FSSCC Financial Services Sector Coordinating Council
for Critical Infrastructure Protection and Homeland Security

April 8, 2013

Via Electronic Submission to cyberframework@nist.gov

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

Developing a Framework to Improve Infrastructure Cybersecurity

Dear Ms. Honeycutt:

The Financial Services Sector Coordinating Council (FSSCC)[1] appreciates the opportunity to provide comments in response to the request for information by the National Institute of Standards and Technology ("NIST") to assist in developing a framework to reduce cybersecurity risks to critical infrastructure ("Cybersecurity Framework" or "Framework").[3]

FSSCC, as the financial sector coordinating council, is submitting this response to NIST's Request for Information as a demonstration of the deep commitment the financial sector has to the public-private partnership envisioned by the Cybersecurity Framework. We believe that our sector should serve as a model for Framework development, and that the cybersecurity requirements already in place in the sector by regulation or sound business practices map closely to NIST and other standards envisioned as part of the Cybersecurity Framework. We also believe that the dynamic processes in place within the financial sector's regulatory agencies to amend cybersecurity regulatory requirements and within financial institutions to amend practices as cyber threats change conform to the risk-based approach the Cybersecurity Framework recommends.

FSSCC shares the Administration's concerns regarding cyber threats. For this reason, our institutions support the efforts of the federal government to combat cyber threats while protecting economic innovation and prosperity, to increase the protection and resiliency of the nation's critical cyber infrastructure and to facilitate sharing of threat data and analysis across and between critical infrastructure sectors and with the public sector. We applaud NIST's efforts to develop an effective Cybersecurity Framework, which we believe will represent an important element in addressing the challenges of

[1] A description of the FSSCC and membership listing is included as Appendix One.
[3] 78 Federal Register 13,024 (Feb. 26, 2013).

improving the cybersecurity of our nation's critical infrastructures. We commit to working with NIST in formulating this Framework.

FSSCC agrees strongly with the principles that NIST has indicated will guide the development and implementation of the Cybersecurity Framework. In particular, we concur with NIST's statements in its request for information that the Cybersecurity Framework should be a set of consensus-based voluntary standards designed to "be compatible with existing regulatory authorities and regulations," enable technical innovation and, thus, "not prescribe particular technological solutions or specifications." We also agree with NIST that an important objective of its efforts should be to encourage widespread adoption of the Cybersecurity Framework across critical industries, as the financial industry's cybersecurity is contingent on the safety and security of other critical sectors, such as telecommunications and energy.

NIST has said that, in conducting its work, it will consider integration of standards "with existing frameworks." ***To this end, we think it is particularly important that NIST's efforts complement and build upon existing cybersecurity standards adopted by the U.S. financial services industry.*** The financial sector's critical infrastructure is subject to a significant number of federal and state laws, regulations, guidance, and examination standards relating to cybersecurity, many of which emanate from the general financial safety and soundness standards and customer information security provisions contained within the Gramm-Leach-Bliley Act of 1999.[4] For example, depository financial institutions must comply with guidance produced by the Federal Financial Institution Examination Council (FFIEC). This guidance sets the standards for financial institution's information systems, outlining the minimum control requirements and directing a layered approach to managing information risks. These are rules applicable to markets as well.

As noted in the December, 2011, United State Government Accountability Office report, "CRITICAL INFRASTRUCTURE PROTECTION: Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use," financial sector regulations, guidance, and examination standards are also substantially similar to the National Institute of Standards and Technology Special Publication 800-53, mapping essentially to all of the recommended controls for federal information systems.[5] Likewise, the Securities and Exchange Commission (SEC) and the self-regulatory organizations (SROs), such as the Municipal Securities Rulemaking Board (MSRB), the Financial Industry Regulatory Authority (FINRA), and the National Futures Association (NFA) review the cybersecurity programs of exchanges, broker-dealers and clearing institutions as part of their ongoing supervisory exams and related activities. Insurance companies'

[4] Financial Services Modernization Act of 1999, (Pub.L. 106-102, 113 Stat. 1338)

[5] U.S. Government Accountability Office, Critical Infrastructure Protection: Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use (December 9, 2011), www.gao.gov/assets/590/587529.pdf.

privacy and security programs are subject to review by state insurance regulators. Health and long-term care insurers' privacy and security programs also are subject to review by the Department of Health and Human Services.

The financial sector also develops and implements leading practices through FSSCC, the Financial Services Information Sharing and Analysis Center (FS-ISAC) and other organizations and associations. For example, under the joint partnership of FSSCC and FBIIC, our sector has developed leading practices to mitigate risks associated with the resiliency of the telecommunications infrastructure including critical undersea cables, , and other important risks or threats facing the security and resilience of the sector. Likewise, the FS-ISAC routinely shares risk mitigation tactics and information to address vulnerabilities and evolving cyber-attacks.

NIST should thus recognize that the U.S. financial services industry, working in close cooperation with federal banking, law enforcement and other agencies, has a long history of facing cyber threats and, in response, has developed strong data security controls, protocols, procedures and business standards. FBIIC members regularly examine the legal, compliance and operational cybersecurity efforts of U.S. banks, securities firms, insurance companies, clearing and settlement and other financial utilities to assess the level of cybersecurity risks to these institutions and evaluate the adequacy of the organization's risk management processes. Accordingly, FSSCC urges NIST to heed the significant work that U.S. financial services institutions and their regulatory agencies have done to ensure that its Cybersecurity Framework does not impede the on-going, well-functioning public and private sector partnerships that the financial services industry has developed.

NIST also has indicated that one of its objectives is to specify "high priority gaps for which new or revised standards are necessary." We agree with this approach. Consistent with existing financial services regulatory requirements, the Cybersecurity Framework should be based on dynamic risk assessment techniques that are designed to prioritize the risk of known threats and vulnerabilities across institutions and across sectors.

