  

February 17, 2017

Robert deV. Frierson, Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue N.W.
Washington, D.C. 20551

DELIVERED VIA EMAIL TO REGS.COMMENTS@FEDERALRESERVE.GOV AND FEDERAL eRULEMAKING PORTAL

Re: Joint Comment on the Enhanced Cyber Risk Management Standards Advance Notice of Proposed Rulemaking, Docket No. R-1550 RIN 7100-AE-61

Board of Governors of the Federal Reserve System:

The undersigned organizations are operators of financial market infrastructures ("FMIs") designated as systemically important financial market utilities ("SIFMUs") under the Dodd Frank Wall Street Reform and Consumer Protection Act of 2010 (the "Dodd Frank Act").[1] We appreciate the work of the Board of Governors of the Federal Reserve System ("Federal Reserve"), the Office of the Comptroller of the Currency ("OCC") and the Federal Deposit Insurance Corporation ("FDIC") (collectively, the "Agencies") to publish a joint advanced notice of proposed rulemaking (ANPR) on enhanced cyber risk management standards. We welcome the opportunity to provide comment regarding these important topics.

Recognizing the importance of these topics and in the spirit of promoting an effective, consistent regulatory regime, we are submitting comments on the ANPR. SIFMUs have great appreciation for the importance of effective cyber risk management. Our organizations dedicate significant time and resources to address ever evolving threats, threat actors and the risks they pose. We appreciate continued efforts to promote a consistent cyber framework.

SIFMUs are already subject to significant regulation and oversight with respect to cyber risks by, as applicable, the Securities and Exchange Commission ("SEC") and the Commodity Futures Trading Commission ("CFTC"). The many various existing requirements, guidance and

[1] In July 2012, pursuant to Title VIII of the Dodd Frank Act, the U.S. Financial Stability Oversight Council ("FSOC") designated as SIFMUs, among other entities: 1) the Chicago Mercantile Exchange, Inc. (in its capacity as a clearing organization) ("CME"); 2) The Depository Trust Company ("DTC"), National Securities Clearing Corporation ("NSCC"), and Fixed Income Clearing Corporation ("FICC"), all of which are subsidiaries of The Depository Trust & Clearing Corporation; and 3) The Options Clearing Corporation ("OCC").

best practices should be harmonized and inconsistent or overlapping regulations should be avoided. Therefore, the ANPR should not seek to include SIFMUs that are not directly regulated by the Federal Reserve and that are subject to SEC and CFTC regulatory oversight.

I. Executive Summary

We support an integrated, risk-based regulatory regime that allows for flexible and dynamic application, and for continuing adaption as technology and best practices evolve. As SIFMUs we are comprehensively regulated, including by primary supervisory agencies that have promulgated regulations addressing cyber risk management. Any regulatory framework addressing cyber security should utilize a risk-based approach regarding the development of cyber security risk management practices and the scope of their application.

The Agencies should reaffirm the primary goal of providing stability to the financial system. The SIFMUs agree that the security of core clearance and settlement systems should be prioritized and balanced with the need to promote the overall operational resilience of those systems. Cyber security presents challenges that may require balancing competing concerns. When designing, for example, due diligence and other monitoring standards, the overall security of an entity's financial system should be taken into account.

We agree with and support the Agencies' emphasis on strong cyber risk governance and management. Entities should be afforded a degree of flexibility in their organizational structure and use of the three lines of defense model so that reporting and governance lines are designed to best promote effective communication of cyber risks and mitigation efforts. Internal and external dependency management are important aspects of an entity's cyber risk management plan, which should reasonably take into account the priority of promoting an entity's overall operational stability and security. Regulators and industry should work together to promote threat information sharing and industry best practices to manage current and future cyber risks.

We request that the Agencies note our issues in the following areas:

1. We encourage a regulatory approach that recognizes that the SIFMU primary supervisory agencies have each prescribed regulations and risk management standards, and seeks to avoid duplicative regulation. The CFTC system safeguards testing rule requires best practices, risk analysis and oversight of key cyber security areas, as does the SEC's Regulation SCI.

