and evaluate the effectiveness of cybersecurity efforts.[18] With the multiple layers of cyber initiatives currently being issued, a multinational FSSCC member estimates that 40% of its cybersecurity efforts are reconciliation and demonstration of compliance, not cybersecurity.[19]

[18] A fragmented approach compounds inefficient parsing, identifying, drafting, and compiling of equivalent data from similar systems multiple times for different regulators. As a result, resources are directed to creating single-use compliance data, rather than security and mitigation techniques that qualitatively improve a firm's cybersecurity.

[19] This comment was gleaned from a 2016 internal survey of FSSCC members.

A risk-focused, principles-based, and consistent approach to cybersecurity would reduce costs, improve risk management, and enhance cybersecurity. A common methodology also would assist internal communications among corporate cybersecurity professionals from the control room to the boardroom, and would facilitate external communication with other firms, sectors, and regulatory agencies. This commonality would facilitate efficient consistent responses to regulatory requests, and importantly, focus resources on improving cybersecurity capabilities.

II. Develop Effective Cyber Requirements through Public-Private Sector Dialogue

The FSSCC strongly agrees with the goal of assuring the safety and security of the sector. To meet this shared objective, it is necessary for all stakeholders, including federal entities, to engage in a meaningful dialogue addressing cybersecurity threats to the sector and nation. Acknowledging the ANPR's purpose to avoid contagion and systemic risk,[20] the cybersecurity response should be considered from a systemic, sector-wide perspective expressed in flexible objectives and risk-based principles, rather than prescribing the activities of individual firms.

A. Initiate a Comprehensive Gap Analysis of Existing Cybersecurity Regulation

While regulatory requirements and guidance can contribute to improved cybersecurity when outcome-focused and narrowly tailored, complex and overlapping rules force industry to focus limited resources on mapping and process translation for differing organizational hierarchies and terminology within the various regulatory regimes instead of protecting networks and systems. To mitigate this complexity, FSSCC suggests a comprehensive review and gap analysis of existing financial services cybersecurity regulatory regimes.

Similar gap reviews were recommended recently by the Commission on Enhancing National Cybersecurity report, *Securing and Growing the Digital Economy,*[21] and the Center for Strategic and International Studies (CSIS) Cyber Policy Task Force report, *From Awareness to Action: A Cybersecurity Agenda for the 45th President*.[22] These bipartisan reports recommend examining regulatory regimes together and holistically, reoccurring risk-based elements identified, requirements supporting those elements evaluated for effectiveness, non-effective requirements streamlined, gaps in the regulatory regime identified, remaining elements, requirements, and identified gaps tied into a risk-based cybersecurity framework, such as the NIST Framework, and identified gaps addressed with risk-based regulatory principles.[23]

---

[20] 81 Fed. Reg., at 74324 (Oct. 26, 2016) "The agencies are considering a requirement that covered entities establish and implement plans to identify and mitigate the cyber risks they pose through interconnectedness to sector partners and external stakeholders to prevent cyber contagion."

[21] The Commission, established under Executive Order 13718 (Feb. 9, 2016), issued its report Dec. 9, 2016. https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf

[22] Composed of co-chairs Sen. Sheldon Whitehouse, Rep. Michael T. McCaul, Karen Evans, and Sameer Bhalotra, CSIS Task Force released its report on Jan. 8, 2017. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/170110_Lewis_CyberRecommendationsNextAdministration_Web.pdf

[23] These gap reviews also would support requirements under the *Economic Growth and Regulatory Paperwork Reduction Act,* 12 U.S.C. § 3311 and the *Unfunded Mandates Reform Act*, Pub. L. No. 104-4, 109 Stat 48 (1995), codified at 2 U.S.C. § 1501.

