February 9, 2016

Via Electronic Submission to cyberframework@nist.gov

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

RE: Views on the *Framework for Improving Critical Infrastructure Security*

Dear Ms. Honeycutt:

The Financial Services Sector Coordinating Council ("the FSSCC")[1] appreciates the opportunity to provide comments in response to the notice and request for information published in the *Federal Register*, Vol. 80, No. 238, on December 11, 2015, by the National Institute of Standards and Technology ("NIST") regarding views on the *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0* (the "*Cybersecurity Framework*" or "the *Framework*").

To develop comments for this submission, the FSSCC used a broad-based, cross-industry collaborative process that included participation from institutions of all sizes and views from the front-line cybersecurity control implementers to the Chief Information Security Officers and the C-Suite, including Chief Executive Officers.

The FSSCC supports the Administration, NIST and Congress in their efforts to foster an open, inclusive and collaborative process for the development of a common cybersecurity taxonomy and framework. These efforts have created the *Cybersecurity Framework*, which is a common, consistent standard by which U.S. companies organize cybersecurity risk management and assess their cybersecurity posture. At the same time, financial services regulatory bodies have begun to diverge from the *Framework*, which will be an impediment to the sector's continued use. NIST can play a vital role to foster continued use of the *Framework* by the financial services and other sectors by facilitating the harmonization of these regulatory efforts with the *Framework* to the greatest extent possible.

Additionally, while adoption has been impressive across sectors, many firms are in the early stages of fully integrating the *Framework* into their cybersecurity governance. Accordingly, the FSSCC believes future revisions should be accomplished incrementally,

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

perhaps on a biennial cycle. As such, NIST should maintain its current role of fostering continued use of the *Framework*, and incremental revisions in the near term.

Finally, to foster advancement of cybersecurity risk management programs through the sharing of lessons learned and *Framework* usage best practices, the U.S. government should promote trusted forums for such exchanges.

I. Financial Services Industry Supports the Goals of the Administration, NIST and Congress of a Common Taxonomy and Cybersecurity Framework and NIST's Open, Collaborative and Cross-Sector Approach.

The FSSCC applauds the open and transparent process directed by Congress and the Administration and used by NIST in creating and seeking to refine the *Cybersecurity Framework*. The financial services sector has found value in this public-private partnership and interagency collaboration and, while voluntary, encourages its use across sectors and regulatory bodies in addressing cyber risks.

The financial services industry, as a sector, is a leader in cybersecurity. At the same time, the sector fully recognizes that it exists within a larger ecosystem with entities that provide other critical infrastructure services such as power, water, telecommunications, and computing. In order to address shared cyber risks and interdependencies, the NIST *Cybersecurity Framework's* common taxonomy and common approach is crucial. As such, to further enhance the NIST *Cybersecurity Framework* and foster its use across the nation's critical infrastructure, the financial services sector requests that NIST maintain its oversight and care of the *Cybersecurity Framework* in the near-term for the next several revision cycles.

II. The NIST *Cybersecurity Framework* is the Common Cybersecurity Framework of U.S. Companies.

According to PwC's recent "Global State of Information Security Survey for 2016," 91% of companies surveyed either use the current NIST *Cybersecurity Framework*, or the ISO standards for cybersecurity risk management.[2] The Office of Financial Research remarked in its 2015 Financial Stability Report that "…the NIST *Cybersecurity Framework* is emerging as a de facto standard for firms seeking guidance in their efforts to counter cyber threats."[3] These findings echo the sector's experiences.

At the individual level, financial services firms continue to report substantial investment of energy and resources in educating board members on the NIST *Cybersecurity Framework*, and, where appropriate, have adjusted reports, documents and other communications. Additionally, media coverage of the NIST *Cybersecurity Framework*, its endorsement by the

---

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

[3] U.S. Department of the Treasury, Office of Financial Research. "Financial Stability Report." 15 December 2015. https://financialresearch.gov/financial-stability-reports/files/OFR_2015-Financial-Stability-Report_12-15-2015.pdf.

National Association of Corporate Directors, and the proliferation of outside materials and ongoing board educational sessions hosted by third party audit firms have created awareness and reinforced reliance on the Framework and its role in cross sector cyber resilience.[4] Firms also continue to reiterate that the value of the NIST *Cybersecurity Framework* is its common vocabulary, which assists firms in describing cyber activities in an accessible manner, conducting an initial assessment of cyber capabilities and gaps, and providing a roadmap to address identified gaps or residual risk. An essential component of the *Framework* is its Rosetta Stone-like capacity to be applicable to all sectors and map informative references across sector-specific risk management jargon, bringing common understanding of risk management terms and phrases. One firm has developed a matrix utilizing the NIST *Cybersecurity Framework* functions to categorize the cybersecurity products and services available in the marketplace and mapped them to a set of asset classes. Another firm has mapped its own internal organizational structure to the five NIST functions. By doing so, these firms have understood how to better address those specific functional security needs.

