February 16, 2017

BY ELECTRONIC SUBMISSION

Robert deV. Frierson, Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, NW
Washington, DC 20551

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

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

Re: Enhanced Cyber Risk Management Standards:
Federal Reserve Board Docket No. R-1550, RIN 7100-AE 61;
OCC Docket No. OCC-2016-0016, RIN 1557-AE06;
FDIC RIN 3064-45

Dear Sirs and Madams:

The Financial Services Roundtable/BITS ("FSR/BITS")[1], the leading advocacy organization for America's financial services industry, submits this letter in response to the

[1] As *advocates for a strong financial future*™, FSR represents the largest integrated financial services companies providing banking, insurance, finance, payment and investment products and services to the American consumer. Member companies participate through the Chief Executive Officer and other senior executives nominated by the CEO. BITS is the technology policy division of FSR and addresses emerging threats and opportunities, particularly those related to cybersecurity, fraud reduction, critical infrastructure protection and innovation. Working with CEOs, CIOs, heads of IT Risk and other senior members of member companies, BITS identifies key issues at the intersection of financial services, technology and commerce and facilitates collaboration to improve the e-commerce environment for member companies and their customers through the development of policies and practices.

above-referenced Advanced Notice of Proposed Rulemaking (the "ANPR") issued by the OCC, Federal Reserve and FDIC (collectively, the "Agencies"). FSR/BITS and the large number of firms that contributed to this response share the Agencies' concern about securing the financial sector from cybersecurity threats and appreciate this advance opportunity to comment upon this critically important matter. We are encouraged by the Agencies' interest in receiving multiple rounds of comments before any final rules are implemented, and look forward to working with the Agencies to make the financial sector safer and more secure from cybersecurity threats.

I. The Agencies Should Adopt a Risk-Based Approach to Cyber Regulation of the Financial Services Sector

FSR/BITS applauds the Agencies' willingness to consider a variety of approaches to cyber regulation in the financial sector and believes that, for several reasons, it is critical that the Agencies adopt a risk-based approach to cybersecurity regulation. A risk-based approach would eschew prescriptive requirements in favor of permitting financial institutions to align their cyber risk strategies with their particular risk profiles. Rather than imposing a rigid set of requirements that purports to fit the needs of all institutions in this very diverse sector, a risk-based approach would hold institutions accountable to develop a customized, enterprise-wide program of cyber preparedness based on a more accurate assessment of their inherent and residual risks.[2]

Risk-based cybersecurity is fundamental to the information security field. It has been recognized by a variety of well-respected entities, most notably the National Institute of Standards and Technology ("NIST")[3], as the most effective approach to managing cyber risks. In 2014, NIST released the *Framework for Improving Critical Infrastructure Cybersecurity*, otherwise known as the NIST Cybersecurity Framework; on January 10th, NIST issued a draft update to this Framework.[4] As the Agencies noted in the ANPR, the NIST Cybersecurity Framework is a risk-based model "intended to be customized by different business sectors and individual organizations to best suit their risks, situation, and needs." The NIST Cybersecurity Framework was developed through a joint effort of both the public and private sectors, the financial services sector contributed greatly to its development, and has been actively using it.

---

[2] On December 28, 2016, the New York Department of Financial Services revised its proposed cybersecurity regulations for financial institutions to a more risk-based approach after receiving a large volume of comments from industry stakeholders and is again seeking stakeholder comment. *See* NYDFS Revised Draft Regulation, http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf.

[3] NIST Framework for Improving Critical Infrastructure Cybersecurity, https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[4] NIST *Framework for Improving Critical Infrastructure Cybersecurity*, *Draft Version 1.1*, https://www.nist.gov/cyberframework/draft-version-11.

The NIST Cybersecurity Framework update – Draft Version 1.1 – is open for comment until April 10, 2017. The financial services sector intends to supply commentary by that date.