Mapping the analytical nexus among overlapping state, federal, and international cybersecurity guidelines—and understanding how the ANPR interrelates—is essential work as frameworks multiply in number and complexity. The FSSCC currently is conducting a comprehensive review of applicable regulation, guidance, frameworks, and tools used in the financial services sector, and would welcome the opportunity to work with the agencies, executive branch, and self-regulatory organizations.[24] Furthermore, efforts to resolve the ANPR questions would be informed and improved by awaiting the proposed NIST Framework, version 1.1 revisions, which also address similar themes of risk measurement and third party cyber supply chain risk management.[25]

B. Adopt a Multifactor Scope of Application, Including Size and Interconnectedness

The ANPR asks whether "alternative size thresholds or measures of risk to the safety and soundness of the financial sector and the U.S. economy" exist that should be considered in determining the scope of application.[26] The FSSCC recommends that the application of any enhanced standard be grounded in multiple factors, which include size and interconnectedness as non-exclusive elements of scope.[27] An emphasis on size or interconnection alone is misplaced—unless the nature of risk flowing through the interconnection is correctly identified.[28] The financial services sector is large, diverse, and not amenable to one-size-fits-all standards.

Appropriately tailored rules that are responsive to a dynamic threat environment and focused in application are best developed collaboratively with industry. A flexible, dynamic process is needed to accomplish the essential work of defining cyber standards that are responsive to size, risk, and business model within an evolving threat environment and a complex, diverse sector. An interactive, ongoing public-private dialogue among institutions, the agencies, and relevant federal entities would best define the scope of application where a fixed prescriptive rule could not capture the dynamic nature of cyber risk to the financial sector.

---

[24] *See* fsscc.morwebcms.com/files/galleries/NISTcommentletterSigned-0001.pdf; www.fsscc.org/files/galleries/FSSCC_Submission_to_the_Presidential_Commission_on_Enhancing_National_Cybersecurity_Letter_vF.pdf

[25] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity Draft Version 1.1* (January 10, 2017). Comments due April 10, 2017. Final revisions are anticipated in Q4 2017 or Q1 2018. https://www.nist.gov/sites/default/files/documents/2017/01/30/draft-cybersecurity-framework-v1.1-with-markup.pdf

[26] 81 Fed. Reg. 207, at 74318.

[27] "…"[I]nterconnectedness" is defined as a broad set of relationships and interactions among financial market participants…The specific institutional setting of these connections may, in turn, affect the type of potential vulnerabilities they create. As institutions form connections, they may contribute to a stronger, more robust system, but they may also create potential channels for the propagation of shocks." Kara, Gazi, Mary Tian, and Margaret Yellen, Board of Governors of the Federal Reserve System, FEDS Notes, *Taxonomy of Studies on Interconnectedness* (July 31, 2015). https://www.federalreserve.gov/econresdata/notes/feds-notes/2015/taxonomy-of-studies-on-interconnectedness-20150731.html#fn1 (last visited Feb. 17, 2017).

[28] For example, factors may include whether an entity is a service provider or not, volume of settlement or payment activity, or the ripple effect of business disruption among interconnected financial services companies.

C. Develop a Balanced Approach towards Third Party Service Provider Compliance and Substitutability

The third-party service provider ecosystem is complex and includes a broad range of services, often facilitated through standard commercial agreements. A balanced cybersecurity risk management approach should consider a firm's risk management practices, the cybersecurity roles and responsibilities of the service providers, and the contractual relationships between the firms and the providers to avoid creating significant business and cyber risks.

i. Due Diligence Requirements and Third Party Service Provider Compliance

Within the ANPR, the agencies consider whether to apply standards directly to third-party service providers.[29] The diversity of financial services companies and the third party service providers upon which they rely creates significant concerns for how broad-based requirements would be feasible and desirable. Additionally, the underlying statutory authorities for applying requirements upon these providers are unclear as information security, cloud services, technology platforms, and cybersecurity operations do not fit neatly within the common definition of bank services.[30] The long-term goal should be agency-approved third party certifications to replacing or supplementing the existing burdensome and piecemeal due diligence process.

As with financial services companies, the appropriate scoping of the applicability of cybersecurity standards to third party service providers is essential. The need for sector-wide security must be balanced with the need for third party provided expertise for efficient, effective operations. Any standard applied to third parties should employ multi-factor scoping to avoid driving third parties out of financial services due to compliance costs or risk-inappropriate requirements.