The objective-based, action-oriented NIST *Cybersecurity Framework* and its corresponding taxonomy is understood not only across firms and sectors, but also from the operations floor to the corporate boardroom. As a result, financial services firms report the *Framework* has a central role in facilitating internal and external communication. Chief Information Security Officers use it to communicate concepts and find consensus for cybersecurity initiatives. Externally, firms rely on it to communicate expectations and requirements, and to understand the cybersecurity capabilities of non-sector vendors and third parties. This is particularly true for institutions as they conduct due diligence review of third parties' cybersecurity risk and risk management programs, as may be required by regulators. Additionally, with the aid of outside consulting firms, some financial services firms use the NIST *Cybersecurity Framework* as a common reference to benchmark themselves against peers.

Upon its release, financial services firms sought to expand usage of the *Framework* by applying it to the due diligence process already in place for the review of a vendor or third party's cybersecurity program. FSSCC responded to member requests to establish a working group tasked with developing an auditable cybersecurity standard for third party risk. Due to the versatility of the *Framework*, the plan is for the standard to be used by financial services firms to satisfy both their internal and external cyber risk assessment requirements. To achieve these objectives, a 50-firm working group, started with the American Institute of CPAs (AICPA) Service Organization Control 2 (SOC2), the NIST *Cybersecurity Framework*, and the firm specific questionnaires, which are being used to facilitate third party risk assessments.[5] By taking advantage of significant overlap in similar core functional areas and applying it to some of the unique requirements of financial services, the combination is designed to better address financial sector requirements and to more readily integrate the NIST *Cybersecurity Framework* into an existing audit methodology. This Financial Services SOC2 will measure a company's service against the SOC2 criteria and the *Framework* sub-categories, providing firms that undergo it an

---

[4] National Association of Corporate Directors. "Cyber Risk Oversight." 10 June 2014. https://www.nacdonline.org/Resources/Article.cfm?ItemNumber=10688.

[5] SOC2 is the succeeding version of the SSAE 16. Further details are available here:http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/AICPASOC2Report.aspx.

attestation as to the presence and operational effectiveness of the controls that enable their cybersecurity program. The FSSCC working group expects the standard to identify and address 90% of relevant requirements within security, technology and business resiliency risk areas. The same initiative is also leveraging the Shared Assessment SIG and AUP assessment methodology with the groups' shared goal of integrating the *Framework* into a commonly used assessment method and aligning cybersecurity requirements across financial services firms and their partners and third party vendors.[6]

The sector has also leveraged the *Framework* in developing cybersecurity risk management programs associated with specific risks and threats. Shortly after the *Framework's* release, SIFMA developed an insider threat best practices guide that aligned with the *Framework* core. Using the NIST structure, the guide encourages firms to individually assess threats most relevant to their own firm and to develop a risk-based approach to resource allocation. This alignment has allowed firms to leverage policies, procedures and systems that link and overlap between cyber risk management programs and insider threat programs and has highlighted how risk management is central to both such programs. Moreover, by using the NIST *Cybersecurity Framework* taxonomy for both, the best practices guide provides a means to communicate effectively and consistently across traditionally separate enterprise areas.[7]

In addition, the sector has incorporated the NIST *Cybersecurity Framework* as the base for its sector-wide *All-Hazards Crisis Response Playbook* ("*Playbook*"). The *Playbook* puts into operation, and provides a means to mature, the NIST *Cybersecurity Framework* "respond" and "recover" controls at a critical sector level. The language of the NIST controls is identifiable in the five main *Playbook* components: Financial Sector (FS) crisis communication; FS Crisis Response Coordination; Government Crisis Response Coordination; Associations, Regional and Multi-Sector Crisis Coordination; and Sector Contingency Plans and Event Closure. This NIST alignment and the *Playbook's* succinct structure provide a higher probability of *Playbook* discussion and reference during crisis response.[8]

Additionally, the sector has begun using the NIST *Cybersecurity Framework* functions, as the criteria to evaluate not only an institution and the sector's cyber capabilities, but also the federal government's cyber assistance capabilities. The sector, in collaboration with the U.S. Government departments and agencies, including the U.S. Departments of the Treasury and Homeland Security, has begun developing a "Cyber Capability Assessment Framework" (CCAF) to capture, organize, prioritize, assess the maturity of, and test cyber and related capabilities that can be called upon collectively by members of the financial services sector to "Identify, Protect, Detect, Respond and Recover" technically and functionally from significant cyber threat activities against the sector. Because the U.S. Government has diplomatic, military,

---

[6] For additional information about the FSSCC Auditable Cybersecurity Standard initiative, please see Appendix B. For more information about Shared Assessments, its SIG, AUP, and other tools, see: https://sharedassessments.org/store/.

