Testimony of

Christopher F. Feeney

On behalf of

The Financial Services Roundtable – BITS

Before the

United States Senate Committee on Homeland Security & Governmental Affairs

Hearing entitled:

"Cybersecurity Regulation Harmonization"

June 21, 2017

Chairman Johnson, Ranking Member McCaskill, and members of the Committee, thank you for the opportunity to testify before you today.

My name is Christopher F. Feeney, and I am the President of BITS, the technology policy division of the Financial Services Roundtable (FSR). BITS addresses emerging threats and opportunities facing some of the largest financial services firms, particularly those related to cybersecurity, fraud reduction, critical infrastructure protection and innovation. Working with CEOs and their C-suite executives, BITS identifies key issues at the intersection of financial services, technology and commerce, and facilitates collaboration, developing policies and practices to improve the technology environment for member companies and their customers.[1]

In addition to my role as BITS President, I am also a member of the Financial Services Sector Coordinating Council's (FSSCC) Executive Committee and Co-chair of the Policy Committee. The mission of the FSSCC is to strengthen the resiliency of the financial services sector against attacks and other threats to the nation's critical infrastructure by proactively identifying threats and promoting protection, driving preparedness, collaborating with the U. S. Federal government, and coordinating crisis response for the benefit of the Financial Services sector, consumers and the nation.[2] I also hold leadership positions in several other industry organizations focused on addressing the security and resiliency of financial institutions.

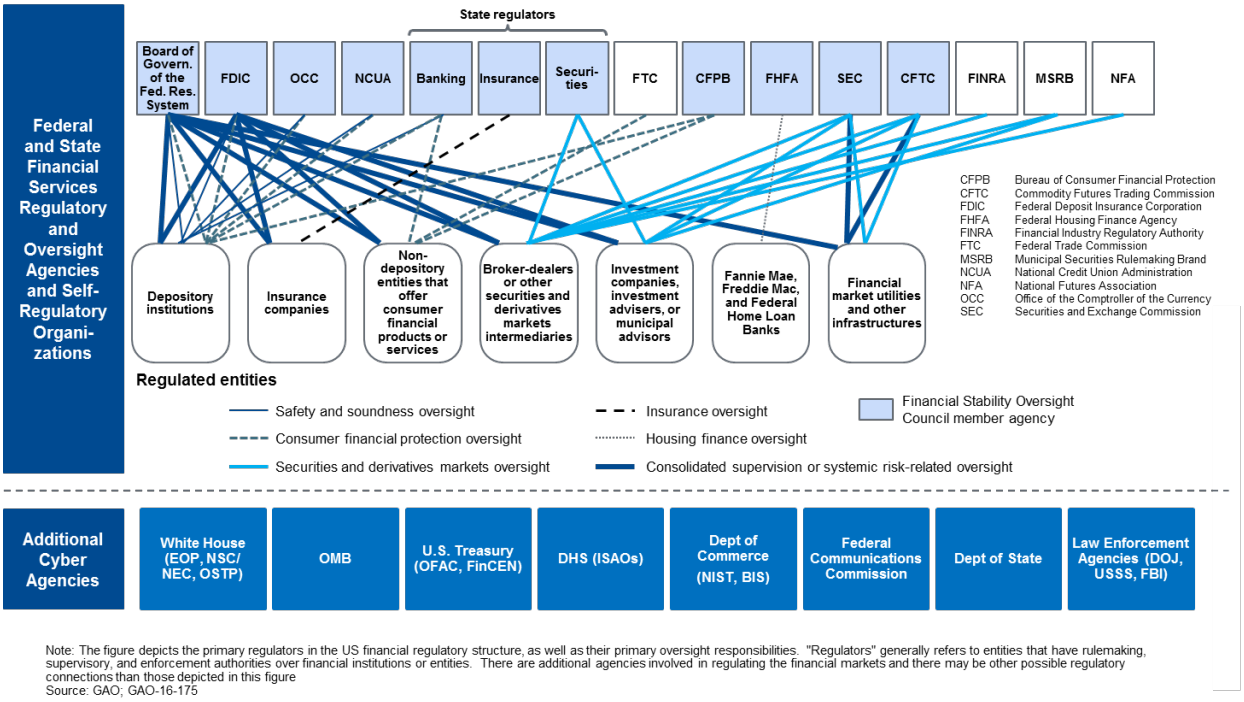
In these roles, my charge is to advance policies to protect the nation's financial infrastructure, firms' infrastructure and, most importantly, the consumers that use and depend on these financial systems every day. On behalf of our member firms, I offer the following testimony regarding the challenging cybersecurity regulatory environment, its potential impact on the security of our nation's critical infrastructure, and the financial sector's efforts to work collaboratively with regulators and across our government.