A risk-based approach as outlined in the NIST Cybersecurity Framework is preferable to more prescriptive approaches for two key reasons. First, cyber adversaries are continually changing their methods and strategies to attempt to compromise defenses. To create an effective security profile, organizations must adapt to meet these ever-changing threats. Similarly, the technologies underlying our business models and the tools available to us to detect and defend against malicious cyber activity are likewise evolving on a constant basis. The reality of rapid technological change also applies to the tools available to hackers and others who seek to compromise our systems or disrupt operations. This constantly evolving environment makes the traditional rulemaking process ill-suited to handle these ever-changing security threats. What are considered best practices today may well be outdated in the near future.

Second, the incredibly wide range of institutions in the financial sector—by business type, size, complexity, and geographic footprint, among many other factors—means that each institution will have a unique risk profile that, in turn, requires a customized program of security. Institutions vary in their size, complexity and impact upon the greater financial sector. Each institution requires the flexibility to build a customized cybersecurity strategy that addresses its particular businesses and is based on a robust assessment of the cyber risks it faces. By contrast, a prescriptive, checklist-style compliance mechanism ultimately makes institutions less safe by introducing unnecessary variables and distracting key personnel from developing the most effective cybersecurity approach for the institution's unique characteristics.

In sum, FSR/BITS encourages the Agencies to limit the use of inflexible, universal requirements in the proposed standards in favor of a framework-based set of security control objectives that each financial institution may accomplish in any appropriate and prudent manner commensurate with its unique technology, business and risk profile.

II. Need for Harmonization of Existing Frameworks

The financial services sector is both keenly aware of and shares the growing concern of state and federal regulators that we collectively need to continue to take more proactive cybersecurity approach. Unfortunately, the significant efforts undertaken by financial institutions to better coordinate their efforts and continually refine a risk-based approach to cybersecurity have not been reflected in the regulatory landscape. The financial services sector is now faced with an overlapping and ever-multiplying number of frameworks, guidance and tools, such as the Interagency Guidelines Establishing Information Security Standards,[5] the FFIEC Cybersecurity Assessment Tool,[6] the recently revised New York Department of Financial Services proposed cybersecurity regulations for financial services companies[7], and the OCC's

[5] https://www.federalreserve.gov/bankinforeg/interagencyguidelines.htm.

[6] https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_June_2015_PDF2.pdf.

[7] New York State Department of Financial Services Proposed Cybersecurity Requirements for Financial Services Companies, http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf.

guidance[8] on third party relationships and risk management.[9] Viewed in isolation, these regulations are each well-intentioned and can contribute to the cybersecurity of the financial services sector. When layered upon one another, however, they create differing and potentially conflicting approaches to cybersecurity, requiring firms' information security professionals and operating staffs to spend substantial time and resources complying with each individual regulatory requirement instead of developing new methods of mitigating the ever changing cyber risks. In short, the focus becomes compliance with an array of disparate requirements rather than development of a comprehensive, tailored cybersecurity program for the company.

FSR/BITS joins FSSCC in calling for a comprehensive review of existing regulations, standards, tools and guidance with a "gap analysis" to harmonize, streamline and strengthen the regulatory regime for the financial services industry. Harmonization would create a common lexicon for sector participants to improve industry collaboration and regulator engagement, enabling information security professionals to focus on security, rather than compliance.[10] The ultimate result would be a universal, risk-based and non-prescriptive cybersecurity regulatory requirement for the financial sector, built from the foundations of existing frameworks. A common framework would not only benefit the financial services sector, but would also serve as an example for other agencies, jurisdictions and industries to follow.

FSR/BITS believes that the Agencies should engage in a robust dialogue with the financial services sector to rationalize the current regulatory environment and address the questions raised in the ANPR before taking any further steps in the rulemaking process.[11] As perhaps the leading target of malicious cyber actors for many years, the financial services sector has a strong understanding of the cyber threats affecting our organizations. We likewise have developed many effective practices to prevent, detect and respond to these threats; in many cases, have brought significant expertise in-house; and work continuously to hold ourselves accountable to a higher cybersecurity standard than any required of us by regulation. In addition, we continuously seek to expand our knowledge in this frontier and respectively request the government to support initiatives that further increase academic and industry research and

---

[8] https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html.