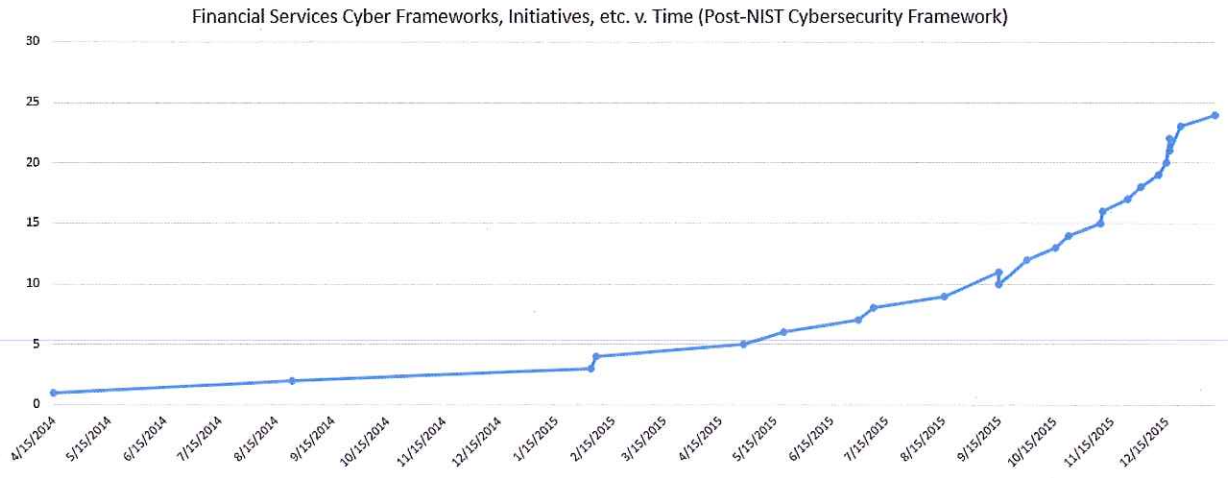
[7] For additional information or to access SIFMA's "Insider Threat Best Practices Guide," see: http://www.sifma.org/uploadedfiles/issues/technology_and_operations/cyber_security/insider-threat-best-practices-guide.pdf?n=92985

[8] For a full description of the FS-ISAC *Playbook* and NIST alignment, please see Appendix C.

economic, law enforcement and operational cyber capabilities that do not map neatly within the five NIST *Cybersecurity Framework* functional categories, the sector and its agency partners have expanded the NIST *Cybersecurity Framework* structure and taxonomy to include these capabilities under a sixth function: deterrence (or "deter"). The other five functions and corresponding categories and subcategories have also been expanded to consider and evaluate government capabilities. With completion of this expanded framework, the sector plans to map cyber capabilities to potential courses of action at the firm level. This expanded framework will also help the sector and its government partners in identifying cyber operational capabilities using a formal, structured methodology based on the commonly used NIST *Cybersecurity Framework*. Moreover, it will assist the sector and its government partners in not only assessing available cyber capabilities, but also capacity for deployment and areas for improvement. This CCAF concept has also been shared with some members of the U.S. Government Cyber Research and Development community to ensure that technologies being developed clearly map to functional cyber operational capabilities and needs.

III. Regulatory, Oversight, and Examination Agency Divergence from the NIST *Cybersecurity Framework* is an Impediment to Financial Services Entities Continued Use of It.

While the financial services industry has aligned and synchronized cybersecurity activities to the NIST *Cybersecurity Framework's* structure and taxonomy, several financial services regulatory agencies and oversight bodies are developing other non-NIST based guidance. Since the *Framework's* release, financial services agencies at the state, federal, and international level have announced, and in some cases implemented, disparate cybersecurity risk management and controls, testing and evaluation, business continuity planning and disaster recovery, and reporting and disclosure plans.[9]



Although some of these cyber initiatives incorporate the NIST *Cybersecurity Framework's* structure or taxonomy, many rely on another known framework or have developed

[9] A complete list of these can be found in Appendix D.

a new bespoke framework. The resulting lack of alignment and harmonization causes firms to expend substantial resources reconciling the NIST *Cybersecurity Framework* with unique, and often competing, examination questionnaires, frameworks, and tools now preferred by various regulatory bodies. Firms are further reporting that an increasingly complex regulatory landscape impacts the ability to contextualize key issues and appropriately evaluate the effectiveness of internal and external cybersecurity efforts. The resulting burden and complexity distracts cybersecurity professionals from identifying and protecting against the threat environment; this undermines the design of cybersecurity strategies and prioritization of control implementation. Industry has a shared concern that the fundamentals of cybersecurity are weakened when, as some firms have reported, approximately 40% of corporate cybersecurity activities are compliance oriented, rather than security oriented. The solution is not merely hiring more cybersecurity personnel as expert staff are becoming an increasingly scarce and costly resource.[10]

NIST can help mitigate some of these divergent frameworks as more fully described in Section VI of this letter. A common cybersecurity risk management taxonomy provides a tool for financial services firms to thoroughly evaluate cross-sectoral critical infrastructure entities.