We believe that, as NIST develops the Cybersecurity Framework, it should consider carefully the challenges that industry participants will have implementing the standards and guidelines that constitute the Framework, including the initial challenge of appropriate allocation of resources. NIST must be cognizant of the fact that organizational resources must be allocated based on the risk of loss resulting from inadequate or failed processes, people, or systems. The Cybersecurity Framework must be sensitive to these resource considerations and ensure that the standards, approaches and guidelines that NIST develops are truly responsive to threats, better secure the sector and are cost and time effective.

Relatedly, NIST must ensure that the Cybersecurity Framework presents achievable results. To this end, NIST must recognize that results or protection levels that are feasible in one industry or for one firm’s system may not be practicable in another based on the risk that industry or firm presents to the overall critical infrastructure. NIST can mitigate this concern by focusing on developing a baseline of commonalities across industries, working to ensure that while appropriate harmonization is pursued, approaches are available that allow maximum flexibility and can be adapted to different situations, circumstances and threats. NIST also should concentrate on “fundamental” infrastructure systems, including those systems that interact with other critical infrastructure systems. By doing so, NIST will help address structures that are interdependent between and among industry sectors. Managing risks resulting from the dependence on other critical infrastructures and providers, including telecommunications, information technology, and energy is a constant challenge.

We further believe that the federal government can play an important role in educating industry participants, retail and business customers and counterparties regarding their role in enhancing cybersecurity and protecting against cyber threats. Increased education is an essential component of any Cybersecurity Framework so that all parties are vigilant in protecting themselves and their personal devices and understand the balance between convenient access to services and security.

Finally, FSSCC recognizes the seriousness of the cyber threat facing our country and supports thoughtful efforts to prevent and mitigate future cyber incidents. We support the development of a standards-based Cybersecurity Framework that incorporates the principles we have outlined in this letter and provides the flexibility to meet new and developing cybersecurity challenges. To assist NIST in its comprehensive review, we have also included an appendix that provides answers to the specific questions posed in NIST’s request for information. The full listings of the FSSCC membership are also included as an appendix to this letter.

We thank NIST for its efforts to develop a Cybersecurity Framework to improve our nation’s cybersecurity posture. Please find attached initial thoughts in response to NIST’s Request for Information. FSSCC welcomes the opportunity to meet with NIST and provide further insights into financial services industry practices and controls.

Respectfully submitted,

Charles Blauner
Chairman
Financial Services Sector Coordinating Council

Appendix One

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, with recognition from the U.S. Treasury, to coordinate critical infrastructure and homeland security activities in the financial services industry.

Associations	Operators	Utilities and Exchanges
American Bankers Association	Allstate	BATS Exchange
American Council Life Insurers	Bank of America	CLS Services
American Insurance Association	BNY Mellon	CME Group
ASIS International	Citi	Direct Edge
BAI	Equifax	DTCC
Bankers and Brokers	Fannie Mae	Intercontinental Exchange
BITS	Fidelity Investments	International Securities Exchange
ChicagoFIRST	Freddie Mac	NASDAQ
Consumer Bankers Associations	Goldman Sachs	National Stock Exchange
Credit Union National Association	JPMorgan Chase	NYSE Euronext
Financial Information Forum	MasterCard	Omgeo
FS-ISAC	Morgan Stanley	Options Clearing Corporation
Futures Industry Association	Navy Federal	The Clearing House
Independent Community Bankers Association	Northern Trust	
Investment Company Institute	PayPal	
Managed Funds Association	Sallie Mae	
NACHA	State Farm	
National Association of Federal Credit Unions	State Street	
National Armored Car Association		
National Futures Association	Travelers	
SIFMA	Visa	
	Wells Fargo	

Appendix Two

Developing a Framework to Improve Critical Infrastructure Cybersecurity Request for Comment Responses to Questions

A. Current Risk Management Practices

As highlighted previously and discussed in greater detail below, the financial services sector has been obligated for many years to comply with various laws and regulations designed to protect the confidential data that institutions in this sector hold on their customer's behalf. As a result, the industry has devoted significant resources and attention to developing robust cyber risk management practices in order to maintain the trust and confidence of our clients and counterparties. Within financial services, it is essential to both protect customer data and ensure the networks are operational.

Cyber risks are included in over-all operational and enterprise risk frameworks. To manage cyber risks and ensure alignment with best practices, FSSCC member institutions observe and use a number of industry and regulatory frameworks, standards and guidelines. Within this broader framework, the industry uses a number of specific tools for threat measurement, monitoring, and detection and validates controls through regular testing and audits. These policies and practices are subject to review and revision in response to lessons learned from events and evaluation of emerging technological developments and evolving threats.

1. *What do organizations see as the greatest challenges in improving cybersecurity practices across critical infrastructure?*

   As a sector, there a number of identified challenges, including:

   - Establishing a robust information security function across inherently diverse cyber environments (e.g., computing, infrastructure, data management practices, security awareness, partner collaboration, third party providers, controls & measurement);

   - Reconciling and appropriately applying multiple requirements from various regulatory bodies;

   - Inconsistent application of protective measures, within institutions and sectors, and across sectors;

   - Staffing and funding, along with identifying effective education for consumers and businesses of all sizes;

- Unwillingness of Internet service and email providers to enforce protocols that would reduce anti-spoofing and impersonation capability;
- Sharing cybersecurity information across critical private sector infrastructure and with government partners given existing liability concerns;
- Keeping up-to-date on current cyber-threat trends and techniques, cyber vulnerabilities and cyber best practices in order to understand and implement technical, and personnel capacities needed to prevent or mitigate attacks;
- Oversight and compliance of third party providers;
- Establishing decision rights and responsibilities as well as guidance on assessing and re-establishing trust within compromised systems to support incident and event management; and
- Streamlining the dissemination of information to private sector critical infrastructure operators.

In addition, institutions – outside the regulated financial services sector – that have not yet established comprehensive information security practices will face a variety of challenges in addition to the challenges noted above and may be susceptible to crippling incidents.