[9] The various standards and guidelines in the financial sector cybersecurity regulatory field are further detailed in the comment letter that will be contemporaneously submitted by the Financial Services Sector Coordinating Council ("FSSCC"). Once posted, that letter can be found at: https://www.fsscc.org/News-and-Publications.

[10] Harmonization of cybersecurity regulations is a designated Action Item in the recently published report from the Presidential Commission on Enhancing National Cybersecurity. *See* Report on Securing and Growing the Digital Economy, Action Item 1.4.3, at 20-21, https://www.whitehouse.gov/sites/default/files/docs/cybersecurity_report.pdf.

[11] On October 20, 2016, the Department of Homeland Security approved a joint working group to facilitate interaction among government entities and representatives from the financial sector-critical infrastructure owners and operators. https://www.dhs.gov/financial-services-working-groups.

development in the area of cybersecurity intelligence, defense and resiliency engineering. Against this backdrop, FSR/BITS members share the Agencies' concerns regarding the cybersecurity preparedness and resiliency of the financial sector and wish to continue their role as leaders in advancing cybersecurity.

FSR/BITS appreciates the Agencies' repeated recognition in the ANPR that many unresolved questions remain and more analysis is needed of potential approaches, demonstrated by the breadth of the ANPR itself, which proposes 84 potential standards across eight distinct areas or categories it proposes. To give these complex issues the attention they warrant and strengthen cybersecurity in the sector, we are eager to engage with the Agencies in an intensive examination of these issues. In this vein, the Presidential Commission on Enhancing National Cybersecurity has identified private-public collaboration as vital for protecting our nation's critical infrastructure, recognizing that "neither the government nor the private sector can capably protect systems and networks without extensive and close cooperation."[12] We welcome such cooperation.

The wide scope and evolving nature of cybersecurity makes this issue uniquely suited for consideration in the already established Critical Infrastructure Partnership Advisory Council ("CIPAC") financial services subgroup. Rather than addressing this complex, dynamic set of issues through a single rulemaking process, leveraging an iterative and structured collaboration between the public and private sectors to address these issues in a sequential and risk-informed manner has the promise of achieving results faster and with a higher degree of protection for our customers.

III. Specific Comments

In addition to the general comments referenced above, which FSR/BITS believes are critical to the development of strong and adaptable cybersecurity standards for the industry, we also would like to provide the following feedback with respect to specific proposals contained in the ANPR.

A. Scope of Application

1. Determination of Covered Entities

The ANPR proposes applying the new cybersecurity standards to financial institutions regulated by the Agencies with consolidated assets of $50 billion or more, including subsidiaries and foreign banks with U.S. operations. FSR/BITS is concerned that this bright-line classification would, in practice, be ineffective in capturing the appropriate entities whose cyber risk should be regulated by the Agencies. Additionally, FSR/BITS is concerned that the ANPR proposes a new standard for institutions that are systemically important to the financial sector. While we recognize that the debate over what intuitions are or are not systemically important is ongoing, at minimum, FSR/BITS believes that the definition should be risk-based and consistent across regulations.

[12] Report on Securing and Growing the Digital Economy 13.

Additionally, the proposed scope of covered entities is demonstrative of the advantages of risk-based standards for cyber risk management. Risk-based standards based on consistent measures for systemic importance would capture the entities that pose the greatest risk to the financial sector, regardless of asset size. FSR/BITS members welcome the opportunity to work collaboratively to develop an agreed-upon sector risk profile and corresponding framework that would inform the Agencies in their future regulatory activities and guide the covered entities in their risk management decision making.

2. Applicability to Third Parties

FSR/BITS appreciates the Agencies' recognition that cyber risk can lie not with financial institutions themselves, but with the third-party vendors that are necessary to the functionality of their systems. FSR/BITS believes that regulation of third parties should be risk-based, evaluating factors such as the vendor's risk profile, cybersecurity policies, experience, personnel, physical security, access controls, and incident response preparation. In particular, we are convinced that the most effective vendor cybersecurity risk management program sets forth guidelines that take into account these and other factors and allow the institution to group vendors by the nature of the risks they present and to develop due diligence standards, access controls, monitoring, contractual provisions and other protections commensurate with these risks.