IV. NIST Should Convene Each Sector, Regulatory Agencies to Encourage Harmonization with NIST *Cybersecurity Framework.*

To moderate regulatory momentum away from the NIST *Cybersecurity Framework*, NIST should convene each industry and each industry's common regulatory agencies to collaboratively pursue regulatory harmonization with the NIST *Cybersecurity Framework*. While fulfilling a needed leadership role as convener and facilitator, NIST could then also act as an advisor to encourage appropriate harmonization or analogous tools to correspond with the NIST *Cybersecurity Framework*. This effort would also fulfill the directive from the "Cybersecurity Enhancement Act of 2014" to "prevent duplication of regulatory processes and prevent conflict with or superseding of regulatory requirements, mandatory standards, and related processes."[11] Sector-specific cybersecurity requirements would be developed within a collaborative synchronization process. Using this model, a regulator would promulgate a new function, category, or subcategory for a specific sector while preserving the essential cross-sector functionality of the structure and taxonomy within the NIST *Cybersecurity Framework*. A notable benefit in harmonizing different regulatory questionnaires, frameworks, and expectations with the NIST *Cybersecurity Framework*, is that it would provide a means for both an individual firm and regulators alike to more readily evaluate the cybersecurity posture and cyber risk management programs of non-sector, third parties. It would be less likely that potential areas for

---

[10] According to the 2015 (ISC)2 "Global Information Security Workforce Study," the projected shortfall in cybersecurity professionals is expected to be 621,000 people worldwide in 2016 alone (271,000 people for the Americas). This shortfall is only expected to grow in the coming years. For 2017, the projected cyber talent shortfall is expected to be 901,000 people worldwide (389,000 people for the Americas). This shortfall grows to 1,172,000 people worldwide in 2018 (516,000 people for the Americas) and 1,536,000 people worldwide in 2019 (649,000 people for the Americas). See also, *NIST Roadmap for Improving Critical Infrastructure*, section 4.4 "Cybersecurity Workforce," which also acknowledges the workforce shortage.

[11] Public Law 113-274. 128 Stat. 2971.

concern would be clouded by sector-specific jargon or lost in a translation from one sector's cyber risk lexicon to another.

In sum, this harmonization process would preserve regulatory objectives and independence, and also strengthen our nation's security by focusing on areas of greatest risk to a particular sector while facilitating the cross-sector coordination crucial for cyber risk identification, mitigation, and incident response.

V. Biennial Updates to NIST *Cybersecurity Framework* Enhance Value as Common Cybersecurity Risk Management Tool.

Uptake of the *Framework, Version 1.0,* has been significant across sectors.[12] It has been quickly integrated into cybersecurity planning, budgeting, strategic planning, and, in some cases, even departmental reorganization. This adoption rate is largely unprecedented and many firms continue to incorporate the current version within their cybersecurity risk management programs. Because of this, the FSSCC observes that Version 1.0 of the *Framework* has not yet reached full maturity, which moderates the call for large-scale revision. Rather, NIST might consider a Version 1.1, revising individual items described in the companion *Roadmap* and selected target areas for an iterative update. A limited revision would enable firms to continue assimilating the current *Framework* without fear that their cybersecurity programs would need a near-term reengineering to accommodate a new *Cybersecurity Framework*. Following a Version 1.1, NIST could schedule biennial updates alternating between major and minor revisions every two years. A scheduled approach enables the Framework to be ingrained within individual firms and across sectors while evolving in response to the dynamic nature of cybersecurity risk management.

The FSSCC suggests that any revision to the *Framework* should first address the following subsections detailed in the *NIST Roadmap for Improving Critical Infrastructure Cybersecurity*: "Federal Agency Cybersecurity Alignment," "International Aspects, Impacts, and Alignment," and "Supply Chain Risk Management."[13] While the "Federal Agency Cybersecurity Alignment" *Roadmap* section focuses on aligning federal agencies' own "Federal Information Security Management Act" ("FISMA") compliance requirements with the *Framework*, NIST should convene each sector and each sector's regulatory, oversight, and examination bodies for the purpose of aligning regimes with the *Framework* (see Section IV for further details). Such an endeavor domestically would assist the international efforts of NIST and Executive Branch agencies as they "[e]ngag[e] foreign governments and entities directly to explain the *Framework* and seek alignment of approaches…"[14] as described in the *Roadmap* subsection "International Aspects, Impacts, and Alignment." A lack of harmonization within the United States will impede

---

[12] To further drive NIST *Cybersecurity Framework* usage, one firm recommends that NIST provide the NIST *Cybersecurity Framework* in downloadable data file formats, such as CSV or other highly used database formats, which would allow firms to integrate the NIST *Cybersecurity Framework* into existing applications. To the extent that this may implicate copyright concerns, clarification of NIST's copyright protections on such materials would be beneficial and welcome.