A. Overview of the Financial Services Sector

The financial services sector consists of more than 13,000 banks and credit unions, payment companies, insurance companies, wealth and asset managers and financial market utilities that process transactions, payments and move money across domestic and international markets.

The sector is overseen by nine federal regulators (all of which are independent from the executive branch), three self-regulatory organizations, The U.S. Department of the Treasury (Treasury) as its sector-specific agency,[3] and every state banking, insurance, and securities agency. When agencies tasked with cybersecurity-related authorities are added, the list expands even further (see Figure 1).

[1] For more information, please visit: http://www.fsroundtable.org/
[2] For more information, please visit: https://www.fsscc.org/
[3] For more information, please visit: https://www.dhs.gov/financial-services-sector



Note: The figure depicts the primary regulators in the US financial regulatory structure, as well as their primary oversight responsibilities. "Regulators" generally refers to entities that have rulemaking, supervisory, and enforcement authorities over financial institutions or entities. There are additional agencies involved in regulating the financial markets and there may be other possible regulatory connections than those depicted in this figure
Source: GAO; GAO-16-175

(Figure 1. The United States Financial Services Regulatory Structure in 2017 as It Relates to Cybersecurity)[4]

Cybersecurity is a top priority for our member firms. It is a key concern and focus area for CEOs and Boards of Directors, all the way to the frontline defenders sitting at keyboards monitoring network activity. Firms' senior management have made clear that cybersecurity risk is not solely a technology issue, but an enterprise-wide risk that should be considered across all levels of the organization. As such, cybersecurity is a regular agenda item at Board of Directors meetings, often with the Chief Information Security Officer or equivalent providing updates on threats, risks, and strategies for mitigation. With this senior-level support, firms have sharpened priorities and their commitment to cybersecurity.

According to a report published by Homeland Security Research Corp., the financial services cybersecurity market in the United States reached an estimated $9.5 billion in 2016, making it the largest non-government cybersecurity market.[5] Of that number, the top four U.S. banks spent nearly $1.5 billion.[6] In addition, other reports

[4] Figure reproduced from the FSSCC and BCG Platinion May 17, 2017 presentation at the NIST Cybersecurity Workshop event: https://www.nist.gov/sites/default/files/documents/2017/05/18/financial_services_csf.pdf
[5] See: http://homelandsecurityresearch.com/2014/10/u-s-banking-financial-services-retail-payment-cybersecurity-market-2015-2020/
[6] 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

indicate that 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."[7]

Recognizing that cybersecurity affects the entire industry, financial firms also have a long history of significant investment and collaboration to improve cybersecurity preparedness, response and resiliency across the sector. For example, prior to the passage of the Homeland Security Act of 2002 and the Cybersecurity Act of 2015, the financial services sector established the cyber threat information sharing and analysis center known as the FS-ISAC – a gold standard for critical infrastructure cyber threat information sharing organizations.

In addition, as a CEO-level organization, the Financial Services Roundtable-BITS has facilitated nine semi-annual CEO-led "Joint Financial Associations Cybersecurity Summits." These summits bring together financial institution CEOs, trade association CEOs, and key Congressional and government agency leaders to actively address sector resiliency, respond to capability gaps, and encourage coordination and investment. Other sector-wide activities include the "Hamilton Series" of cybersecurity response exercises; the establishment of a not-for-profit organization – Sheltered Harbor – that has developed standards for the safe storage and restoration of financial account data in the event of a catastrophic cyber incident; fTLD Registry Services, a secure website domain for banking and insurance companies; and updates and testing of the sector's cyber response plans, including the "All-Hazards Crisis Response Playbook," which provide guidance on intra-sector and government coordination in the event of a cyber incident.

Much of this collaborative work includes regulators, and our government partners at the Treasury and Department of Homeland Security (DHS). Under the DHS National Infrastructure Protection Plan, Treasury is our sector-specific agency and helps organize regular meetings of the FSSCC along with our government counterparts, referred to as the Financial and Banking Information Infrastructure Committee (FBIIC). These meetings help our industry, our regulators and our government partners work collaboratively to improve resiliency and the policies that enable it.

B. Cybersecurity Regulatory Overlap

Industry and regulators share the same goal: To ensure the financial services sector is strong, safe and secure. We support regulators' attention to the critical issue of cybersecurity; however, as recently noted by the Treasury, there is growing duplication and overlap in financial cybersecurity regulations and a need to better harmonize efforts among regulators.[8] We have requested regulators' collaborate more closely among themselves and with industry to ensure that the multitude of layered requirements does not detract from firms' ability to perform critical security work.