[29] 81 Fed. Reg. 207, at 74318. "As noted, the agencies are considering whether to apply the standards to thirdparty service providers with respect to services provided to depository institutions and their affiliates that are covered entities (covered services)."

[30] Bank Services Company Act of 1968, 12 U.S.C. § 1863. "…a bank service company may perform, the following services []: check and deposit sorting and posting, computation and posting of interest and other credits and charges, preparation and mailing of checks, statements, notices, and similar items, or *any other clerical, bookkeeping, accounting, statistical, or similar functions* performed for a depository institution." (emphasis added).

ii. *Practicality of Third Party Substitutability and Redundancy*

The ANPR preference for substitutability for critical third parties may not be practicable. Alternate providers for every service or redundancy are not always available depending on the expertise required or type of service. For example, some critical settlement services may only be offered by a national government, central bank, or other federal entity.[31]

D. Specify a Range of Scenarios for Incident and Recovery Planning

The FSSCC shares the goal of resuming sector-critical operations quickly and safely. To be achievable, FSSCC recommends adopting a risk-based scenario-dependent approach that permits financial institutions a reasonable amount of time to determine the nature and scope of the incident that acknowledges existing recovery guidance applicable to the sector.[32] The development of examples and hypothetical scenarios in collaboration with the agencies, relevant executive branch stakeholders, and cross-sector Information Sharing and Analysis Centers (ISACs) would assist incident and recovery planning by illustrating risk-based and scenario-dependent recovery objectives and reference points.

i. Adopt Flexible Resumption of Service and Recovery Time Objectives (RTO)

Timeliness of recovery should be contingent on many factors, including the cause of an operational disruption:

1) physical event, such as a natural disaster, or a cyber event;
2) outage of a private provider or component of the public infrastructure, such as the electric grid;
3) system compromise requiring data restoration; or
4) cyber attack, resulting from the singular act of a cybercriminal, or a sustained attack by a nation-state.

Each of these scenarios would have a varying and differing RTO. A fixed two-hour recovery time could result in premature return to operations and sector-wide vulnerability. A firm needs adequate time to confirm whether potentially destructive malware is propagating, or the possibility of negative cascading events due to system compromise.

---

[31] The FSSCC, in conjunction with the Financial and Banking Information Infrastructure Committee (FBIIC), plans to work on substitutability as an outcome of the October 20, 2016 meeting with U.S. Treasury Secretary Jacob J. Lew and Assistant to the President for Homeland Security and Counterterrorism Lisa Monaco. *Readout from a Treasury Spokesperson of the Administration's Meeting with Financial Regulators and CEOs on Cybersecurity in the Financial Services Sector* https://www.treasury.gov/press-center/press-releases/Pages/jl0589.aspx. *See also* www.fbiic.gov.

[32] *E.g.*, CFTC's *System Safeguards Testing Requirements for Derivatives Clearing Organizations*, 81 Fed. Reg. 181, 64322 (Sept. 19, 2016). SEC's *Regulation Systems Compliance and Integrity* (Regulation SCI), 79 Fed. Reg. 234, 72252 (Dec. 5, 2014).

ii. Accommodate Sheltered Harbor Enabled Recovery Planning and Preservation of Record Requirements

The ANPR's consideration of recovery plan requirements and preservation of critical records is similar to the capabilities enabled by the private-sector Sheltered Harbor resolution enabling tool.[33] The purpose of Sheltered Harbor is to quickly and securely implement resiliency measures and customer account protections, and would only be invoked after all resiliency and business continuity planning measures are exhausted. Contingent on an agency determination that the firm is no longer viable, a Sheltered Harbor enabled restoration would require several days to implement.

Born out of the public-private Hamilton Series cybersecurity tabletop exercise, industry created Sheltered Harbor as a voluntary cooperative program to create operating standards to restore account data in the event of failure or a catastrophic incident of a bank of security firm. In the past year, industry developed Sheltered Harbor standards for data formats, encryption, and vaults to enable offsite restoration of retail customer account data at the direction of pertinent regulatory agencies. The process continues to be dynamic, and as implementation begins, industry is learning and advancing standards as needed. Encouragement from the agencies would be beneficial, and endorsement of Sheltered Harbor's goals is important, but a dynamic, detailed, and proprietary process does not lend itself to the long change cycles of precise regulation.