2. The best approach is a risk based focus on critical, or core, systems, rather than an enterprise-wide application. Consistent with existing regulations, each entity should prioritize critical, core, or other priority systems, rather than risk diluting their efforts that might not yield commensurate benefits.

3. SIFMU's should not be subject to third-party service provider due diligence conducted by covered entities. Regulators conduct thorough examinations of SIFMUs, which include a review of sensitive cyber security information. Subjecting SIFMU's to private due diligence requirements is duplicative, and could introduce other, unintended security risks into the financial system. Current oversight into the vendor selection and risk process provides Agencies with visibility and oversight into third parties and the critical system support they may be providing.

4. Firms should be afforded flexibility in implementing the three lines of defense risk management framework. Fostering a culture that appreciates the importance of cyber security at every level of an organization is one of the most effective defenses. We believe that regulators should clarify that it is not their intent to suggest that business areas, by themselves, might be able to identify all potential risks or vulnerabilities, and that other risk management professionals may provide guidance or assessments to business units.

5. It is neither practical nor necessary for an entity to continuously monitor "all" internal and external assets and business functions. We believe, in line with current regulatory requirements, risk-based testing is appropriate. We request that the agencies make clear that it is their intent to support risk-based management of cyber risk through appropriately applied controls.

6. Taking into account the important issues of data integrity and validation, the most appropriate recovery point for a cyber event may not be easily determined. We request further discussion on how several factors might inform an appropriate recovery time objective (RTO) to a cyber event based on the facts and circumstances of a given event.

II. Leveraging Existing Supervisory Programs, Regulatory Requirements and Guidance

The ANPR recognizes primary supervisory agencies' existing supervisory programs that have adopted regulatory requirements regarding cyber security practices for both covered entities and their third party service providers, and states that the enhanced standards outlined in the ANPR would be integrated into existing supervisory frameworks. Under the current framework for SIFMUs, the role of primary supervisory agencies is recognized.[2] The SEC and CFTC each prescribe regulations with risk management standards, in consultation with the Federal Reserve, for the designated entities for which each is the primary supervisory agency.[3]

---

[2] *See* Dodd-Frank Wall Street Reform and Consumer Protection Act ("DFA"), Pub. L. No. 111-203, § 803(8), 124 Stat. 1376, 1806-807 (2010).

[3] *See id.* DTC, NSCC, FICC and OCC are all registered designated clearing agencies ("DCAs") primarily supervised by the SEC, and CME, in its clearing capacity as a derivatives clearing organization ("DCO"), is primarily supervised by the CFTC; *note* DTC, as a New York Limited Purpose Trust Company and state member bank of the Federal Reserve System, is also subject to supervision and examination by the New York State Department of Financial Services and

Under this regime, the Federal Reserve is consulted before the primary supervisory agency takes action on proposed changes by SIFMUs to their rules, procedures or operations that are subject to advance notice requirements. The Federal Reserve, at its discretion, also participates in supervisory examinations.[4] SIFMUs, as a result, are already subject to comprehensive supervisory and prudential oversight.[5]

The CFTC and the SEC, as primary supervisory agencies for DCOs and DCAs respectively, have both finalized comprehensive rules addressing cyber security. The CFTC system safeguards testing rule requires DCOs to maintain a best practices based program of risk analysis and oversight that at a minimum addresses key cyber security topic areas.[6] The CFTC rule also requires annual completion of an enterprise technology risk assessment ("ETRA"), vendor risk management, controls testing and independent internal audit reviews, and regular, effective governance both by senior management and a DCO's Board of Directors.[7] Likewise, the SEC's Regulation SCI requires DCAs to adopt policies and procedures informed by best practices and standards to address key "domains", or examination areas, taking into account a risk based approach.[8]