---

[7] See: https://go.kaspersky.com/rs/802-IJN-240/images/Financial_Survey_Report_eng_final.pdf.

[8] See: https://www.treasury.gov/press-center/press-releases/Documents/A%20Financial%20System.pdf

Since the publication of the National Institute of Science and Technology's (NIST) Cybersecurity Framework in 2014 – which was intended to provide a common way of identifying and addressing cyber risks – we have tracked the issuance of nearly 30 new or proposed cybersecurity rules, guidelines, tools or frameworks that directly affect firms. [9] While regulators may have different statutory authorities and areas of specific focus, much of the information they seek from firms is common.

Some of these new cybersecurity proposals incorporate the NIST Cybersecurity Framework's organizational structure and terminology, but many do not, instead opting for novel approaches and different language. The lack of harmonization and alignment causes firms to expend substantial personnel and resources reconciling notionally similar, but semantically different cybersecurity proposals and agency expectations.

This unnecessary duplication has been a growing concern of our member firms because it diverts the attention of cybersecurity professionals away from keeping up with dynamic cyber threats and implementing new protective measures, to instead focus on comparing and answering compliance questionnaires.

For example, one firm's Chief Information Security Officer estimated that 40% of his time and that of his team was devoted to reconciling various requirements of regulatory agencies. Due to one framework issuance in particular, the reconciliation process delayed the implementation of a security event monitoring tool intended to better detect and respond to cyber-attacks by 3-6 months. Choices like these are made by firms every day as they work to respond to changes in cyber issuances. Each new issuance requires them to develop or modify operating procedures and reporting to properly respond to examination requests, while also keeping their customers and our financial systems secure.

This challenge is compounded by the shortage of cybersecurity professionals. According to the 2015 (ISC)[2] "Global Information Security Workforce Study," the estimated 2017 shortfall of cybersecurity professionals in the Americas will be 389,000; for 2018, it increases to 516,000.[10] Our member institutions report similarly: One FSR member firm stated that as of last month, it had over 40 open positions related to cybersecurity that it was struggling to fill. This trend is expected to continue, with the global shortfall reaching 1.8 million positions by 2022.[11]

C. Enhancing Alignment to the NIST Cybersecurity Framework

Over the last two years, we have had numerous discussions within our industry and with regulators about a possible solution to the growing overlap and complexity of

[9] See Appendix A table 1, plus tables 2 and 3 for additional cybersecurity-related issuances.
[10] See: https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)%C2%B2-GlobalInformation-Security-Workforce-Study-2015.pdf.
[11] See: http://blog.isc2.org/isc2_blog/2017/02/cybersecurity-workforce-gap.html

cybersecurity requirements. We believe harmonization can be achieved based on the NIST Cybersecurity Framework. Doing so would provide a number of benefits to industry and regulators, and help foster collaboration with other critical infrastructure sectors, such as energy and telecommunications.

The NIST Cybersecurity Framework was developed through a transparent multi-stakeholder process and produced a cybersecurity risk management framework for critical infrastructure based on international standards and best practices. Federal and state agencies, sector-representative organizations and individual private sector entities from across the country participated. The financial services sector was a key contributor throughout the process.

From that collaborative endeavor, NIST issued the "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0"[12] (NIST Cybersecurity Framework) in February 2014. In passing the Cybersecurity Enhancement Act that same year, Congress codified its approval of the Framework, the process used to develop it, and NIST's role in its evolution. Perhaps because of NIST's multi-stakeholder development process and the Framework's accessibility from the control room to the boardroom, firms began to quickly integrate the NIST Cybersecurity Framework into their information security programs. By late 2015, PwC reported that approximately 91% of companies it surveyed were using either the NIST Cybersecurity Framework or ISO standard.[13] Certain sectors and subsectors, such as telecommunications,[14] electricity,[15] manufacturing,[16] and the maritime bulk liquids transfer subsector[17] worked with either NIST, their sector-specific agencies, regulatory agencies, or some combination thereof to harmonize existing and proposed assessment or regulatory regimes around the NIST Cybersecurity Framework.