This private sector effort should be encouraged, and any regulatory activity should not impede completion and efforts for broad adoption. A secure, ongoing public-private sector collaboration could offer a venue for sharing Sheltered Harbor details and confidentially addressing regulatory questions while protecting Sheltered Harbor's intellectual property.

E. Employ Flexible Risk Governance and Reporting Principles in a Diverse Financial Services Sector

The FSSCC suggests a principles-based corporate governance and reporting structure that describes oversight objectives that are flexible and risk-based. Diversity of size, charter, holding company structure, geography, and business model is a distinct feature of the American financial services sector. Entities should have governance structures consistent with their business needs and overall risk management strategies.

---

[33] "The agencies are [] considering requiring covered entities to establish protocols for secure, immutable, off-line storage of critical records, including financial records of the institution, loan data, asset management account information, and daily deposit account records, including balances and ownership details, formatted using certain defined data standards to allow for restoration of these records…." 81 Fed. Reg. at 74324.

Existing within FS-ISAC's umbrella focal point for sector-wide cybersecurity efforts, Sheltered Harbor is closely aligned with FSSCC and other public-private cooperative cyber security initiatives. It is governed by a board of directors representing a diverse banking and brokerage industry, trade associations, and core processors. This governance model successfully and cost-effectively builds, funds, and operates the effort. https://www.fsisac.com/sites/default/files/news/SH_FACT_SHEET_2016_11_22_FINAL3.pdf

As proposed, the ANPR makes reference to common risk-based activities of "developing and maintaining a formal cyber risk management strategy, as well as a supporting framework of policies and procedures," but, contrary to risk-based frameworks, it prescribes specific actions such as board level cyber expertise and detailed mapping of all internal and external dependencies, regardless of risk.[34] These required structures, internal staffing hierarchies, and governance configurations impose compliance costs and organizational burdens without correlated improvement in cybersecurity or internal oversight.

F. Build a Consensus-Based Cross-Sector Method to Quantify Cybersecurity Risk

The first step in developing "a consistent, repeatable methodology to support the ongoing measurement of cyber risk"[35] is articulating and agreeing to the objectives and the purpose of quantitative methods. The need to develop tools to quantify cyber risk and to assist risk management is well-recognized, as is the current lack of commonly accepted measurement practices. In January 2017, the bipartisan Center for Strategic and International Studies (CSIS) Cyber Policy Task Force released its cybersecurity recommendations for the incoming administration, which describe cybersecurity metrics as "essential information for guiding policy."[36] Echoing the recommendation of the 2016 Commission on Enhanced National Cybersecurity,[37] CSIS reiterates that the "lack of measurements on adoption and effectiveness remains a problem for assess[ment]..." and recommends public sector collaboration "…working with the private sector… [and] publiciz[ing] specific implementation examples and measurement tools that organizations can use to implement the framework."[38] As there is no common method to quantify cyber risk across firms or sectors, significant time is needed to develop a consensus on a risk measurement standard that would enable financial services to measure and mitigate their individual risk.[39]

---

[34] *Category 1—Cyber Risk Governance*, 81 Fed. Reg. 207, at 74320.

[35] *Approach to Quantifying Cyber Risk*, *Id.* at 74326.

[36] "Metrics provide essential information for guiding policy. The lack of measurements on adoption and effectiveness remains a problem for assessing the framework. NIST should be tasked to develop these metrics, working with the private sector. In doing this, NIST should publicize specific implementation examples and measurement tools that organizations can use to implement the framework." CSIS, at 21.

[37] "NIST, in coordination with the [commission proposed] National Cybersecurity Private–Public Program (NCP[3]), should establish a Cybersecurity Framework Metrics Working Group (CFMWG) to develop industry-led, consensus-based metrics that may be used by (1) industry to voluntarily assess relative corporate risk, (2) the Department of Treasury and insurers to understand insurance coverage needs and standardize premiums, and (3) DHS to implement a nationwide voluntary incident reporting program for identifying cybersecurity gaps. This reporting program should include a cyber incident data and analysis repository (CIDAR)." Cyber Commission 2016, Recommendation 1.4.1, at 26. https://www.whitehouse.gov/the-press-office/2016/02/09/executive-order-commission-enhancing-national-cybersecurity

[38] *See supra* at Note 34, p 55.