Most importantly, developing an improved level of trust between sectors will be needed, but first trust must be fostered within the sectors. The creation of a common methodology within sectors, across sectors and with government partners for sharing will be a key component. This process needs to ensure a streamlined submission process that allows the data to be anonymized and a process that can be accessed easily and distributed across multiple platforms. In addition, the process must include a common set of agreed upon warnings and indicator data fields that offer the most efficient means to reach the goals to be achieved (must avoid the tendency to include data overload). In addition, a most robust two-way sharing of information from government partners is needed.

2. What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?

NIST will face a number of challenges, some of which are discussed above, in developing a cross-sector standards-based Framework for critical infrastructure, including:

- Identifying which best practices adequately respond to the known risks;

- Achieving uniform regulatory expectations, given the different levels of maturity of industry sectors (with different sectors at different stages and with individual institutions pursuing different goals) and the lack of, or variety of, regulatory requirements in certain industries;

- Achieving agreement on sound cross-sector Cybersecurity Framework;

- Gaining sufficient industry input and participation;

- Time and funds, which may result in the temptation to reduce research or reuse past frameworks;

- Ensuring standards are flexible so that institutions can devise solutions that fit their own risk-based needs, and

- Developing a consistent understanding of cross-sector risk and interdependency.

3. *Describe your organization's policies and procedures governing risk generally and cybersecurity risk specifically. How does senior management communicate and oversee these policies and procedures?*

For many firms, cybersecurity is governed by Enterprise or Operational Risk Management functions, working in conjunction with Information Technology, Information Security, and Technology Risk teams. Regular reporting occurs at various levels, including the Board of Directors and the Business Risk Committee of the Board of Directors, as well as executive and senior management.

Across the sector, financial services firms have developed specific risk-based policies and standards to address cybersecurity. Policies and standards are re-enforced through regular employee training and periodic knowledge testing. Additionally, adherence to policies, procedures and associated standards is validated through inspection, testing and, where possible, automated metrics. Internal and third party audits are also performed.

For many FSSCC member-institutions, cyber programs are designed to be consistent with internationally-accepted best practices. To achieve this result, institutions benchmark themselves and actively share cybersecurity threat and vulnerability information and best practices with peers in the financial services industry and outside the industry. As a result of continuous benchmarking, policies and practices are regularly updated, and senior management is typically involved in this process.

In summary, financial services institutions use advanced control processes, robust risk assessment techniques and a strong corporate and policy governance mechanism to maintain the efficacy of their cybersecurity policies across their institutions. Given the fast moving pace of the cyber threats and increasing sophistication levels of the attacks, there is residual risk that, even with strong controls, the attacks can potentially result in the compromise of a firm's systems. Moreover, while all regulated entities must adopt policies, processes and system that meet cybersecurity requirements, smaller firms will not have resources to deploy equivalent resources and capabilities to larger complex firms.

4. *Where do organizations locate their cybersecurity risk management program/office?*

Institutions' approaches vary, but generally focused around Information Security, Technology and Operations with various connections to the Board of Directors or CEO. For example, the program or office may be located in the following places:

- Information Security and Operations,
- Chief Information Officer ("CIO"),
- Enterprise Information Security Office ("ISO"),
- Chief Information Security Officer ("CISO"),
- Technology and Operations group with a connection to the Corporate Risk group,
- Information Technology Department reporting to the CIO,
- Corporate Risk Management Program ("CRMP"),
- Business Resiliency, and
- Systems Infrastructure.

5. *How do organizations define and assess risk generally and cybersecurity risk specifically?*

Institutions noted that they define and assess risks according to various risk definitions. Some focus on those found in the operational risk aspects of the Basel II[6] and Basel III[7] l frameworks for assuring adequate levels of capital and liquidity for internationally active banks. The Basel frameworks are international standards that seek to strengthen the regulation, supervision, and risk management of the banking sector across the globe. The Basel frameworks address not only credit and market risks but also operational risks, including risks from external fraud and cyber activities. Institutions also use IOSCO[8] and BIS/IOSCO/CPSS[9].

Institutions map risks inherent in certain business lines and develop risk tolerances and mitigation techniques per business line. Depending on the nature of the threat and impact comprising the risk, institutions may map at an organizational level. Specifically, cybersecurity risks are defined and assessed using threat vector analyses, which entail mapping risks to operational controls and support by active monitoring and risk metrics.

6. *To what extent is cybersecurity risk incorporated into organizations' overarching enterprise risk management?*

Institutions vary in how cybersecurity risk is incorporated. In general, information security risks are often provided to management and enterprise risk organizations for incorporation into larger risks analysis efforts. This information and analysis is used to determine the appropriate resources and prioritization needed for risk treatment or acceptance. These programs provide horizontal views of risk, and consistency to risk management approaches across lines of business.

The team responsible for cybersecurity risk provides proactive and reactive monitoring, assessment and communication of the internal and external landscape for relevant cyber events, risks and threats related to malicious code, vulnerabilities and attacks.

It is important to note that smaller financial organizations may have more focused requirements and may rely on third party service providers for a substantial part of their risk assessment management functions. However, they will still require an enterprise wide policy, plan, processes, and practices.

[6] Basel Committee on Banking Supervision, International Convergence of Capital Measurement and Capital Standards (June 2006), http://www.bis.org/publ/bcbs128.pdf

[7] Basel Committee on Banking Supervision, Basel III: A global regulatory framework for more resilient banks and banking systems (June 2011), http://www.bis.org/publ/bcbs189.pdf

[8] Available at http://www.iosco.org/library/pubdocs/pdf/IOSCOPD78.pdf

[9] Available at http://www.bis.org/publ/cpss101a.pdf

7. *What standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational and technical levels?*

A number of industry and regulatory frameworks, standards and guidelines exist, which institutions leverage for risk management. These are used to provide a responsive, transparent environment, which may be periodically reviewed by internal and external audit groups. Institutions will often have policies and standards influenced by and aligned to such laws, regulations, and guidance as: Federal Financial Institution Examination Council IT handbooks[10], NIST SP 800—series[11], ISO/IEC 27000 series[12], state data privacy laws, Sarbanes-Oxley Act[13], Gramm-Leach-Bliley Act[14], Health Insurance Portability and Accountability Act[15], Payment Card Industry Data Security Standards[16], COBIT 5[17], and CERT Resilience Management Model[18].