As financial sector agencies have issued cybersecurity proposals that use new terminology and methodologies, many firms spend countless hours trying to align their internal processes to the new requirements. To assist financial institutions in the reconciliation process, the FSSCC began mapping a select set of cyber regulations and regulatory proposals against the NIST Cybersecurity Framework. This effort took several months, and once completed, the mapping document was uploaded to a data visualization and analysis tool. The resulting graphic illustrates the complexity in

---

[12] See: https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[13] PwC. "Global State of Information Security Survey 2016." 9 October 2015: http://www.pwc.com/gx/en/issues/cyber-security /information-security-survey.html.

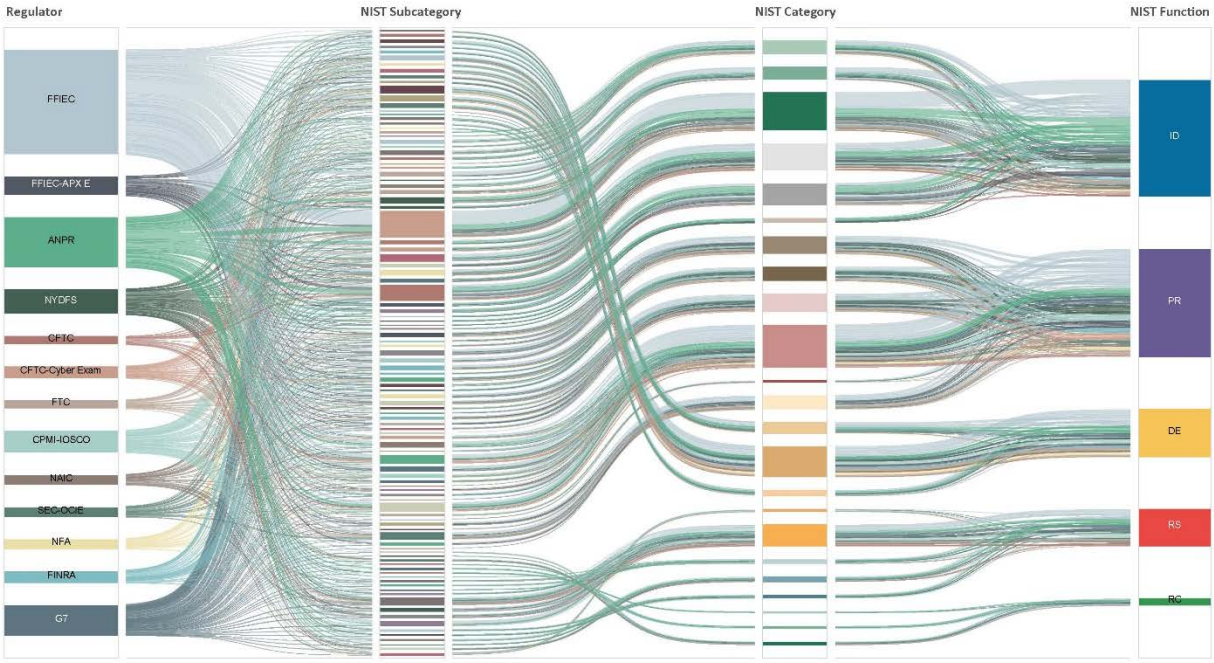
[14] See: https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

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

[16] See: http://csrc.nist.gov/cyberframework/documents/Manufacturing-Profile-DRAFT.pdf.

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

reconciling a subset of select proposals against the NIST Cybersecurity Framework (see Figure 3).



(Figure 3. Complexity in Reconciling Select Proposals to the NIST CSF)

The current fragmented approach introduces inefficiencies by requiring institutions to identify, draft, and compile functionally equivalent sets of data from the same systems to satisfy each different regulator and each different regulatory standard. As a result, institutions are forced to create single-use compliance data, rather than focusing their time on developing security and mitigation techniques that improve a firm's cybersecurity program. While each agency proposal or set of requirements may have its own merit, when continuously layered, the added complexity is unsustainable as there are simply not enough cybersecurity professionals available to perform the necessary work. One example of the complexity of cyber regulations is captured in Appendix B, which summarizes the differing expectations adopted by multiple regulators to address the common practice of penetration testing.

The lack of harmonization also complicates efforts to coordinate across critical infrastructure sectors and with the federal government for cyber incident response. A key focus for the federal government and DHS, in particular, has been to foster a "whole of nation" approach to cybersecurity. This effort to foster greater public-private partnership is critical if we are to effectively protect our economy, our customers, and our citizens from cyber threats. As regulations pull financial institutions away from using NIST, this could endanger not only our sector, but other critical infrastructure sectors if a coordinated response is needed.