[13] An important matter which should be undertaken separately from the NIST RFI process would be further consideration of the "Authentication" section of the *Roadmap*.

[14] NIST. *Roadmap for Improving Critical Infrastructure Cybersecurity*. Page 7. 12 February 2014. http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf.

global harmonization to the *Framework* and may fail to elicit alignment amongst our international partners.

VI. Sector-Specific Extension Templates Will Assist in Regulatory Harmonization with the NIST *Cybersecurity Framework*.

To further enable domestic harmonization, NIST should consider collaboratively developing, cataloguing, and displaying NIST *Cybersecurity Framework* extension templates for each sector, so that each sector could extend the NIST *Cybersecurity Framework* to meet their particularized product, threat, regulatory, etc., needs and requirements. As part of that work, NIST would engage each sector to map that sector's current frameworks, tools, guidance, etc., back to the NIST *Cybersecurity Framework* (perhaps in the informative references section) so that the common taxonomy and visual base holds across sectors. For example, the Federal Financial Institutions Examination Council (FFIEC) recently released its *Cybersecurity Assessment Tool.*[15] In that tool, it appropriately asks institutions to assess their own governance structures, internal audit functions, and third party cybersecurity risk management programs. These areas of concentration are not explicitly described within the NIST *Cybersecurity Framework* Core. Accordingly, if NIST was to develop an extension template for the financial services sector, it could add these items to the NIST *Cybersecurity Framework* core and also translate the *Cybersecurity Assessment Tool's* taxonomy into the more common NIST *Cybersecurity Framework* taxonomy.[16]

While not all firms use the *Framework* exclusively, establishing a common lexicon through the use of extension templates and translatable documentation furthers the collaborative goals of the *Framework* in improving the cyber risk posture of firms.

VII. FSSCC Supports NIST's Engagement and Information Sharing with Foreign Governments and Standards Developing Organizations.

The FSSCC recommends NIST adhere to its four-point *Roadmap* strategy to govern international engagement:

1. "Engaging foreign governments and entities directly to explain the *Framework* and seek alignment of approaches when possible;
2. "Coordinating with federal agency partners to ensure full awareness with their stakeholder community;
3. "Working with industry stakeholders to support their international engagement; and

---

[15] Federal Financial Institutions Examination Council. *Cybersecurity Assessment Tool.* June 2015. https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_with_Overview_and_Additional_Resources_June_2015_PDF1_5.pdf.

[16] By addressing the described third party concern in an extension template form, NIST would be addressing the "Supply Chain Risk Management" subsection of its *Roadmap*.

4. "Exchanging information and working with standards developing organizations, industry, and sectors to ensure the *Cybersecurity Framework* remains aligned and compatible with existing and developing standards and practices."

The FSSCC suggests that the focus on information exchange and standard development should include coordination with the International Organization for Standardization (ISO) and the International Organization of Securities Commissions (IOSCO) on global harmonization and the Cloud Security Alliance to integrate its "Cloud Controls Matrix" into the *Framework* within the function and category level, and informative references section, as appropriate.

VIII. U.S. Government Sanctioned "Trusted Forums" Will Enable Best Practices and Use Case Sharing, Driving Advancement in Cybersecurity Risk Management Programs.

The FSSCC encourages the U.S. government to enable trusted forums wherein firms can exchange NIST *Cybersecurity Framework* and standards usage use cases and best practices without fear of public disclosure demands and adverse regulatory actions. Through this type of uninhibited and sanctioned sharing, participating firms would be more apt to discuss both the successes as well as the shortcomings of their own approaches. From these discussions, firms would be able to learn from sector peers and peers from other sectors. They would be able to iterate and advance their own cybersecurity programs based on the best practices shared. It would also assist in establishing some level of conformity and make adherence to best practices more efficient, while reducing duplication of efforts.

In addition, the FSSCC suggests NIST continue the National Cybersecurity Center of Excellence (NCCoE) and requests the Center further explore white papers and researched analysis of NIST *Cybersecurity Framework* use, methods, and the development of a quantifiable metric tracking internal rates of return from *Framework* use.