Institutions also leverage tools for measuring, monitoring, and managing cybersecurity risks, such as automated configuration verification systems, information loss prevention systems, network forensic tools and processes, vulnerability scanners and application testing tools. To understand the vulnerabilities of their systems, institutions may hire third parties to do penetration testing. The third parties then provide feedback on gaps and improvements to the system.

Standards, guidelines and tools are periodically assessed internally and by external regulators to confirm compliance and validate effectiveness. The information security framework focuses on people, process and technology and is designed to ensure effective transparency, measurability, reporting and oversight.

[10] FFIEC IT Examination Handbook Infobase, http://ithandbook.ffiec.gov/.

[11] NIST Computer Security Resource Center, Special Publication 800 Series, http://csrc.nist.gov/publications/PubsSPs.html.

[12] ISO/IEC 27000:2012. Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary, http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=56891

[13] Pub.L. 107–204, 116 Stat. 745 (2002)

[14] Pub.L. 106–102, 113 Stat. 1338 (1999)

[15] Pub. L. No. 104-191, 110 Stat. 1936 (1996)

[16] PCI Data Security Standards: https://www.pcisecuritystandards.org/security_standards/

[17] COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. http://www.isaca.org/COBIT/Pages/default.aspx

[18] CERT Resilience Management Model. http://www.cert.org/resilience/rmm.html

8. *What are the current regulatory and regulatory reporting requirements in the United States (e.g., local, state, national, and other) for organizations relating to cybersecurity?*

As noted above, financial services institutions are subject to an array of regulatory standards and requirements.

Financial institutions are subject to numerous U.S. federal laws – including the Gramm-Leach-Bliley Act[19] ("GLBA"), the Fair Credit Reporting Act[20] ("FCRA") and the Right to Financial Privacy Act[21] ("RFPA"), Computer Fraud and Abuse Act[22] ("CFAA"), the Health Insurance Portability and Accountability Act ("HIPAA")[23], and the Electronic Communications Privacy Act[24] ("ECPA") – relating to the protection of the consumer information that they possess. For example, since 1970, the FCRA has promoted the accuracy, fairness and privacy of personal data assembled by "consumer reporting agencies" (which includes many institutions in the industry). The GLBA requires financial institutions to adopt privacy policies and safeguards and to provide notices to consumers about those policies. Together, the FCRA and GLBA establish a comprehensive framework of fair information practices and include requirements for data quality, data security, identity theft prevention, data use limitations, data destruction, notice, user consent and accountability.

Individual institutions also have various federal reporting requirements. In the event of an attack that accesses consumer data or critical institutional data, institutions must file a Suspicious Activity Report ("SAR") with the Financial Crimes Enforcement Network ("FinCEN").[25] Institutions also may have similar reporting requirements in the case of international incidents and may have state SAR filing obligations as well.

Institutions that issue securities registered with the U.S. Securities and Exchange Commission ("SEC") also may be required to disclose known or threatened cybersecurity incidents and risks. The SEC's Division of Corporation Finance

[19] 15 U.S.C. § 1681et seq.
[20] 12 U.S.C. § 3401 et seq.
[21] 18 U.S.C. § 1030 et seq.
[22] 18 U.S.C. § 1030. http://www.gpo.gov/fdsys/pkg/PLAW-112publ283/html/PLAW-112publ283.htm.
[23] 42 USC 1320d et seq. and Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Final Rule, 78 Fed. Reg. 5565,
[24] 18 U.S.C. § 2510 et seq.
[25] Per The Currency and Foreign Transactions Reporting Act of 1970. 31 U.S.C. 5311-5314e.

has provided detailed guidance to institutions regarding their cybersecurity risk disclosure obligations.[26]

These federal standards are coupled with various U.S. state law requirements. For example, forty six states have adopted data breach notice legislation.[27] Some states, like Massachusetts, have gone further to impose affirmative data protection requirements, including the safeguarding of data through means such as encryption of personal data and network security controls, on financial institutions operating in their jurisdictions.[28] According to the National Conference of State Legislatures, at least 13 states considered legislation in 2012 that would introduce security breach notice requirements, expand the scope of existing laws, set additional requirements for notification, or change the penalties associated with breaches.

The various regulatory requirements are re-enforced by regular, proactive review by highly specialized regulators that are supported by the Federal Financial Institutions Examination Council ("FFIEC"), an interagency entity that issues data privacy and cybersecurity guidance and examination and monitoring procedures. The FFIEC, for example, has published the following standards: (i) Interagency Guidelines Establishing Standards for Safeguarding Customer Information;[29] (ii) Interagency Guidelines Establishing Information Security Standards;[30] (iii) Interagency Guidelines on Response Programs for Unauthorized Access to Customer Information and Customer Notice;[31] and (iv) Information Technology Examination Handbooks.[32]

Institutions participating in the securities and futures markets are also subject, in addition to SEC rules, to Commodity Futures Trading Commission's ("CFTC") rules. For example the Commodity Exchange Act[33] ("CEA") establishes a comprehensive statutory framework to reduce risk, increase transparency, and promote market integrity within the financial system by, among other things, "Operational Safeguards Designed to Prevent Unauthorized Access to the System" based upon the "Core Principles" established by the CTFC.

[26] See Item 503(c) of Regulation S-K and "CF Disclosure Guidance: Topic No. 2 Cybersecurity" (Oct. 13, 2012), *available at* http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[27] State Security Breach Notification Laws, Nat'l Conference of State Legislatures, http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx (last updated August 20, 2012)

[28] MA 201 CRM 17

[29] http://ithandbook.ffiec.gov/media/resources/3379/joi-safeguard_customer_info_final_rule.pdf

[30] http://ithandbook.ffiec.gov/media/resources/3484/ots-ceo-ltr-231.pdf

[31] ithandbook.ffiec.gov/media/resources/3488/ots-ceo-ltr-214.pdf

[32] http://ithandbook.ffiec.gov/it-booklets.aspx

[33] 7 U.S.C. 1 et seq

Financial services regulators have also been active recently in proposing new rules that would require some institutions to implement new policies and procedures in this area. Specifically, the SEC proposed Regulation Systems Compliance and Integrity[34], which would replace existing voluntary standards applicable to securities exchanges, clearing agencies and certain other market participants with rules intended to better protect trading markets from vulnerabilities posed by technology issues. The proposed rule targets systems, whether in production, development, or testing that directly support trading, clearance and settlement, order routing, market data, regulation, or surveillance. In addition, this proposed rule would encompass requirements for notifications, reporting and recordkeeping, and place additional controls on all systems within a firm that may have some interaction with a core trading, clearing or settlement system.