D. Interactions with the Regulatory Community

The industry first suggested regulators align their efforts more closely to the NIST Cybersecurity Framework in a September 21, 2015 submission[18] to the Federal Financial Institutions Examination Council, a coordinative body for the banking-specific agencies and organizations.[19] This suggestion included a request that regulators work collaboratively with industry to find a solution that would allow regulators to fulfill their responsibilities while better allowing firms to focus on critical cybersecurity activities.

In October 2016, industry (through the FSSCC) and our government coordinating council, the FBIIC, agreed to a joint working group to discuss opportunities to better harmonize cybersecurity related requirements and expectations. The FSSCC had hoped to begin an ongoing and constructive dialogue immediately but the regulatory community requested additional time to organize and prepare for these discussions.

In the interim, industry undertook the mapping project discussed above. In late February of this year, the FSSCC began customizing the NIST Cybersecurity Framework for the financial sector by incorporating key focus areas and priorities of our regulators. This effort is referred to as the "Financial Services Sector Specific Cybersecurity Profile" and is designed to help demonstrate how alignment to the NIST Framework could be used to meet the needs of regulators, assist firms in reducing the compliance burden and satisfy market-specific requirements. This customized profile, along with a proposed set of common examination questions, is intended to help generate discussion with the regulatory community.

In May of this year, the FSSCC previewed draft portions of this NIST customization with a number of financial services regulatory agencies and with the larger cybersecurity community at the NIST Cybersecurity Framework workshop on May 16-17. The draft was well-received by NIST, the private sector, and financial services agency representatives in attendance. Coming out of the meeting, interest in collaboration around this working draft and the proposed common set of examination questions was renewed.

---

[18] See: https://www.fsscc.org/files/galleries/FSSCC_FFIEC_Cybersecurity_Assessment_Comment_Letter_(FR_2015-17907).pdf.

[19] For more information on the FFIEC, including its membership and statutory authorities, please see: https://www.ffiec.gov/. Chaired by the U.S. Department of Treasury's Assistant Secretary for Financial Institutions, members include representatives from the 2) American Council of State Savings Supervisors, 3) Commodity Futures Trading Commission, 4) Conference of State Bank Supervisors, 5) Consumer Financial Protection Bureau, 6) Farm Credit Administration, 7) Federal Deposit Insurance Corporation, 8) Federal Housing Finance Agency, 9) Federal Reserve Bank of Chicago, 10) Federal Reserve Bank of New York, 11) Federal Reserve Board, 12) National Association of Insurance Commissioners, 13) National Association of State Credit Union Supervisors, 14) National Credit Union Administration, 15) North American Securities Administrators Association, 16) Office of the Comptroller of the Currency, 17) Securities and Exchange Commission, and 18) Securities Investor Protection Corporation.

From those interactions, FSSCC learned that under Treasury's leadership, the FBIIC established a cybersecurity harmonization working group. Additionally, Treasury signaled its support and approval of this approach in its recently released report to the President of the United States – "Core Principles for Regulating the United States Financial System."[20] In the report, they recommended greater coordination in two respects: "First, financial regulatory agencies should work to harmonize regulations, including using a common lexicon. Second, financial regulators should work to harmonize interpretations and implementation of specific rules and guidance around cybersecurity."[21] To achieve this, Treasury recommended FBIIC as the coordinative body. The FSSCC supports these recommendations.

E. The Sector's Congressional Requests

Congress has an important role to play in encouraging the agencies to meet with the private sector and coordinate amongst themselves to achieve regulatory harmonization. A multi-stakeholder process of agencies and private sector representatives, similar to the one employed by NIST, is necessary for success.

To foster this collaboration, we encourage this Committee to recommend that agencies pause any in-process cybersecurity related proposals, rulemakings, or other formal activities to allow time for effective collaboration. There are several agency cybersecurity initiatives that if completed and issued[22] would further complicate an already complex regulatory environment.

F. Conclusion

The financial services sector shares the same cybersecurity-related goals as our regulatory community: Advancing the safety, soundness, and resilience of the financial system by protecting financial institutions and the financial sector from increasing cybersecurity risks. Given the complexity of our regulatory environment, a lack of harmonization negatively impacts the ability of financial institutions to devote resources to security activities.

This is only exacerbated by the shortage of cybersecurity professionals, and we hope that all would agree the experts that are available should be able to devote more time to security rather than interpreting notionally similar, but semantically different regulatory expectations.