[39] The January 2017 proposed revision to the NIST Framework addresses measuring and demonstrating cybersecurity risk in Section 4. *See supra* at Note 7, p 21.

G. Harmonize Sector Critical Designation with Existing Definitions, Terms, and Criteria

The FSSCC recommends that the agencies conform the ANPR's use of the term "sector-critical" with existing definitions, terminology, and criteria used to identify critical systems and operations within the financial services sector.[40] Among the existing related designations are the ANPR referenced *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System*,[41] Section 9 of Executive Order 13636*, Improving Critical Infrastructure Cybersecurity,* designating the U.S. Department of the Treasury as the sector-specific agency for the financial sector,[42] the Federal Reserve's designation of systemically important financial institutions and critical operations for purposes of enhanced supervision and resolution planning,[43] the Financial Stability Oversight Council's designation of systemically important financial market utilities,[44] SEC Regulation SCI,[45] and the Commodity Futures Trading Commission's critical infrastructure regulations.[46]

The ANPR introduces the concept of a two-tiered system without defining the scope of sector critical systems. Without these details, it is difficult to evaluate the merits of the proposal or how it would affect compliance with existing cybersecurity frameworks, which also identify critical systems and enhanced standards.

Identifying systems that generate true sector systemic risk is not a trivial task. It requires technical expertise and detailed understanding of individual firms, broader financial sector dynamics, and market mechanics. Moreover, identification of such systems demands holistic understanding of the financial services sector's relationship with broader critical infrastructure, such as the telecommunications and energy sectors. A new term, definition, or criteria in the ANPR for sector-critical systems should be harmonized with existing definitions of criticality. Consistency would provide clarity and increase sector efficiency.

Given these complexities and the need for further clarification, FSSCC suggests a deliberate approach through a public-private dialogue to harmonize the identification of and cyber expectations for sector critical systems. A collaboration focusing on systemic risk and resiliency could first determine which financial services systems should be considered sector-critical. Once such a definition is established, the agencies and industry can work together clarify identified systemic risk, ensuring harmonization with existing definitions and sector criticality frameworks.

---

[40] 81 Fed. Reg. at 74319 (October 26, 2016), *Part IV: Sector-Critical Systems.*

[41] Federal Reserve System, Office of the Comptroller of the Currency, and the Securities and Exchange Commission, *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System*, 68 Fed. Reg. 17809 (Apr. 11, 2003), https://www.occ.gov/news-issuances/bulletins/2003/OCC2003-14a.pdf.

[42] Exec. Order 13636, 78 Fed. Reg. at 11739 (Feb. 12, 2013).

[43] Federal Reserve System, *Enhanced Prudential Standards for Bank Holding Companies and Foreign Banking Organizations*, 12 C.F.R. pt. 252, https://www.gpo.gov/fdsys/pkg/FR-2014-03-27/pdf/2014-05699.pdf.

[44] 12 C.F.R. pt. 1320.

[45] 17 C.F.R. § 240, 242, and 249.

[46] 17 C.F.R. pt. 39.

III. Convene a Public-Private Sector Dialogue in CIPAC Cybersecurity Profile Development Working Group

Recognizing its structure, mission, and legal authority, FSSCC suggests CIPAC is best positioned to address the numerous, complex issues and questions expressed in the ANPR. CIPAC and its existing financial services subgroup, the Cybersecurity Profile Development Working Group is an environment for iterative, informed sector-level conversations on strengths and weaknesses of current practices. This venue would allow for the necessary analysis of proposed standards with a mutual goal of addressing regulatory gaps. A CIPAC-led public-private dialogue could serve as a precursor to developing consensus-based cyber standards that are responsive to a dynamic threat and a diverse industry.