Similarly the SEC has instituted, for SROs and certain alternative trading systems ("ATSs"), a voluntary "Automation Review Policy ("ARP")". Under ARP, Commission staff has worked with SROs and certain ATSs to assess their automated systems. The ARP Inspection Program was developed to implement the Commission's ARP policy statements issued in 1989 and 1991 ("ARP Policy Statements"). In 1998, the Commission adopted Regulation ATS which, among other things, imposed by rule certain aspects of the ARP Policy Statement on significant volume ATSs. Under the ARP Inspection Program, Commission staff reviews the capacity, integrity, resiliency, availability, and security of the systems of ARP entities. Specifically, Division staff conducts inspections of ARP entities' systems, attends periodic technology briefings presented by staff of ARP entities, monitors the progress of planned significant system changes, and responds to reports of systems problems at ARP entities. As noted above, the SEC has recently proposed to replace the voluntary ARP program with proposed Regulations SCI. Proposed Regulation SCI would codify and expand the ARP Program. Although not rising to the level of a regulatory obligation, a variety of industry rules have developed and constitute additional standards financial institutions must follow to access payment services. For example, the Payment Card Industry Data Security Standards ("PCI DSS"), promulgated by the PCI Security Standards Council, provide a framework for developing robust payment card data security process and include prevention, detection and appropriate reaction to security incidents.

Recently, the European Commission published on a draft Network and Information Security (NIS) Directive, as part of its EU Cybersecurity Strategy, which would institute risk management and reporting requirements on 'key industries', including banking and financial institutions. Similarly, the European

[34] http://www.sec.gov/rules/proposed/2013/34-69077.pdf

Parliament has proposed new regulations increasing data breach requirements on institutions.

As noted in the December, 2011, United State Government Accountability Office report, “CRITICAL INFRASTRUCTURE PROTECTION: Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use,” financial sector regulations, guidance, and examination standards are also substantially similar to the National Institute of Standards and Technology Special Publication 800-53, mapping essentially to all of the recommended controls for federal information systems.

9. *What organizational critical assets are interdependent upon other critical physical and information infrastructures, including telecommunications, energy, financial services, water and transportation sectors?*

As noted by both NIST and the Presidential Executive Order, sectors rely on each critical infrastructure sector for specific aspects of their business. We agree with the assessment made in the Executive Order that the communications and energy sectors are uniquely critical. We identify these sectors as an outage in one of their key systems can create a cascading outage effect to other critical infrastructure sectors. What performance goals do organizations adopt to ensure their ability to provide essential services while managing cybersecurity risk?

Organizational strategy includes the roles and responsibilities for producing policy, communications, security technology design, and implementation approaches. All services are evaluated and categorized from the cybersecurity risk perspective. These processes ensure that business services deemed crucial to an institution’s ability to operate receive a higher level of scrutiny.

Critical services are assigned the most stringent controls, which include redundancy and diversity measures, and validation of these controls is performed continuously. Critical processes are also targeted for the development of contingency plans, which are tested in case of service disruption regardless of the cause.

The corporate business continuity plan incorporates all processes where security considerations are imbedded. Enterprise security programs include processes wherein cybersecurity risk is appropriately balanced against the inherent service risk such that the organization is able to maintain critical services acceptable to customers while not causing undue risk to the organization or its customers and employees.

10. *If your organization is required to report to more than one regulatory body, what information does your organization report and what has been your organization's reporting experience?*

Financial institutions report to a large number of regulatory agencies in response to financial (e.g., capital), operational (e.g., data management) and risk issues (e.g., privacy). Institutions also report to both regulatory and non-regulatory bodies, including law enforcement, FinCEN, state agencies, and the SEC. In addition, cybersecurity frequently is the subject of inquiries from institutions' primary regulators in the U.S. and internationally. The reports vary in their requirements based on the needs of the primary audience and the potential secondary audiences.

Various reporting requirements are burdensome and costly to financial institutions with little reciprocal benefit. It is necessary to consider the current reporting requirements and data shared prior to requiring new data reporting requirements.

11. *What role(s) do or should national/international standards and organizations that develop national/international standards play in critical infrastructure cybersecurity conformity assessment?*

Standards bodies are critical to establishing a risk framework but should not play a direct role in conformity assessment. However, they should provide tools (e.g., checklists) to equip risk assessors to effectively measure critical infrastructure compliance. These tools should focus on control functionality rather than management process.

FSSCC urges NIST to coordinate and align U.S. and international standards to reduce the conflicts and duplication of effort that can accompany different local-jurisdictional requirements and so that institutions can rationalize and streamline operations. International conformity can aid in enabling collaboration, foster sharing techniques and provide guidance to institutions that have less mature risk management capabilities.

FSSCC urges NIST to ensure the framework consists of generally applicable standards and guidelines that can be modified by industry to fit varying businesses, practices and local-law requirements across the globe and can respond to potential worldwide cyber threats.

B. Use of Frameworks, Standards, Guidelines and Best Practices

As discussed above, the financial services industry employs a wide variety of control frameworks and best practices. The industry takes a "mature" and well-developed approach to cybersecurity, as reinforced by regulatory requirements and supervisory expectations. These standards, guidelines, and practices must take into account the widely varying nature of financial businesses and organizations and the vast differences in size between institutions as well.