The ANPR notes that its intent is to be complementary to existing guidance, best practices and standards, and we welcome that approach. The proliferation of cyber security

---

the Federal Reserve Bank of New York under delegated authority from the Federal Reserve. As such, it would be directly covered by the proposals laid out in the ANPR. *See also* Regulation HH, 12 CFR Pt. 234 (2017) (sets forth risk-management standards governing the operations related to the payment, clearing, and settlement activities of SIFMUs and expressly excludes "a designated financial market utility that is a derivatives clearing organization registered under section 5b of the Commodity Exchange Act (7 U.S.C. 7a–1) or a clearing agency registered with the Securities and Exchange Commission under section 17A of the Securities Exchange Act of 1934 (15 U.S.C. 78q–1), which are governed by the risk-management standards promulgated by the Commodity Futures Trading Commission or the Securities and Exchange Commission, respectively, for which each is the Supervisory Agency".)

[4] DFA §§ 806(e)(4) and 807(d).

[5] *See* DFA § 805. Each of undersigned are subject to comprehensive regulatory oversight designed to ensure that we are prepared to respond to a wide variety of extreme but plausible potential crises, including cyber-attacks.

[6] *See* 17 CFR § 39.18 (2017) (requiring that DCO's program of risk analysis and oversight address: 1) information security; 2) business continuity and disaster recovery planning and resources; 3) capacity and performance planning; 4) system operations; 5) systems development and quality assurance; and 6) physical security and environmental controls.)

[7] *Id.*

[8] *See* Regulation Systems Compliance and Integrity ("Regulation SCI"), 79 Fed. Reg. 72,251, 72,302 (Dec. 5, 2014) (requiring DCAs to address systems capacity, integrity, resiliency, availability and security through nine domains, namely: 1) application controls; 2) capacity planning; 3) systems development methodology; 4) information security and networking; 5) computer operations and production environment controls; 6) contingency planning; 7) audit; 8) outsourcing; and 9) physical security.)

guidance has the potential to unintentionally introduce inconsistencies and redundancies as entities consider and manage multiple frameworks. The ANPR discusses some of the sources of guidance regarding cyber security that are regularly used to communicate general expectations and best practices, including: the Federal Financial Institutions Examination Council (FFIEC); the FFIEC Cyber Security Assessment Tool; the Interagency Guidelines Establishing Information Security Standards; the National Institute of Standards and Technology (NIST) Cybersecurity Framework; the Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System; and the recently published June 2016 Committee on Payments and Market Infrastructures (CPMI) and the Board of the International Organization of Securities Commissions (IOSCO) Guidance on Cyber Resilience for Financial Market Infrastructures. There are many other domestic and international sources of cyber and related guidance, including those published by the International Organization for Standardization (ISO), and the recently proposed regulations from the New York State Department of Financial Services ("NYSDFS").[9]

The process of considering and tailoring different best practices encourages entities to evaluate their own risks from different informed perspectives. The CFTC, SEC, CPMI-IOSCO and others have noted that permitting entities to consider which best practices are suited to their risk profiles helps them to adopt the most effective policies, procedures and controls.[10] An entity may reasonably determine, taking into account its own risks, which aspects of different standards might best be suited to those risks, or that a standard or practice is either not applicable or does not provide a meaningful mechanism to mitigate an identified risk.

Further, the existing supervisory framework for SIFMUs recognizes the importance of adopting a risk based approach to addressing cyber security. Each SIFMU must itself evaluate its own risks, informed by several factors including the nature of the critical financial services it provides, its operational capabilities and infrastructure, and the threats it faces. Overly prescriptive regulations will likely become outdated and less effective, especially given the speed with which technological advancements are made and how quickly the associated threat landscape changes.[11] Standards and best practices evolve over time, and often outpace changes in regulations.