Conclusion

The questions outlined in the ANPR offer an opportunity for further collaboration and dialogue with industry. Beginning with a gap analysis to identify priorities, a public-private sector approach would share the work of defining applicability criteria, addressing third party compliance and substitutability, refining incident and recovery planning, developing risk-based governance and reporting principles, and building a consensus on risk measurement methods.

The FSSCC and financial services sector remains keenly supportive of public-private sector collaboration to improve national and sectoral cybersecurity—a systemic imperative requiring combined efforts and full focus. Our shared goal is a nimble harmonized response to policy, regulation, and critical infrastructure protection coordinating multiple sectors within an international landscape.

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 A. Critical Infrastructure Partnership Advisory Council (CIPAC)

Considering the breadth of the task outlined in the ANPR, the agencies will require comprehensive and ongoing feedback. The ANPR rulemaking process, even with supplementary opportunities for comment overtime, is neither adequate nor appropriately adaptive for the desired result. The FSSSCC suggests tabling the ANPR in favor of CIPAC for an iterative structured process for public and private sector representatives to collaboratively advance standards to achieve the desired outcome.[47]

What is CIPAC?

The Department of Homeland Security established the Critical Infrastructure Partnership Advisory Council (CIPAC) in 2006 to facilitate interaction among the public sector and critical infrastructure owners and operators. CIPAC is a forum for public and private sector entities to organize as coordinating councils and jointly support and coordinate critical infrastructure security and resilience efforts. It supports the implementation of the U.S. Department of Homeland Security's (DHS) *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security Resilience* prepared in response to the *Presidential Policy Directive 21, Critical Infrastructure Security and Resilience*.[48]

In the 2006 Federal Register notice announcing the formation of CIPAC, DHS noted that "[p]rotecting critical infrastructure and key resources (CI/KR) requires a comprehensive, effective, and collaborative partnership between all stakeholders."[49] Furthermore, "an effective partnership must be predicated on the ability to have ongoing, immediate, and multidirectional communication and coordination between the CI/KR owners and operators and government, including under highly exigent circumstances."[50] With the creation of CIPAC, DHS sought to further these goals and:

> *…to facilitate interaction among government representatives at the Federal, State, local, and tribal levels and representatives from the community of [CI/KR] owners and operators in each critical sector to engage in, among other things, planning; coordination; security program implementation; operational activities related to critical infrastructure protection security measures, including incident response, recovery, and reconstitution from events both man-made and naturally occurring; and the sharing of information about threats, vulnerabilities, protective measures, best practices, and lessons learned."*[51]

[47] There is precedent for ongoing agency collaboration with the private sector to achieved desired outcomes. In 2015, the Federal Reserve established a multi-stakeholder set of task forces to improve both the speed and security of the U.S. Payment system. More information can be found here: https://fedpaymentsimprovement.org/.

[48] 78 Fed. Reg. 11737 (Feb. 19. 2013).

[49] 71 Fed. Reg., at 14932 (March 24, 2006).

[50] *Id.*

[51] *Id.*

CIPAC is a Sector-Level Collaborative Body without Rulemaking Authority

In the same notice, DHS provided that under the auspices of CIPAC, individual sectors could form CIPAC subgroups consisting of respective sector coordinating council, and government coordinating council to address sector-specific concerns.[52] Within the flexible CIPAC structure, subgroups could rely on the protections afforded under the notice and the Homeland Security Act of 2002, Section 871, which together exempt them from Federal Advisory Committee Act constraints.[53]

The ANPR's focus on addressing sector level concerns is expressed in the: (a) stated purpose of increasing the resilience of interconnected firms and reducing the impact of a cyber event on the financial system as a whole; (b) creation of higher standards for "sector-critical systems," and (c) requirement that a firm consider individual actions in context of impact on the sector as a whole.[54]

[52] *Id.*

[53] The Federal Register notice establishing CIPAC also functioned as its first Charter, a charter, which pursuant to Homeland Security Act, Section 871(b), requires renewal every two years. The most recent renewal occurred on November 30, 2016, with DHS Secretary Jeh Johnson's CIPAC Charter signature. See: https://www.dhs.gov/sites/default/files/publications/cipac-charter-11-30-16-508.pdf. 71 Fed. Reg., at 14933 (March 24, 2006).