In developing its Cybersecurity Framework, NIST should recognize the many affirmative steps already taken by the sector and should incorporate the industry's approaches into the guidelines and standards that NIST develops. NIST also may need to account for differences in sectors when developing its framework. A 'one-size-fits-all' approach would likely be ineffective, as sectors will approach the Cybersecurity Framework from different positions (in terms of maturity and regulatory requirements) and face different threats. Best practices should be used to define the objective – not the specific processes and procedures to achieve the objective. This approach can provide the latitude for defining a strong Framework without constraining an organization to use its creativity and innovation.

As appropriate, the relationship between the FSSCC and FBIIC through the sector specific agency, the Department of the Treasury, should be leveraged. It is essential that any new processes support and strengthen the existing infrastructure. When an institution faces a data breach or cyber-threat, it has to interact with multiple regulators and governmental groups of varying degrees of utility from the perspective of the sector. Further consideration should be given to improving the flow of requests and information within the context of the complex statutory requirements and mandates of the regulatory, law enforcement and intelligence communities.

1. What additional approaches already exist?

As mentioned above, institutions use a number of frameworks, standards, guidelines and best practices. Guidance commonly referred to by information security professionals when developing or maturing practices include NIST SP 800 series and the ISO/IEC 27000 series. Audit professionals often also refer to regulatory and international standards. Regulatory standards include:

Basel III, FFIEC Information Security Handbook, and general IT controls required by the Sarbanes-Oxley Act.

International standards include: ISACA Control Objectives for Information and Related Technology (COBIT), Payment Card Industry Data Security Standards

(PCI-DSS), COSO Financial Controls Framework[35], Information Technology Infrastructure Library[36], Capability Maturity Model[37] (CMM), Information Security Management Maturity Model[38] (ISM3), CERT Resilience Management Model, Open Web Application Security Project[39] (OWASP), ASC X9 standards[40], CERT Control Systems Security Program[41], and CERT Cyber Security Policy Planning and Preparation.[42]

Technology professionals count on NIST, CIS, and SANS for guidance on secure device configurations.

Likewise, the SEC and the SROs, such as the MSRB, FINRA, and the NFA review the cyber security programs of exchanges, broker-dealers and clearing organizations as part of their ongoing supervisory exams and related activities. Similarly, the CFTC reviews the cybersecurity of financial market infrastructures as part of its supervisory activities.

2. *Which of these approaches apply across sectors?*

Though some are designed to address requirements of specific sectors, all can apply to other sectors, but they must be adapted appropriately. In addition, many of the general (non-sector specific) regulations and laws apply across sectors but may not be applicable to all institutions (e.g., SEC requirements).

3. *Which organizations use these approaches?*

Institutions within financial services use a mix of the standards and approaches listed above to assist in managing the cyber risk. However, no one approach is used across the sector.

4. *What, if any, are the limitations of using [existing] approaches?*

The prime risk posed by any published standard is that it was developed at a given “point in time” and so reflects the judgment of the publication committee at that time. Cybersecurity risks may shift faster than the assessment, policy, standards and remediation can adapt. Existing approaches for cybersecurity, a discipline

[35] Enterprise Risk Management — Integrated Framework. http://www.coso.org/guidance.htm
[36] http://www.itil-officialsite.com/
[37] CMMI Institute powered by Carnegie Mellon http://cmmiinstitute.com/results/
[38] www.ISM3.com
[39] www.owasp.org
[40] https://www.x9.org/home/
[41] http://ics-cert.us-cert.gov/csetdownload.html
[42] http://ics-cert.us-cert.gov/csstandards.html#plan

that is, by its nature, highly dynamic and ever changing, are limited in the ability to adapt as cyber risks evolve.

Any Cybersecurity Framework must be both highly structured, yet, nimble and flexible enough to adapt in real time as threats emerge. In addition, standards or guidelines that amount to a static set of "checklists" without an initial risk-based approach may result in institutions being "compliant" without being effectively secure. There is also the risk to common standards developing within and across sectors, which prevent or limit a firm's ability to innovate in protecting its systems in a way that is not used by others. By adopting a common framework we could open the sector and critical infrastructure more generally to the same risks and threats due to the lack of independent development.

Another key limitation is that current cybersecurity approaches are specific to their mission and goals. Each was developed independent of the others and, as a result, different standards may be hard to reconcile with each other.

Finally, standards, guidelines and best practices may not be sufficient if skilled resources are not deployed in a particular organization. For some institutions and sectors, resource constraints have been a factor limiting cybersecurity and will continue to be a factor in implementing any standards proposed by the Cybersecurity Framework.

5. *What, if any, modifications could make these approaches more useful?*

A successfully-designed common framework will allow for better compatibility across industry and sector approaches. Modifications to harmonize existing standards into a common framework include: consolidating existing standards, broadening the scope of existing standards to make the standards more encompassing, and clearly marking the standards to be used for a particular type of asset.

Mapping controls to risks and threats across diverse frameworks is another modification that can help in the structure, execution and analytics of the key operational techniques being used for effective cybersecurity risk management. The development of one common cross-framework taxonomy would not only support the mapping process, but also help to identify existing or potential gaps that may appear in one or more of the best practices.

However, no approach will be useful unless it has developed clear and actionable frameworks, standards and guidelines. Clarity can be established through improved coordination between and among standards-making bodies, and an actionable framework is one that is designed and empowered to identify, assess and respond to threats as they occur. Finally, standards should not be static or technology specific, but should be risk-based to fit the local situation.

6. *How do these approaches take into account sector-specific needs?*

Several are designed for specific needs that may or may not flow across different sectors. As such, they may take different approaches on the same issue. In addition, for those that do not take a sector approach, they rely on the interpretation based on the specific needs of the sector to allow a more effective use of the approach.

For example, within the FFIEC IT Handbook reference is made to specific standards for use to assess risk. The Handbook also may identify alternative applications to the standards or specific applications.

As NIST develops the Cybersecurity Framework, it must be an agile and flexible approach that accounts for size, complexity, and nature of the information and/or services an institution maintains or provides.

Two more specific examples are outlined below.