IX. Conclusion.

The FSSCC would like to thank NIST for reviewing our comments. Should you require any clarification or additional information about the points raised in our letter, please do not hesitate to contact us.

Sincerely,

Russell Fitzgibbons

Appendix A

Financial Services Sector Coordinating Council Membership

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

Associations (23)	**Operators (32)**	**Utilities and Exchanges (14)**
American Bankers Association (ABA)	AIG	BATS Exchange
American Council of Life Insurers (ACLI)	American Express	CLS Bank International
American Insurance Association (AIA)	Aetna	The Clearing House
American Society for Industrial Security International (ASIS)	Bank of America	CME Group
Bank Administration Institute (BAI)	BB&T	Direct Edge
BITS/The Financial Services Roundtable	BNY Mellon	Depository Trust & Clearing Corporation (DTCC)
ChicagoFIRST	Charles Schwab	First Data
Consumer Bankers Associations (CBA)	Citi	Intercontinental Exchange (ICE) / NYSE
Credit Union National Association (CUNA)	Comerica	International Securities Exchange (ISE)
Financial Information Forum (FIF)	Convergex	LCH Clearnet
Financial Services Information Sharing and Analysis Center (FS-ISAC)	Equifax	NASDAQ
Futures Industry Association (FIA)	Fannie Mae	National Stock Exchange
Independent Community Bankers of America (ICBA)	Fidelity Investments	Omgeo
Institute of International Bankers (IIB)	FIS	Options Clearing Corporation
Investment Company Institute (ICI)	Freddie Mac	
Managed Funds Association (MFA)	Goldman Sachs	
Money Management Institute (MMI)	JPMorgan Chase	
National Automated Clearing House Association (NACHA)	Manulife Financial	
National Association of Federal Credit Unions (NAFCU)	MasterCard	
National Armored Car Association	Morgan Stanley	
* National Futures Association	Navient	
Property Casualty Insurers Association of America (PCI)	Navy Federal	
Securities Industry and Financial Markets Association (SIFMA)	Northern Trust	
	PNC	
	RBS	
	State Farm	
	State Street	
	Sun Trust	
	Synchrony Financial	
	US Bank	
	Visa	
	Wells Fargo	

* While NFA is a member of the FSSCC, it is a self-regulatory organization and did not participate in the drafting of this submission.

Appendix B - Auditable Third Party Risk & Cybersecurity Standard

AUDITABLE THIRD PARTY RISK & CYBERSECURITY STANDARD FOR THE FINANCIAL SERVICES INDUSTRY

FEBRUARY 2016

Contents

The Third Party Risk Challenge

Regulators Want More Transparency Regarding Cybersecurity Practices, Including Third & Fourth Parties

Boards and Senior Leaders Need Greater Oversight of Entire Business Ecosystem (Internally & Externally)

Current Methods Place Reliance on Trusting Vendor's Responses without Means to Verify or Compare Against Other Providers

Significant Cost and Resourcing Across Vendors and Financial Firms to Coordinate and Respond to Due Diligence Questionnaires

Point-in-time Assessments Don't Provide Ongoing View into Dynamic Risk Environments

The Solution: A New Standard for Financial Services

Transparency	Efficiency	Standardization
• Improved Awareness Across Organization	• Reduction of Cost & Resources	• Industry Standard of Care
• Increased Visibility into Threats & Vulnerabilities	• Targeted Assessments for Vendors	• Driven by and Aligned to Regulatory Requirements
• Better Communication with Vendors and Key Stakeholders (i.e. Board of Directors, Insurers, etc.)	• Fewer Onsite Visits • Leverage Single Review Multiple Times	• Focus on remediation of issues • "Operationalizing" the NIST Cybersecurity Framework

Decreased risk and better information for decision making

Increased confidence in controls and risk programs at vendors

Improvement in the level of information available to all firms across the industry

Working Group Mission, Deliverable & Objectives

Mission:

Streamline the third party assessment process for financial services by increasing the coverage of the AICPA SOC2 to encompass the needs of the sector, incorporate the content of the NIST Cybersecurity Framework and align the risk that is evaluated to other assessment methods.

Deliverable:

Financial Services SOC2 that can be delivered by an AICPA audit firm at a financial services firm or vendor to assess and communicate the controls that are in place and attest as to their effectiveness.

Objectives:

- Expand the coverage of the SOC2 to incorporate areas currently covered in firm specific questionnaires (in partnership with the AICPA).
- Promote use of the Financial Services SOC2 as a standardized method for assessing and communicating risk controls between customers and vendors.
- Align coverage to the AUP and promote its use as another standardized method in this process (in partnership with Shared Assessments).
- Encourage firms to accept standardized assessments.

Development of a Third Party Risk Standard for Financial Services

Typically addresses about 60-70% of the requirements that firms have in regards to measuring 3rd party risk.