[54] E.g., "…[C]overed entities would support the reduction of the cyber risk exposure of business assets to the enterprise *and the sector*…; and support timely responses to cyber threats to, and vulnerabilities of, the enterprise *and the financial sector*." (emphasis added) 81 Fed. Reg. at 74322, *Proposed Rules Category 3—Internal Dependency Management.*

"Covered entities would be required to prioritize monitoring, incident response, and recovery of systems critical to the enterprise *and the financial sector*; support the continued reduction of the cyber risk exposure of external dependencies to the enterprise *and the sector…*; support timely responses to cyber risks to the *enterprise and the sector*; monitor the universe of external dependencies that connect to assets supporting systems critical to the enterprise *and the sector*…." (emphasis added) 81 Fed. Reg. at 74323, *Proposed Rules Category 4—External Dependency Management.*

"…[I]n order to address the rapidly changing and complex threat landscape, the agencies are considering a requirement that covered entities continually apply and evaluate appropriate controls to reduce the cyber risk of external dependencies to the enterprise and the sector." (emphasis added) 81 Fed. Reg. at 74324, *Part IV: Sector-Critical Systems.*

Appendix B: Key Financial Sector Cyber Accomplishments and Initiative

The U.S. financial services sector has worked diligently over the past two decades to enhance cyber defenses in collaboration with U.S. Government agencies and other critical infrastructure sectors. The following are key financial sector cyber accomplishments and initiatives:

- 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 to coordinate the development of critical infrastructure strategies and initiatives with its financial services members, trade associations, and other industry sectors. The FSSCC has built and maintained relationships with the Federal Government's Financial and Banking Information Infrastructure Committee (FBIIC), which serves as the Government Coordinating Council for the Financial Services Sector and includes the U.S. Department of Treasury (Treasury) and Department of Homeland Security (DHS), all the federal financial regulatory agencies, and law enforcement agencies.
- Developed and convened 13 **"Hamilton Series"** cyber exercises in 2014 - 2016 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 at 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 eight **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 enhance resiliency and provide augmented protections for financial institutions' customer accounts and data. The focus of Sheltered Harbor is to extend the industry's capabilities to securely store and restore account data, should the need arise. Sheltered Harbor is an additional layer of protection on top of existing defenses that many financial firms utilize. It is one of a series of proactive initiatives undertaken by the U.S. financial services industry to improve sector-wide resilience. The concept for Sheltered Harbor arose during a series of successful cybersecurity simulation exercises between public and private sectors and known as the "Hamilton Series."
- 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 (February 2013).
- 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.

APPENDIX C. 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 individual issuance. Rather, this catalogue intends to illustrate the complexity of the cyber landscape for financial services companies.

For a list of statutory and regulatory requirements that predate the NIST Framework and which apply solely to banking firms, please refer to the FSSCC's September 21, 2015, submission on the "FFIEC Cybersecurity Assessment Tool,"[55] as well as the Center for Strategic and International Studies' (CSIS) July 2015 report, *The Evolution of Cybersecurity Requirements for the U.S. Financial Industry*.[56]

Regulatory Requirements, Issuances, and Proposals Affecting Financial Institutions' Cybersecurity Programs Directly

	Issuing Org	Date	Description
1	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
2	NYDFS	12/28/2016	Once updated cybersecurity regulatory requirements proposal, entitled, "Cybersecurity Requirements for Financial Services Companies," 23 NYCRR 500 http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf
3	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

[55] 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

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

	Issuing Org	Date	Description
4	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
5	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
6	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
7	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
8	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
9	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
10	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_informtion.pdf

	Issuing Org	Date	Description
11	NAIC	8/17/2016	Issuance of proposed "Insurance Data Security Model Law," Version 2. 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/committees_ex_cybersecurity_tf_exposure_mod_draft_clean.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	MA	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
20	TX	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

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 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

	Issuing Org	Date	Description
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

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
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

	Issuing Org	Date	Description
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