---

[9] *See* 23 NYSDFS, 23 NYCRR 500 (proposed Dec. 28, 2016), *available at* http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf (NYSDFS proposed cyber security requirements, currently scheduled to go into effect March 2017, which add a separate, and in some cases, unique set of requirements. These requirements address the covered entity's risk assessment, covering both internal systems, customer data, data breach notification, and third party vendor oversight, along with new technical controls and an annual certification by a corporate officer that all the requirements have been met.)

[10] *See* Regulation SCI, 79 Fed. Reg. at 72,302 79 FR 72302 (Dec. 5, 2014) (SEC Regulation SCI final rule preamble noting that entities may design their policies and procedures taking into many different best practices and standards); *see also* System Safeguards Testing Requirements for Derivatives Clearing Organizations ("Regulation SST"), 81 Fed. Reg. 64,321, 64,323 (CFTC System Safeguards Testing final rule for DCOs permitting flexibility).

[11] *See* Regulation SCI, 79 Fed. Reg. at 72,300 ("The [SEC] agrees that, in an industry that relies heavily on technologies that are constantly evolving, the prescription of hard-coded solutions that may become quickly outdated is not the better approach"); *and* Regulation SST, 81 Fed. Reg. at 64,325 (explaining that the final rule

The existing supervisory framework should continue to be adaptive. We encourage a regulatory approach that will leverage the current regulations promulgated by primary supervisory agencies that require the adoption of policies and procedures based on best practices and guidance. We recommend against more prescriptive standards that may address aspects of a current situation but often fail to allow flexibility to address changes to the cyber threat landscape. Using policy statements and/ or guidance that will be understood as best practices, or form a baseline of accepted practices is a flexible, highly effective approach that allows entities to maintain resilient cyber defenses as cyber threats continue to evolve.

III. Scope of Application

A. *Risk Based Focus on Critical Systems v. Enterprise Wide Application*

The ANPR considers applying enhanced cyber risk management standards on an enterprise-wide basis to covered bank holding companies because the Agencies argue "cyber risks in one part of an organization could expose other parts of the organization to harm." The Agencies should consider an approach consistent with existing regulations, best practices and guidance that recognize the value of a risk based approach, focusing on critical or "core" systems versus ancillary ones. For example, the SEC's Regulation SCI permits DCAs to segregate their environments to limit the scope of the regulation on a risk basis.[12] Similarly, the CFTC's final system safeguards testing rule adopted a risk based approach that enabled DCOs to focus their efforts and capabilities on their highest risk systems and applications.[13] Adopting this type of risk based approach will encourage entities to take tailored actions to improve their overall cyber resilience, which might include, as an entity deems appropriate, segregating systems and focusing cyber defense efforts where most impactful. An overly broad approach should not be adopted because it would have the unintended consequence of causing entities to dilute their efforts and incur outsized costs that do not yield commensurate benefits.

The ANPR asks which criteria the Federal Reserve should consider in exempting subsidiaries of an enterprise from its enhanced cyber risk management standards. First, to avoid creating overlapping and potentially inconsistent standards, SIFMUs should not be included as covered entities. Second, in line with current regulatory requirements, entities best know their own infrastructure and networks, and are in the best position to evaluate the risks they face. Through a risk assessment process, entities themselves should identify which parts

---

was designed to allow DCOs flexibility in adapting their programs to current industry best practices, which the Commission recognized would evolve over time). *See also* CPMI IOSCO GUIDANCE ON CYBER RESILIENCE FOR FINANCIAL MARKET INFRASTRUCTURES 7 (2015), *available at* http://bis.org/cpmi/publ/d138.pdf ("Guidance requiring specific measures today may quickly become ineffective in the future.")

[12] *See* Regulation SCI, 79 Fed. Reg. at 72,277-279.

[13] *See* Regulation SST, 81 Fed. Reg. at 64,325.

of their business should be subject to enhanced standards. For example, entities should consider the degree to which a control area supports a function critical to fulfilling core regulated clearance and settlement activities. Entities might also prioritize customer facing, external networks, systems or applications.