FSR/BITS has concerns, however, about how the standards would be applied to third parties and the statutory authority the Agencies have in applying them. As a practical matter, FSR/BITS is concerned that responsibility for oversight of third parties will be placed upon the covered entities, creating a new and potentially onerous operational risk in both time availability of skilled resources and cost. Financial institutions contract with hundreds, if not thousands, of third-party vendors for a variety of services. Requiring financial institutions to audit each and every one of these vendors rather than commensurate with their risk profile and the particular contractual relationship, to the extent doing so is even feasible, would not only strain the resources of the covered entities themselves, but also the vendors, as many of them contract with multiple financial institutions.

FSR/BITS members are similarly wary of requiring certain contractual terms to be included in third-party contracts. There is often minimal leverage for the negotiation of vendor contracts, particularly with respect to larger (and potentially more secure) third-party vendors, such as Amazon or Microsoft. Should prescriptive contractual terms be required by the enhanced standards, financial institutions would be forced to contract with those limited number of third parties willing to add such language to their contract. Vendors willing to adopt these terms may not be the most secure or competitive choices for the services, creating inefficiencies and raising potential security risks across the sector.

FSR/BITS encourages the Agencies to consider whether direct application of the standards is possible under the current statutory framework. FSR encourages the Agencies to work closely with other stakeholders, and leverage existing public-private partnerships to identify any necessary changes to authorities. Also, FSR/BITS joins FSSCC in recommending that the Agencies consider allowing financial institutions to rely on widely accepted industry certifications (or a similar industry-wide vetting mechanism) to demonstrate a vendor's

compliance with any enhanced standards. For example, our members subject to oversight as third parties have spoken favorably to us regarding the evaluation process in the FFIEC IT Examination Handbook. [13]

B. Sector-Critical Systems

1. Identifying Sector-Critical Systems

The ANPR defines sector-critical systems as any systems of covered entities that support at least five percent of the value of transactions in critical markets. FSR/BITS joins FSSCC in expressing concern that this represents a new, incomplete, and potentially contradictory definition of sector-critical systems. The focus on transaction values does not account for other risks that particular systems may pose to the entire sector or mitigations that may already be in place. FSR/BITS believes that the identification of sector-critical systems should be driven by a broader risk analysis that considers a variety of risk factors to both covered entities themselves and the role of the functions they perform to the sector as a whole. Further, many systems that are sector critical to the financial sector are beyond the control of financial institutions, such as energy and telecommunications. We urge the Agencies to review existing definitions of sector-critical systems and engage in a collaborative process such as the already-established CIPAC financial sector subgroup to have a fulsome discussion of which systems may qualify as sector critical.[14]

2. Two-Hour Recovery Time Objective ("RTO")

The ANPR proposes a two-hour RTO for sector-critical systems experiencing a cyber attack. Returning sector-critical systems to a functional state as quickly and safely as possible is a laudable goal that FSR/BITS shares with the Agencies. However, establishing an inflexible two-hour RTO timeframe is not only overly prescriptive, but also a potential impediment to security.

The two-hour RTO timeframe could actually compromise sound operational judgment and hinder a risk-based determination of when systems should be restored. Ideal RTO will depend on the type of cyber event, the extent of the damage caused, and the confidence that the attackers' access and any malware or other malicious tools have been successfully eliminated or at least contained. There may be times when two hours is more than sufficient to restore a system's functionality. However, there will also be instances where increased assurance is needed before rushing a system back into operation. Further, recovery often involves coordination with third-party service providers, law enforcement and customers, adding a layer of complexity to the process that can complicate any fixed RTO time frame. Although a service disruption can create negative impacts, the most important duty of a financial institution in a cyber event is the integrity of both our customers' personal information and the financial system as a whole.