The NIST SP 800 series is specific to the governmental sector when it is prescriptive, but it is also generic enough that other institutions and sectors can adopt the guidance and adapt it to their environment without significant difficulty. For institutions that work with / provide services to governmental bodies, this alignment helps ensure the governmental body that appropriate security controls are considered.

In the case of standards such as the ISO/IEC 27000 series, the guidance is abstract so that it can be interpreted and applied by an organization such that the required controls can be met in a manner specific to the organization's business, technology and risk environments. Where prescriptive minimal requirements are specified, they are generally considered acceptable across institutions and sectors. Additionally, this is an internationally accepted set of standards that provides flexibility to ensure institutions can adapt the controls to fit the various legal and regulatory environments in which they operate.

7. *When using an existing framework, should there be a related sector-specific standards development process or voluntary program?*

Given that all sectors are at risk to similar threats, there is a need to have basic core element requirements across sectors. In addition, it is essential to provide sector specific guidance. One common standard for all sectors would be ineffective as different sectors, and within each sector, face vastly different threats. Sector-specific guidelines would be useful to ensure continuity and applicability across the sector. Guideline development could be led by those institutions that have more mature cybersecurity risk management institutions. The development of a guideline will allow those smaller players in the sector to participate more easily in the voluntary standards. We support the development and adoption of voluntary sector-specific standards which are flexible and adaptable based on an organization's existing size and complexity.

8. *What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches?*

As noted above, a common approach for all sectors would be ineffective. We believe sector-specific agencies and sector coordinating council play a critical role in developing sector-specific guidelines. Sector-specific agencies, along with the sector regulators may be sufficient to foster the continued performance improvements. Sector coordinating councils can enable the collaboration, cooperation and dialogue across the diverse mix of institutions within each sector and facilitate action for sector-wide risk issues.

9. *What other outreach efforts would be helpful?*

Trade associations that facilitate cybersecurity work in the financial services sector-- such as American Bankers Association, BITS, Securities Industry and Financial Markets Association and others, should be involved in framework development, along with the FSSCC, as noted above. Likewise the Financial Services Information Sharing and Analysis Center (FS-ISAC) should be included given their experience with incident response and intelligence sharing in the sector.

C. **Specific Industry Practices**

The following responses relate to the specific industry practices identified by NIST (separation of business from operational systems; use of encryption and key management; identification and authorization of users accessing systems; asset identification and management; monitoring and incident detection tools and capabilities; incident handling policies and procedures; mission/system resiliency practices; security engineering practices; and privacy and civil liberties protection).

1. *Are these practices widely used throughout critical infrastructure and industry?*

The practices identified by NIST in this section of its request for information are widely used throughout the banking and financial services industry, as legal and regulatory compliance requires that such practices are implemented and maintained. Encryption, to give one example, is a regulatory requirement for specific types of data and, thus, commonly employed.

The practices listed by NIST are employed to specific systems or assets for the secure operation of critical infrastructure and are essential.

2. *How do practices relate to existing international standards and practices?*

Cybersecurity is a universal problem and, as a result, financial industry practices take into account international standards. These practices are often combined at the institution level, as the practice may not have been developed with a full understanding of international requirements.

The current practice is to focus on standards developed as part of the Basel international framework. While much of the Basel criteria are focused on capital and liquidity criteria, Basel makes a number of operational recommendations that should be taken into consideration when developing a cybersecurity program.

The Basel Committee on Banking Supervision has issued two papers on operational risk to promote improvement in this area. Originally issued in 2003, "Principles for the Sound Management of Operational Risk" outlines important principles based on industry best practices and supervisory experience for governance, risk management, and disclosure.[43] In 2011, the Committee, through its Operational Risk Subgroup (SIGOR) issued "Supervisory Guidelines for the Advanced Measurement Approaches (AMA)"[44] to suggest effective operational risk management and measurement practices for the development and

[43] http://www.bis,.org/publ/bcbs195.pdf

[44] Basel II provides for three methods of calculating operational risk; the Advanced Measurement Approach (AMA) is the most sophisticated and risk sensitive of the three methods.

maintenance of key internal governance, data and modeling frameworks underlying AMA. The recommendations include: (i) "third line of defense structures" with independent validation and verification; (ii) review of corporate operational risk management function and risk measurement systems by independent internal or external auditors; (iii) use tests and experience; (iv) granular, well-defined operational risk categories; and (v) dependence modeling for operational risks with assumptions being supported by a combination of empirical and expert judgment.[45]

Practices are consistent with the NIST SP 800-53 security standards and guidelines and ISO/IEC 27001.

3. *Which of these practices do commenters see as being the most critical for the secure operation of critical infrastructure?*

As noted, we believe that these should be leveraged based on risk-based assessment and, therefore, no single framework or practice is most critical. In general, the following practices are critical: use of encryption and key management, identification and authorization of users accessing systems, monitoring and incident detection tools and capabilities.

4. *Are some of these practices not applicable for business needs within particular sectors?*

All are applicable to some systems or assets within the financial services sectors. Other sectors, guided by a risk-based assessment, will find that the practices will be applicable to specific systems or assets. Given each sector's unique priorities, these may differ based on a sector's responsibility for protection of physical versus digital assets.

5. *Which of these practices pose the most significant implementation challenge?*

Institutions currently implement many of the specific practices noted above within their critical systems or assets per a risk-based assessment. The main concern of institutions is to identify, understand and rank threats and institutional weaknesses and then employ the necessary protection strategies based on that assessment. The challenges for institutions may arise in the identification of assets in an efficient, repetitive and continuous fashion. These challenges may vary depending on the size and complexity of an institution.

[45] http://www.bis.org/publ/bcbs196.pdf

Another challenge is when the requirements are at odds with one another or in limited instances, is mutually exclusive, and based on the institution's regulatory requirements. Implementation in those circumstances requires parallel or duplicate infrastructure or operational implementations that are designed to meet diverse requirements. This challenge arises most frequently in the privacy and civil liberties practices, given the variety of requirements in numerous geographies.