B. Third-Party Service Providers

The ANPR also asks whether third-party service providers to covered entities should be directly regulated and subject to the ANPR's enhanced cyber risk management standards. As an alternative it asks what the advantages and disadvantages are of requiring covered entities to maintain appropriate service agreements or otherwise receive services only from third-party service providers that meet the enhanced cyber risk management standards with regard to the services provided. The ANPR notes that the Federal Reserve is considering requiring that services be subject to the same standards that would apply as if the services were being conducted by the entity itself.

Clearing houses are already subject to robust regulatory frameworks and supervisory oversight. Regulators conduct thorough examinations of SIFMUs, including by reviewing and questioning the most sensitive security related information. A requirement that covered entities themselves conduct due diligence on SIFMUs as third party service providers results in, at best, duplicative review of control environments by private entities. The process often also has the unintended consequence of creating security risks. For example, regulated entities subject to current third party service provider due diligence requirements often ask SIFMUs detailed questions about highly sensitive cyber security testing, including penetration testing results, and require the disclosure of sensitive information to continue business relationships. In addition to the security risk it creates, the third party service provider due diligence process is widely regarded as a labor intensive, inconsistent process that creates significant costs for the industry as a whole. Clarification that covered entities should not conduct due diligence on DCOs and DCAs as third party service providers would both remove unnecessary security risk from the financial system and eliminate some of the cost of conducting private entity due diligence assessments that are less effective and not as in depth as the requisite federal regulatory examinations of SIFMUs.

The Agencies should make clear that financial institutions subject to the Gramm-Leach-Bliley Act (GLBA) do not need to conduct due diligence on DCOs and DCAs. Further, when a covered entity conducts third party due diligence a risk based approach that also takes into account the overall operational risk of not being able to secure a service from a particular entity would be appropriate. Certain vendors are uniquely able to provide their service. Power and utility companies are unlikely to allow financial institutions to audit their services on a granular level, and often provide services that are unavailable from other equally reliable vendors.

IV. Sector-Critical Systems

The ANPR discusses requiring covered entities with sector critical systems to substantially mitigate the risk of a cyber disruption to those systems. In addition to firms that consistently clear or settle at least five percent of the value of transactions in that critical market, the ANPR considers whether systems that support the clearing or settlement of at least five percent of the value of transactions in other markets, i.e. exchange traded and over the counter derivatives, should be considered sector critical systems. The ANPR discusses considering additional factors like substitutability and interconnectedness when identifying sector critical systems. It questions whether firms should report their sector critical systems to agencies. Finally, the ANPR notes that any services provided by third parties that support a covered entity's sector critical systems would be subject to the same sector critical standards.

Focusing on sector critical standards is consistent with a risk based approach. Firms are capable of leveraging their existing enterprise risk management capabilities to identify the systems that present the most risk to their firms and customers. Current standards, like the CPMI-IOSCO guidance, articulate the expectation that a firm's Board of Directors and senior management oversee a firm's risk tolerance regarding its most critical systems. Adopting an approach consistent with current regulatory requirements, for example the SEC Regulation SCI's requirement to identify critical SCI systems, would allow the Federal Reserve to leverage the existing supervisory framework and provide additional guidance regarding the factors firms might consider in identifying their sector critical systems. As a participant in supervisory examinations, the Federal Reserve would have the ability to review the processes and governance over a firm's identification of sector critical systems. Engaging with the industry in this way has the benefit of allowing the Federal Reserve to both continue a dialogue as best practices evolve and avoid the unintended consequence of centralizing risk with regulators if lists of all industry sector critical systems are provided to and stored by regulators in a single location.

A consistent risk based approach would also have the benefit of allowing the industry to focus their efforts on those systems that are subject to the most risk. The ANPR notes that any services provided by third parties that support sector critical systems would be subject to the same standards. The Federal Reserve should clarify that it intends that firms complete risk assessments of the criticality of third party services to sector critical systems. The criticality of the service would in turn determine the degree to which those services must be subject to enhanced standards. Firms might also reasonably decide after completing a risk assessment that a third party service is not critical to a system, and as a result, might be exempted from an enhanced standard.