---

[13] *See* http://ithandbook.ffiec.gov/.

[14] The Treasury Department is currently undertaking a collaborative review of such systems.

FSR/BITS members' experience with cyber events has demonstrated the danger in rushing systems back to functionality. Haste can generate new vulnerabilities and propagate existing threats, creating new victims on top of the original ones, re-victimizing original targets, and risking the destruction of evidence critical to improving future cyber resiliency and assisting law enforcement in pursuing those responsible for the attack. In addition, the evidence left behind after an attack is critical to improving future cyber resiliency and risk reduction for the targeted institution, as well as the entire cybersecurity community if the intelligence collected on the attack is retained and shared.

Accordingly, FSR/BITS asks the Agencies to allow for financial institutions to create a risk-based set of protocols that can be used to identify appropriate RTO timeframes, with consideration for exploring sector protocols for a return to operations. These factors would consider not only information security by itself, but also broader business considerations that reflect the full range of potential risks to customers, employees, third party partners and other constituents. This approach stands in contrast to a fixed RTO requirement. Further, we reiterate that leveraging our existing private-public discussions would provide an appropriate outlet for financial institutions and the Agencies not only to discuss the right factors to consider, but also to identify methods to improve RTO in the event of a disruption to a sector-critical system.[15]

3. Most Effective Commercially Available Controls Requirement

The ANPR would require that institutions minimize cyber risks to sector-critical systems "by implementing the most effective, commercially available controls." FSR/BITS is concerned with the ambiguity and potential breadth of this requirement. Although we appreciate the intent behind this proposal, it is questionable in practice whether this is either a realistic goal or one that maximizes security.

Firms have spent, and continue to spend, considerable time analyzing, applying engineering and design efforts and staffing technical resources to developing multi-faceted systems. Replacing these systems when a "better" control is available often would be more disruptive than keeping these systems updated, patched and tested regularly. In the same vein, many such systems have undergone detailed integration efforts to work in harmony with one another, such that adding new variables and complexity may improve a "point solution" or capability, but across an integrated platform, they can actually undermine the goal of improving cybersecurity. Second, there is no established mechanism for determining which commercially available control is the most effective. This could lead to financial institutions with sector-critical systems continually purchasing each new commercially available tool for testing to ensure compliance, adding unnecessary cost and diverting security personnel. Third, the requirement assumes that a financial institution is unable to provide an internal solution that is more effective in its own environment than any commercially available control. We urge the Agencies to avoid this prescriptive requirement and adopt a risk-based approach that better

[15] Please also see Roman Numeral III, Subsection G, for a description of the Sheltered Harbor initiative and how it relates to the restoration of account data following a cyber incident rendering a firm no longer operationally viable.

reflects how systems are interconnected and work in concert for determining how best to manage residual cyber risk.

C. Cyber Risk Governance

The ANPR proposes increasing the role of boards of directors with respect to cybersecurity in a manner that strains their historical governance role and would significantly hamper a financial institution's ability to manage cyber risk as an integrated part of its overall risk management efforts. The ANPR proposes requiring an enterprise-wide cyber risk management strategy approved and overseen by the board to a degree that it can challenge management "in matters related to cybersecurity and the evaluation of cyber risks and resilience." To accomplish this, the board would be required to have or have access to expertise on day-to-day cyber risk vulnerabilities to the equivalent of that currently required of management, and particularly those in management with specialized cyber expertise. At the same time, covered entities would be required to establish independent senior leadership with direct access to the board of directors to oversee cyber risk. We support access being available for Boards and cybersecurity personnel. However, FSR/BITS is concerned that a move beyond current guidelines would change the nature of a board's role in a financial institution from oversight to hands-on management and introduce a level of complexity in both prioritization and execution risk that yields little likely upside.