---

[20] See, p.31: https://www.treasury.gov/press-center/press-releases/Documents/A%20Financial%20System.pdf

[21] See, p.31 and Appendix B, p.123: https://www.treasury.gov/press-center/press-releases/Documents/A%20Financial%20System.pdf

[22] E.g. the advancement of the jointly issued Federal Reserve System-Office of the Comptroller of the Currency-Federal Deposit Insurance Corporation advanced notice of proposed rulemaking on proposed "Enhanced Cyber Risk Management Standards" to the notice of proposed rulemaking stage, a substantial revision of the FFIEC issued Cybersecurity Assessment Tool, and the completion of a National Association of Insurance Commissioners authored "Cybersecurity Model Law"

As discussed, there is a solution: The sector-specific "Profile," if adopted, would provide the harmonized and rationalized approach to cybersecurity regulation our sector needs. We request that you recommend to agencies to pause further cyber-related issuances while the "Profile" is being considered.

We stand ready to work with our regulatory community on this more rationalized approach, and we ask for your public encouragement. It is needed.

Thank you.

Appendix A

Cybersecurity-related Regulations, Requirements, Examination Expectations, and Other Initiatives Affecting Financial Institutions since the release of the NIST Cybersecurity Framework, Version 1.0 in February 2014.

The following tables illustrate the complexity of the cyber regulatory landscape for financial services firms and include rules, guidance, tools and recommendations since the release of the NIST Cybersecurity Framework, version 1.0 in February 2014. These lists are not exhaustive, and inclusion does not represent a judgment of the relative benefits or burdens of each singular issuance.

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,"[23] as well as the Center for Strategic and International Studies' (CSIS) July 2015 report, entitled, "The Evolution of Cybersecurity Requirements for the U.S. Financial Industry"[24].

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

	Issuing Org	Date	Description
1	DE	5/16/ 2017	House Bill 180 would expand data breach notification law to include requirement that those "conducting business" in Delaware must "implement and maintain reasonable procedures and practices to prevent the unauthorized access to or acquisition, use, modification, disclosure, or destruction of personal information collected or maintained in the regular course of business. " http://legis.delaware.gov/BillDetail?legislationId=25794
2	NV	3/20 /2017	Senate Bill 395 would require cybersecurity plans for all critical infrastructure in the state. https://legiscan.com/NV/text/SB395/2017

[23] 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

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

	Issuing Org	Date	Description
3	CO	3/6/2017	Notice of Proposed Rulemaking of the Colorado Division of Securities; proposed rules include "guidance to broker-dealers and investment advisers on what factors the Division will consider when determining if the procedures by the firm are reasonably designed to ensure cybersecurity." https://drive.google.com/file/d/0BymCt_FLs-RGUWI5c3lDUVlzeDg/view
4	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
5	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.
6	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
7	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
8	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.

	Issuing Org	Date	Description
			https://www.federalregister.gov/documents/2016/10/26/2016-25871/enhanced-cyber-risk-management-standards
9	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
10	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
11	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
12	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
13	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
14	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

	Issuing Org	Date	Description
			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
15	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
16	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
17	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
18	CFTC	12/23/2015	*Federal Register* notice of proposed rulemaking, "System Safeguards Testing Requirements." http://www.cftc.gov/LawRegulation/FederalRegister/ProposedRules/2015-32143
19	FFIEC	11/10/2015	Revised "IT Examination Handbook: Management Booklet" issued. http://ithandbook.ffiec.gov/it-booklets/management.aspx
20	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

	Issuing Org	Date	Description
21	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
22	Mass.	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
23	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
24	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
25	FFIEC	6/30/2015	FFIEC Cybersecurity Assessment Tool https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_June_2015_PDF2.pdf
26	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
27	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

	Issuing Org	Date	Description
28	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
29	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
30	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
31	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

	Issuing Org	Date	Description
			regulators. https://www.swift.com/myswift/customer-security-programme-csp_#topic-tabs-menu
32	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
33	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
34	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
35	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
36	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
37	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
38	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
39	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
40	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
41	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

	Issuing Org	Date	Description
42	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
43	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
44	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
45	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
46	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 B

Penetration Testing – Non-Exhaustive

As an example of the overlap among financial services cybersecurity related requirements, below is a sample of existing guidelines and expectations regarding a component of vulnerability management: penetration testing. Penetration testing is used to determine how an adversary may infiltrate a firm's information systems. Once known, firms work to close the system gaps exposed by the testing.