V. Enhanced Cyber Risk Management Standards

The ANPR organizes discussion of its enhanced cyber risk management standards into five categories. It places an emphasis on cyber risk governance and cyber risk management, and also discusses the management of dependencies, incident response, situational awareness and cyber resilience.

A. *Risk Based Cyber Risk Governance*

We agree that effective cyber risk governance is an important aspect of a firm's efforts to improve its operational resilience and reduce negative impacts from a cyber attack. We appreciate that the ANPR recognizes that each entity should determine its own appropriate level of residual cyber risk. Developing and maintaining a written cyber risk management strategy, reviewed at the Board of Directors level and supported by a framework of implementing policies and procedures, is consistent with existing risk based regulatory requirements.[14] Firms should continue to focus their efforts through well informed, risk based decisions, and address their infrastructure in a way that enables them to appropriately reduce their residual cyber risk. Given the practical realities of cyber threats, no firm should be expected, regardless of its commitment or resources, to be able to completely mitigate residual cyber risk.

The Agencies should focus any regulatory proposal on the ability of a Board to access information to support the effective governance of cyber security risks, and not on the composition of a Board. The ability for the Board of Directors to provide reasonable and credible challenge[15] to a firm's cyber security risk management strategy requires the Board to have access to resources with the requisite knowledge of cyber security risk management *and* business operations. Directors must consider all firm obligations, including responsibilities to complete critical clearance and settlement functions. Maintaining a strong cyber security posture most often complements and supports operational needs, but the totality of a firm's responsibilities must be taken into account.

As a result, and in line with existing regulations, firms develop cyber risk management strategies in line with their size, complexity of operations, customers and counterparties, and market interconnectedness. Similarly, the composition of a firm's Board of Directors should be tailored to its own individual risks, which foreseeably will evolve over time. The quickly evolving cyber threat landscape especially will likely outpace the membership election cycle for most boards. Acquiring current and informed expertise regarding the cyber threat landscape is an exercise that calls for flexibility and resourcefulness. This reality makes it all the more important that the Agencies recognize that a board may effectively access the appropriate information and knowledge necessary to provide reasonable and credible challenge to a firm's cyber security risk management strategy in varied ways. For example, as recommended and permitted in the FFIEC Audit IT Examination Handbook, a board may obtain external training in any given area.[16]

---

[14] *See* Regulation SST, 81 Fed. Reg. at 64,326. We would, however, welcome additional discussion regarding the "substantial mitigation" of cyber risk standard, which foreseeably may be inconsistently applied by both regulators and industry.

[15] *See generally* 12 CFR pts. 30 & 170 (Sept. 2, 2014) (known as the OCC "Heightened Standards", which require that a Board of Directors provide "credible challenge" to management's recommendations and decisions).

[16] *See* FFIEC, AUDIT IT EXAMINATION HANDBOOK (Apr. 2012) *available at* http://ithandbook.ffiec.gov/it-booklets/audit.aspx.

Finally, the ANPR also discusses the view that senior leaders with responsibility for cyber risk oversight should be independent of business line management. It states that entities would be required to include in their framework delineated cyber risk management and oversight responsibilities for the organization, including reporting structures and expectations for independent risk management and internal audit personnel. We agree that both second line risk management and third line internal audit personnel have important, complementary roles in supporting a firm's cyber risk framework. Firms should be allowed flexibility in designing their framework, including reporting structures. We would welcome additional clarity and discussion regarding how the three lines of defense should support effective governance.

B. *Flexibility and Clarity Regarding Cyber Risk Management Frameworks*

The ANPR discusses the intent of the Agencies to develop a rule that would require covered entities "to the greatest extent possible and consistent with their organizational structure" to integrate cyber security risk management into the responsibilities of at least three independent functions, or lines of defense. We agree that fostering a culture that appreciates the importance of cyber security at every level of a business is one of the most effective cyber defenses.