As currently drafted, the ANPR recasts the board in terms of approving protocols. We respectfully submit that this is inappropriate from a governance standpoint and not consistent with the board's role within a financial institution. The FSR/BITS believes that the board's role in ensuring management is adequately addressing cyber risk should be consistent with the board's current oversight role with respect to other types of risk. While the board should be involved in and provide risk management oversight, it should be senior management's role to develop risk management strategies and protocols and to ensure their implementation. Cyber risk is a unique and significant risk to financial institutions, but it is not fundamentally different from other enterprise-wide risks they face. Cyber risk should be managed in a manner consistent with other enterprise-wide risks—with board oversight, not board control.

D. Cyber Risk Management

The ANPR envisions cyber risk management involving three lines of defense, each with independent functions: individual business units; independent risk management with its own line of reporting; and audit. FSR/BITS agrees with the Agencies that these three lines of defense are important to managing a financial institution's cyber risk, and our members have largely adopted such multi-faceted structures for their own cyber risk management. Regarding the specifics of these independent functions, however, we encourage the Agencies to allow firms the flexibility to achieve this goal of independent reporting based on their own risk profile, the organization of their internal business units and independent risk management function, and the audit functions they use for cyber risk management.

Despite wide agreement regarding the overall internal structure for cyber risk management, there are great variations among firms in the details of how these lines of defense are implemented. We understand that cyber issues need to be elevated as necessary, but

institutions require organizational flexibility to effectively meet this goal. As such, FSR/BITS is concerned with the rigid nature of some of the possible requirements suggested in the ANPR. For example, the ANPR would require each individual business unit to maintain or have access to resources and staff able to assist in cybersecurity responsibilities. This approach risks the introduction of inefficiency to an institution's cyber risk management and may strain already limited cybersecurity resources. Additionally, requiring each individual business unit to have its own expertise could place cyber teams in conflict from an operational and implementation perspective. Effective cyber risk management should allow for each business unit to have access to cybersecurity personnel able to assist in their cyber risk management. Accordingly, permitting financial institutions latitude in concentrating resources in a risk-based manner would be preferable.

E. Internal Dependency Management

The ANPR would require covered entities to inventory and continually track all internal assets and business functions supporting the firm's cybersecurity management strategy. As FSR/BITS understands the ANPR, each financial institution would be required to have real-time inventory of internal assets and business functions. Further, they would be required to "track connections among assets and cyber risk levels throughout the life cycles of the assets and support relevant data collection and analysis across the organization." While we agree that it is a best practice for a financial institution to know its information assets and architecture, we are concerned about the feasibility of the proposed standard. Additionally, the requirement would include "current and complete…mappings to other assets and other business functions, information flows, and interconnections." Financial institutions may have hundreds or thousands of internal assets and a complex and dynamic array of business functions, information flows, and interconnections. We recognize the value of the goal that the Agencies hope to achieve, however FSR/BITS members already employ a risk-based approach to managing their internal dependencies, and, as such, concentrate efforts on identifying risk and specific mitigations. We encourage the Agencies to endorse this approach and provide the sector with flexibility in addressing the wide range of factors involved in tracking internal assets and business functions in a practical, efficient manner.

F. External Dependency Management

The ANPR proposes that financial institutions be required to monitor in real-time their vulnerabilities due to external dependencies. Further, the ANPR requires that this monitoring be current, accurate and complete. As addressed above in Section III.A.2, because vendors have differing functions and widely varying degrees of access to systems, each poses different levels of risk. FSR/BITS believes that this is a representative example of how in practice a risk-based approach to cybersecurity is most effective in achieving the objective. We believe this approach is best embodied in a vendor cybersecurity risk management program with guidelines considering the range of factors that allow the institution to group vendors by the nature of the risks they present and to develop due diligence standards, access controls, monitoring, contractual provisions and other protections appropriate to address these risks

Further, because not all external dependencies present equal risk, some will require more constant and diligent monitoring than others. For instance, access controls are often a potential

vulnerability for cyber-attacks. However, a different level of monitoring is necessary for a food vendor as opposed to a cloud storage provider. Whereas real-time monitoring for some third-party service providers may be necessary and practicable, it would be unnecessary and infeasible for others. FSR/BITS encourages the Agencies to adopt a risk-based approach to determining the level of monitoring necessary for each third-party vendor, which would provide financial institutions flexibility in assessing the risks posed (and commensurate level of oversight or mitigations required) by external dependencies.