SHARED ASSESSMENTS
Standard Information Gathering (SIG)
Agreed Upon Procedures (AUP)

AICPA SOC
AICPA SOC 2 & Trust Services Principles and Criteria

In order to fill the 30-40% gap that firms believe exist in the current assessment methods we gathered data from multiple sources to compile a more complete set of criteria and controls.

Firm Vendor Questionnaires

Working Group Feedback

Lessons Learned from Pilot Projects

In order to better address cybersecurity risks the working group mapped the criteria and controls to the NIST-CF subcategories to allow for communication and measurement.

NIST Cybersecurity Framework

We expect that this standard will address approximately 90% of the security, technology and business resiliency risk areas that firms care to measure and monitor at their vendors and allow for the measurement of achieving the outcomes of the NIST Cybersecurity Framework.

FSSCC

5

Components & Coverage of a Financial Services SOC 2

AICPA SOC 2 & Trust Services Principles and Criteria

- Organization and Management
- Communications
- Risk Management
- Design of Controls
- Implementation of Controls
- Monitoring of Controls
- Logical Access Controls
- Physical Access Controls
- System Operations
- Change Management
- 4th Party Risk Management
- Information Security
- Availability (Business Resiliency)
- Confidentiality (Data Management)

System Definition: Infrastructure, Software, People, Procedures and Data

NIST Cybersecurity Framework

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy
- Access Control
- Awareness and Training
- Data Security
- Information Protective Process
- Maintenance
- Protective Technology
- Anomalies and Events
- Security Continuous Monitoring
- Detection Processes
- Response Planning
- Recovery Planning
- Analysis
- Improvements
- Mitigations
- Communications

Financial Services Specific Controls and Guidance

- More specific implementations of SOC2 and NIST-CF Controls
- Specific regulatory requirements and incorporation of guidance
- Specific timelines for certification and recertification
- Signing Authority
- Secure Software Design
- Use of Open Source Software
- Privacy Policies and PII Handling
- Threat Management
- Penetration Testing

Financial Services SOC2 Report Opinion Scope

- **Description of service organization's system is accurate & fairly presented**
- **Controls in the description are suitably designed to meet standard's criteria**
- **Controls were operating effectively to meet applicable standard's criteria**

FSSCC

6

Components & Coverage for Shared Assessments Program Tools

TRUST	VERIFY
Standardized Information Gathering (SIG): Questionnaire	**Agreed Upon Procedures (AUP): Onsite Assessment Testing Procedures**
• Developed using ISO 27001/2 for the framework methodology • Standards align to ISO, PCI-DSS, HIPAA/HITECH, COBIT, and FFIEC guidance (Appendix J) • Aligns with OCC 2013-29 and NIST Cybersecurity Framework • Complete picture of service provider controls • Scoring capability for analysis and reporting • Standardized and repeatable process	• Shared Assessments AUP provides objective, robust, repeatable and consistent procedures to evaluate key controls under 16 different risk domains • Factual-based reporting which does not provide an opinion • Objective test of controls allowing for validation of SIG responses for the vendor self-assessment(s). AUP Report Template may be used to report results and compensating items • Companies view results in the context of their unique vendor risk management requirements

On-Going Improvements

- Development of a "Superset" Shared Assessments AUP framework for collaborative onsite assessments by multiple outsourcers of a single service provider where they share common services
- Inclusion of guidance on incident response found within AICPA, DOJ, FCC, HIPAA, NERC, NIST, and US-CERT incident notification guidelines
- Significant changes to the Business Resiliency; Network Security; Operations and Management; and Operational Risk related to information security sections of the AUP

Beyond Assessments

Assessment Methodology	**Financial Services SOC2 Augmented / SuperSet AUP Self Assessment**
Reporting & Opinion	**Machine Readable, Indexed and Structured for Financial Services Opinion on SOC2 and NIST Cybersecurity Framework**
Issues Resolution	**Consolidated Remediation of Issues, Re-Testing and Reporting**
Continuous Monitoring	**Standard for Outcomes Provides Foundation on Which to Build Multiple Sources Provide Data to Measure Effectiveness of Controls**
Performance Ratings	**Check & Balance for Vendors' Ongoing Performance Strategic Alignment with the NIST-CF for Metrics and Analytics**

Appendix C

FS-ISAC *All Hazards Crisis Response Playbook*

Developed and maintained by the Financial Services Information Sharing and Analysis Center ("FS-ISAC"), the *Playbook* was reduced from over 70 pages to 10 pages and re-designed for cyber and business resiliency executives and crisis response teams. Industry exercises, such as the Quantum Dawn series and the Hamilton series, have repeatedly pointed to the need for a unified *Playbook*. Similar to the NIST *Cybersecurity Framework*, the *Playbook* was developed over a six-month period relying heavily on public and private input and recommendations.