It is essential that there is a cross sector approach to risk which identifies cross sector priorities. In addition, we must recognize the unique profiles of sectors and identify the specific priorities for each sector.

6. *How are standards or guidelines utilized by organizations in the implementation of these practices?*

Standards and guidelines allow for the development of a consistent approach by allowing institutions to leverage the collective knowledge of the standards bodies. It also provides a consistent evaluation tool for use by internal and external audit teams.

In addition, institutions may develop internal standards or guidelines through their risk governance functions, which allows for the consistent implementation of requirements enterprise-wide. This allows institutions to effectively and efficiently secure infrastructure and comply with international requirements.

7. *Do organizations have a methodology in place for the proper allocation of business resources to invest in, create, and maintain IT standards?*

In general, the financial services industry has a methodology in place, stemming from a regulatory structure that calls on financial institutions to maintain the necessary investment-levels. Institutions have various efforts to accomplish this goal, including sourcing strategies that align resources to priority work and methodologies requiring staff, financial and partnerships, to effectively allocate business resources. In addition, institutions participate in the FSSCC, FS-ISAC and various security-focused associations (e.g., ISACA, SANS, CIS) to identify upcoming priorities for necessary funding.

8. *Do organizations have a formal escalation process to address cybersecurity risks that suddenly increase in severity?*

In general, financial institutions have processes in place to escalate such risks. Particularly, institutions have cybersecurity programs, which are designed to identify and react to immediate and emerging threats quickly. These programs may include response teams with specific protocols for monitoring, assessing, communicating and escalating cybersecurity issues. These programs leverage mature incident response processes that include appropriate management escalation and end-user notification procedures that apply to any technology-related outage or other service disruption. Depending on the threat, institutions may choose to immediately notify the Board or shareholders. In addition, institutions have robust business continuity requirements, which include developing processes for escalation and notification.

In addition, the sector has developed and continues to update the Financial Services Sector All-Hazards Crisis Response Playbook. The playbook describes the sector's organizational roles and functions and outlines actions that member institutions may take to prepare for, respond to and recover from cyber and physical incidents. It documents the sector's core capabilities and constitutes a coordinated cyber and physical response process, predicated on a simple, consistent and structured framework, fully integrated with sector-specific and national level frameworks. The playbook is developed collaboratively between the FSSCC and the FS-ISAC. It recognizes the specific roles of each within the sector during a crisis.

Most recently, following the recent distributed denial of service attacks, the Office of the Comptroller of the Currency released an alert to elevate the risks for all companies.[46]

9. *What risks to privacy and civil liberties do commenters perceive in the application of these practices?*

Privacy and data security are intertwined and should be considered congruently. Attaining the appropriate level of privacy, individual and corporate, and assuring civil liberties is a continuing challenge to maintaining cybersecurity. Understanding these sensitivities is essential to the successful security of an organization. This becomes even more challenging and difficult for institutions that operate in numerous countries.

Institutions employ all appropriate and necessary privacy protections, as well as notify their customers as to this use of the data. In general, implementing and/or maturing security practices should not create risks to privacy, assuming that individual institutions remain in control of the data within and the security controls directly attached to their infrastructure and systems.

Institutions implement systems and procedures in response to regulatory and legal requirements imposed by Congress. Congress creates legislation that protects civil liberties (such as limiting the ways that the federal government can access

[46] http://www.occ.gov/news-issuances/alerts/2012/alert-2012-16.html

information about U.S. citizens), and private sector institutions adopt practices in response (such as practices that have been implemented to comply with the Right to Financial Privacy Act, which requires subpoenas and other formal steps when government seeks bank and other records).

The financial services sector faces heightened scrutiny regarding information use and disclosure practices. This has an impact on institutions' willingness and ability to share information for cybersecurity purposes, particularly where there are regulatory or other concerns, such as consent. The Cybersecurity Framework will only work well if institutions are not constantly worried about potential privacy-related liability.

10. *What are the international implications of this framework on your global business or in policymaking in other countries?*

Depending on the results of this framework, it may add to the need to continue to advocate for consistent regulatory requirements across countries. Though the development of this framework provides the opportunity to create consistency and reduce duplications that currently exist.

As the sector has experienced in its implementation of CFTC Cross-Border Swap Rules for Internal Business Conduct, when rules are not harmonized it leads to increased compliance costs, confusion on the application of the rules and ultimately limited increased protections to the institution or the customer.

11. *How should any risks to privacy and civil liberties be managed?*

Institutions have operational risk, privacy officers and counsel within their institutions that bring the expertise and understanding of privacy concerns. It is essential that they be involved in the development of internal practices and alert of any concerns. This should be done at the institution level, as each institution develops and holds data in unique ways as necessary by their business needs. Privacy concerns need to be considered across the entire enterprise and the subject matter experts on privacy should be integrated into both policy and operational activities to ensure concerns are addressed.

Civil liberties protections are encompassed at a different level – these protections are found in the laws passed by Congress. Private-sector institutions comply with such laws, which protect civil liberties by limiting government (not private institutions) access to personally identifiable data of citizens.

In addition, in identifying and responding to threats institutions share threat data across the sector. This is essential to protecting the individual systems. This data is specific to threat identification and response. In today's environment it is necessary to share this data across the various sectors and legislation must be passed to alleviate the liability and anti-trust concerns, so that institutions may share across sectors.

12. Are there other practices that should be included in the standards?

Education of consumers as to the need for securing their personal networks and demanding secure technology to ensure a clean digital work environment is essential as to the future of this work. Without this knowledge, individuals may unknowingly be aiding in a cyberattack. This may include a commercial offering by those within specific sectors to offer scanning and mitigation services.

There are network security services (e.g. DNS black holing) that may be more efficient to be implemented at the carrier level (versus at each individual enterprise). Implementation of these services does not obviate the responsibility of institutions to protect their individual enterprises, but instead provides a base level of security to all participants, and amortizes the cost across all participats. Given the substantial influence of the NIST Cybersecurity Framework initiative, this may help to encourage the Internet Service Providers (ISPs) to create and expand these types of services.