G. Incident Response, Cyber Resilience and Situational Awareness

The ANPR proposes that financial institutions be able to recover quickly from a catastrophic event by establishing protocols for restoration, including transferring business, where feasible, to another entity or service provider. The financial services industry has been cooperatively working to accomplish these very goals, and to overcome myriad complexities in so doing. Establishing a mandatory standard would disrupt these ongoing efforts, and it would risk not accounting for additional mitigations financial institutions are pursuing. As such, FSR/BITS asks that the Agencies refrain from regulation regarding these particular issues in order to allow the industry to continue its active work and progress in accomplishing these objectives as identified in the ANPR.

Under the auspices of the FSSCC, the Hamilton Series of exercises has been a successful public-private collaboration to improve the cybersecurity of the U.S. financial system, and our collective maturation in these exercise programs and recent collaboration at the most senior levels of government represent real advances in this area, with more needed. As a follow-up, industry participants— firms representing the majority of retail bank and brokerage accounts in the United States—created, as one example the Sheltered Harbor initiative as a voluntary and cooperative program to create the necessary operating standards for restoration of bank and securities firms account data in the event of a catastrophic event wherein all established firm specific resiliency and business continuity planning measures have been exhausted (i.e., an event resulting in firm failure). The industry has moved rapidly in the last year to develop the Sheltered Harbor specific standards for data formats, data encryption and data vaults that would enable this restoration of retail customer account data at another processing plant or financial institution after a major incident. However, such a restoration cannot occur in a matter of hours, but rather several days once the decision has been made that the firm attacked is no longer operationally viable. The process to date has been very dynamic, and as implementation starts, the industry is learning from this experience and advancing the standards as needed. This fast time to market does not yet lend itself to the long change cycles of precise regulation.

H. Quantification of Security Risk

The ANPR proposes the development of a quantitative measure of cyber risk within covered entities. FSR/BITS shares the Agencies' desire to explore methodologies for cyber risk quantification.[16] Before this can be accomplished, however, an agreement on the factors to be

[16] The need for quantification is also shared by NIST, who recently released a draft version of a revised Cybersecurity Framework with the addition of a section on "Measuring and

considered for quantification of risk is required, as there is currently no consensus. While there is currently no way to comprehensively quantify cyber risk, there certainly are merits in discussing and working towards how to quantify it. FSR/BITS members have articulated a desire to work together with the public sector to answer the questions necessary to create an agreed-upon quantification methodology for measuring cyber risk. However, any developed quantitative measure should be used to inform risk-based decision making within firms and not as a tool to enact prescriptive requirements. For example, the ANPR proposes requiring covered entities to "measure (quantitatively) their ability to reduce the aggregate residual cyber risk of their sector-critical systems and their ability to reduce such risk to a minimal level." While this may be an appropriate use for quantitative measurement, that decision should be left to individual firms in a risk-based manner.

***

FSR/BITS and its members remain willing and interested in working together with the public sector to establish effective, risk-based cyber risk management standards. Both financial intuitions and the public sector face significant cyber threats. As fellow practitioners in the cybersecurity field, FSR/BITS members bring a wealth of knowledge that can help regulators understand the environments in which we operate and our technical abilities. Working cooperatively, we can develop effective standards to secure our platforms, institutions and consumers.

Thank you for your consideration of these comments.

Respectfully submitted,

Richard Foster
Senior Vice President & Senior Counsel
for Regulatory and Legal Affairs
600 13th St, NW, Suite 400
Washington, DC 20005
Richard.Foster@FSRoundtable.org

Christopher F. Feeney
BITS President
600 13th St, NW, Suite 400
Washington, DC 20005
Chris.Feeney@FSRoundtable.org

Demonstrating Cybersecurity." NIST Draft Cybersecurity Framework v1.1, at 21, Jan. 10, 2017, https://www.nist.gov/file/344206.