The *Playbook* puts into operations, and provides a means to mature, the NIST cybersecurity respond and recovery controls at a critical sector level. The language of the NIST controls is identifiable in the five main *Playbook* components: Financial Sector (FS) crisis communication; FS Crisis Response Coordination; Government Crisis Response Coordination; Associations, Regional and Multi-Sector Crisis Coordination; and Sector Contingency Plans and Event Closure.

The succinct structure of the *Playbook* provides ease of use and a higher probability of *Playbook* discussion and reference during crisis response. The response and recovery activities of public and private crisis groups are defined throughout the *Playbook* so that critical sector teams, and individuals, will know their roles, as well as the roles of government, other sectors and critical third parties.

Through voluntary FS-ISAC information sharing practices, the crisis groups, defined in the *Playbook*, develop trusted communities of interest that coordinate crisis communication, analysis and mitigation, response and recovery. Business Continuity leaders in the sector are integrated into the cyber and physical threat analysis process and are able to contribute their knowledge of potential operational impact to critical sector resources, systems and third party dependencies.

Supplementing the *Playbook* is a library of crisis resource guides, event specific plans and templates for use during sector exercises and actual crisis events. *Playbook* templates provide a means for the sector to incorporate lessons learned and identify plan improvements during crisis events and exercises. FS-ISAC will facilitate and maintain the development of the ongoing library of sector-coordinated contingency planning that generates from *Playbook* usage.

To promote broad awareness and adoption of the *Playbook*, financial sector leadership has expanded the 2016 sector exercise program to feature prominent use and exposure of the *Playbook*.

Appendix D

Table of Regulatory, Oversight, and Examination Agency/Body Cyber Initiatives

	Issuing Org	Date	Description
1	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."
2	CFTC	12/23/2015	*Federal Register* notice of proposed rulemaking, "System Safeguards Testing Requirements for Derivatives Clearing Organizations"
3	OCC	12/17/2015	*Federal Register* notice of proposed enforceable guidelines, "Guidelines Establishing Standards for Recovery Planning by Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches," with reference to cyber stress testing
4	NAIC	12/17/2015	NAIC adoption of "Roadmap for Cybersecurity Consumer Protections," which includes proposed 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"
5	OFR	12/15/2015	OFR "2015 Financial Stability Report," which suggests that regulatory agencies consider further regulatory disclosure requirements regarding cyber incidents
6	NIST	12/11/2015	NIST *Federal Register* request for information regarding experiences with NIST *Cybersecurity Framework* usage, impediments to use, potential revision, and future governance
7	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
8	BIS CPMI-IOSCO	11/24/2015	Consultative white paper entitled, "Guidance on cyber resilience for financial market infrastructures," proposing principle-based cybersecurity requirements
9	FFIEC	11/10/2015	Revised "IT Examination Handbook: Management Booklet" issued
10	New York	11/9/2015	NYDFS' "Letter to Federal and State Financial Regulators on Potential New NYDFS Cyber Security Regulation Requirements for Financial Institutions"
11	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
12	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
13	Massachusetts	9/30/2015	Division of Banking's Bulletin regarding "Cybersecurity Assessments & the FFIEC Cybersecurity Assessment Tool," requiring measurement of "inherent cyber risks" and "cybersecurity maturity" using the FFIEC CAT by 3/31/2016 or to call Division staff to discuss whether use of an alternative framework would be acceptable
14	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
15	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
16	NAIC	8/16/2015	Meeting minutes indicating NAIC Cybersecurity Task Force review and update of NAIC model laws and regulations to further advance cybersecurity, including potential updates to "NAIC Insurance Information and Privacy Protection Model Act (#670)"; "the Privacy of Consumer Financial and Health Information Regulation (#672)"; the "Standards for Safeguarding Consumer Information Model Regulation (#673)"; and the "Insurance Fraud Prevention Model Act (#680)"
17	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"
18	FFIEC	6/30/2015	FFIEC Cybersecurity Assessment Tool
19	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)
20	SEC	4/28/2015	Division of Investment Mgmt's "Guidance Update: Cybersecurity Guidance" for investment advisors
21	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"
22	FINRA	2/3/2015	Summary of cybersecurity principles and effective practices as reported in its February 3, 2015 Report

	Issuing Org	Date	Description
			on Cybersecurity Practice
23	FTC	8/24/2014	FTC's application of cybersecurity standards in UDAP enforcement actions post Federal Trade Commission v. Wyndham Worldwide Corporation, _____ (3d Cir. 2015)
24	SEC	4/15/2014	Office of Compliance Inspections and Examinations' "Risk Alert" announcing cyber exams of broker/dealers and investment advisors