I. Voluntary Guidance

1. National Institute of Standards and Technology
   NIST Cybersecurity Framework
   https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

   NIST Protect Function, Information Protection Processes and Procedures Category, Subcategory: A vulnerability management plan is developed and implemented

2. *Federal Financial Institutions Examination Council (FFIEC)*
   Cybersecurity Assessment Tool
   https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017.pdf

Cybersecurity Maturity Domain	Assessment Factor	Component	Maturity Level	Mapping Number	Declarative Statement
3: Cybersecurity Controls	3: Corrective Controls	2: Remediation	Evolving	D3.CC.Re.E.2	Formal processes are in place to resolve weaknesses identified during penetration testing.
3: Cybersecurity Controls	3: Corrective Controls	2: Remediation	Advanced	D3.CC.Re.A.1	All medium and high risk issues identified in penetration testing, vulnerability scanning, and other independent testing are escalated to the board or an appropriate board committee for risk acceptance if not resolved in a timely manner.

3: Cybersecurity Controls	2: Detective Controls	1: Threat and Vulnerability Detection	Baseline	D3.DC.Th.B.1	Independent testing (including penetration testing and vulnerability scanning) is conducted according to the risk assessment for external-facing systems and the internal network. (FFIEC Information Security Booklet, page 61)
3: Cybersecurity Controls	2: Detective Controls	1: Threat and Vulnerability Detection	Evolving	D3.DC.Th.E.1	Independent penetration testing of network boundary and critical Web-facing applications is performed routinely to identify security control gaps.
3: Cybersecurity Controls	2: Detective Controls	1: Threat and Vulnerability Detection	Intermediate	D3.DC.Th.Int.1	Audit or risk management resources review the penetration testing scope and results to help determine the need for rotating companies based on the quality of the work.

II. Agency Expressed Requirements and Expectations

1. ***New York Department of Financial Services (NYDFS) (a State-based regulator)***
   23 NYCRR 500 - Cybersecurity Requirements for Financial Services Companies
   http://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf

   Section 500.05 Penetration Testing and Vulnerability Assessments.
   The cybersecurity program for each Covered Entity shall include monitoring and testing, developed in accordance with the Covered Entity's Risk Assessment, designed to assess the effectiveness of the Covered Entity's cybersecurity program. The monitoring and testing shall include continuous monitoring or periodic Penetration Testing and vulnerability assessments. Absent effective continuous monitoring, or other systems to detect, on an ongoing basis, changes in Information Systems that may create or indicate vulnerabilities, Covered Entities shall conduct:

(a) annual Penetration Testing of the Covered Entity's Information Systems determined each given year based on relevant identified risks in accordance with the Risk Assessment; and

(b) bi-annual vulnerability assessments, including any systematic scans or reviews of Information Systems reasonably designed to identify publicly known cybersecurity vulnerabilities in the Covered Entity's Information Systems based on the Risk Assessment.

2. *National Futures Association (NFA)*
9070 - NFA COMPLIANCE RULES 2-9, 2-36 AND 2-49: INFORMATION SYSTEMS SECURITY PROGRAMS
http://www.nfa.futures.org/nfamanual/NFAManual.aspx?RuleID=9070&Section=9

Review of Information Security Programs.
Members should monitor and regularly review the effectiveness of their ISSPs, including the efficacy of the safeguards deployed, and make adjustments as appropriate. A Member should perform a regular review of its ISSP at least once every twelve months using either in-house staff with appropriate knowledge or by engaging an independent third-party information security specialist. Under appropriate circumstances, a Member's review may include penetration testing of the firm's systems, the scope and timing of which is highly dependent upon the Member's size, business, technology, its electronic interconnectivity with other entities and the potential threats identified in its risk assessment.

3. *Commodity Futures Trading Commission (CFTC)*
System Safeguards Rule - 17 CFR 37.1401
https://www.law.cornell.edu/cfr/text/17/37.1401

(h) A swap execution facility shall conduct regular, periodic, objective testing and review of its automated systems to ensure that they are reliable, secure, and have adequate scalable capacity. It shall also conduct regular, periodic testing and review of its business continuity-disaster recovery capabilities. Such testing and review shall include, without limitation, all of the types of testing set forth in paragraph (h) of this section.

(3) *External penetration testing.* A swap execution facility shall conduct external penetration testing of a scope sufficient to satisfy the requirements set forth in paragraph (k) of this section.
(i) A swap execution facility shall conduct such external penetration testing at a frequency determined by an appropriate risk analysis.

(ii) A swap execution facility shall conduct external penetration testing by engaging independent contractors or by using employees of the swap execution facility who are not responsible for development or operation of the systems or capabilities being tested.

(4) *Internal penetration testing.* A swap execution facility shall conduct internal penetration testing of a scope sufficient to satisfy the requirements set forth in paragraph (k) of this section.

(i) A swap execution facility shall conduct such internal penetration testing at a frequency determined by an appropriate risk analysis.

(ii) A swap execution facility shall conduct internal penetration testing by engaging independent contractors, or by using employees of the swap execution facility who are not responsible for development or operation of the systems or capabilities being tested.

(k) *Scope of testing and assessment.* The scope for all system safeguards testing and assessment required by this part shall be broad enough to include the testing of automated systems and controls that the swap execution facility's required program of risk analysis and oversight and its current cybersecurity threat analysis indicate is necessary to identify risks and vulnerabilities that could enable an intruder or unauthorized user or insider to:

(1) Interfere with the swap execution facility's operations or with fulfillment of its statutory and regulatory responsibilities;

(2) Impair or degrade the reliability, security, or adequate scalable capacity of the swap execution facility's automated systems;

(3) Add to, delete, modify, exfiltrate, or compromise the integrity of any data related to the swap execution facility's regulated activities; or

(4) Undertake any other unauthorized action affecting the swap execution facility's regulated activities or the hardware or software used in connection with those activities.

4. *Securities and Exchange Commission Office of Compliance Inspection and Examination*

OCIE's 2015 Cybersecurity Examination Initiative
https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf

APPENDIX

This document provides a sample list of information that the U.S. Securities and Exchange Commission's Office of Compliance Inspections and Examinations ("OCIE") may review in conducting examinations of registered entities regarding cybersecurity matters. Some of the questions track information outlined in the "Framework for Improving Critical Infrastructure

Cybersecurity," 2 released on February 12, 2014 by the National Institute of Standards and Technology. OCIE has published this document as a resource for registered entities. This document should not be considered all-inclusive of the information that OCIE may review or the validation and testing we may perform of firm policies and procedures. Accordingly, OCIE will alter its requests for information it reviews, as well as whether it asks for production of information in advance of an examination or reviews certain information on site, as it considers the specific circumstances presented by each firm's business model, systems, and information technology environment.

Governance and Risk Assessment

• Information regarding the firm's policies related to penetration testing, whether conducted by or on behalf of the firm, and any related findings and responsive remediation efforts taken.

5. *Federal Financial Institutions Examination Council (FFIEC)*
FFIEC IT Examination Handbook, Information Security Booklet
https://ithandbook.ffiec.gov/it-booklets/information-security/iv-information-security-program-effectiveness/iva-assurance-and-testing/iva2-types-of-tests-and-evaluations/iva2(b)-penetration-tests.aspx

IV.A.2(b) Penetration Tests
A penetration test subjects a system to real-world attacks selected and conducted by the testers. A penetration test targets systems and users to identify weaknesses in business processes and technical controls. The test mimics a threat source's search for and exploitation of vulnerabilities to demonstrate a potential for loss. Some tests focus on only a subset of the institution's systems and may not accurately simulate a determined threat actor. There are many types of penetration tests (e.g., network, client-side, web application, and social engineering), and management should determine the level and types of tests employed to ensure effective and comprehensive coverage.

The frequency and scope of a penetration test should be a function of the level of assurance needed by the institution and determined by the risk assessment process. The test can be performed internally by independent groups, internally by the organizational unit, or by an independent third party. Management should determine the level of independence required of the test.

6. *Federal Financial Institutions Examination Council (FFIEC)*
FFIEC IT Examination Handbook, E-Banking Booklet

http://ithandbook.ffiec.gov/it-booklets/e-banking/risk-management-of-e-banking-activities/information-security-program/information-security-controls.aspx

Information Security Controls

Security threats can affect a financial institution through numerous vulnerabilities. No single control or security device can adequately protect a system connected to a public network. Effective information security comes only from establishing layers of various control, monitoring, and testing methods. While the details of any control and the effectiveness of risk mitigation depend on many factors, in general, each financial institution with external connectivity should ensure the following controls exist internally or at their TSP [Third Party Service Provider].

- *Independent testing*. Financial institutions should have a testing plan that identifies control objectives; schedules tests of the controls used to meet those objectives; ensures prompt corrective action where deficiencies are identified; and provides independent assurance for compliance with security policies. Security tests are necessary to identify control deficiencies. An effective testing plan identifies the key controls, then tests those controls at a frequency based on the risk that the control is not functioning. Security testing should include independent tests conducted by personnel without direct responsibility for security administration. Adverse test results indicate a control is not functioning and cannot be relied upon. Follow-up can include correction of the specific control, as well as a search for, and correction of, a root cause. Types of tests include audits, security assessments, vulnerability scans, and penetration tests.