Allowing for flexibility on how the three lines of defense model is implemented within covered organizations, in line with a firm's overall cyber risk management framework, would allow for adoption of models most capable of addressing a firm's profile, organizational structure and the various businesses it provides. Regulators should take into account the effective variations that firms employ in designing the roles and responsibilities of their first, second and third lines of defense frameworks. Providing clarity on expectations for how the three lines of defense might complement one another in a notice of proposed rulemaking would allow industry to provide additional feedback on how firms employ effective overall controls frameworks. We would welcome additional discussion on the agencies' views on the roles and responsibilities of the first, second and third lines of defense.

1. The First Line of Defense: Business Units

The ANPR discusses the intent to require the first line, or units responsible for the day-to-day business functions of a covered entity, to continuously assess cyber risks. The first line would be responsible for sharing information regarding such risks with senior management, including the chief executive officer (CEO). Business units would assess the risks and potential vulnerabilities associated with "every business asset, service and IT connection point."

Requiring the first line to assess its own cyber risks and potential vulnerabilities for every business asset, service and IT connection point may not be the most effective way to promote a strong risk based three lines of defense model. Completing, evaluating and interpreting cyber risk assessments often requires specialized expertise that would not likely be

consistently present in the first line of defense. As a result, requiring the first line to report cyber risks to senior management, including the CEO, may have the unintended consequence of inhibiting effective communication of a firm's cyber risks. Without the expertise to contextualize and interpret risk assessments, the first line reporting on cyber risks may make it more difficult to understand a firm's risks and prioritize the correct efforts. Regulators should clarify that it is not their intent to suggest that business units might be able to identify all potential vulnerabilities.

2. The Second Line of Defense: Compliance and Risk Management

Firms might use their existing second line of defense independent risk management professionals to provide guidance to, or conduct risk assessments of, the first line of defense. Some risk assessments might be done effectively through first line of defense self-assessments that are evaluated by an independent second line of defense. Other qualitative assessments are only meaningful if completed by independent risk professionals with the requisite expertise to conduct them. While it is imperative that the business areas understand and make decisions taking into account cyber security risks, an independent risk management function may conduct risk analyses of threats to technology assets and services, and provide the first line business areas with the information necessary to make informed decisions on these risks.

A second line risk function might also report to senior management, including the CEO, or in certain organizational structures to a Board of Directors governance body. Such reporting might include, for example, those risks where: 1) if realized may result in a material impact to the organization; or 2) the organization is operating outside of its defined risk tolerance. Firms should develop procedures suited to their needs that appropriately enable senior management and Board level governance over cyber risk management by taking into account frequency of reporting, reporting thresholds and alignment with the organization's risk reporting mechanisms.

Many firms also use second line of defense regulatory compliance professionals to assess and report on compliance with applicable laws, regulations and related guidance. Compliance personnel, in addition to assessing the business' adherence to laws and regulations, will also often implement internal controls based on best practices that are designed to address risks posed to the firm. Firms take into account risk assessments, testing and other inputs to appropriately focus their control efforts; they appreciate that not every business asset will present risk to a firm's clearance and settlement mechanisms. Diverting attention from the more critical pieces of a firm's infrastructure is less effective than prioritizing efforts on a risk basis.

The ANPR's enhanced cyber risk management standards regarding controls for sector critical systems suggest that firms should use commercially available controls. While additional clarity regarding the Agencies' intent would be welcome, generally we would note that firms should not be required to avail themselves of commercially available controls. NIST, ISO and other publishers of best practices and standards provide widely available, government

sponsored controls libraries.[17] Limiting firms to commercially available controls would limit an entity's ability to design the most effective controls framework for its environment by choosing from all available best practices and standards.

3. The Third Line of Defense: Internal Audit

The Agencies are considering explicitly requiring "the audit function to assess whether the risk management framework of a covered entity complies with applicable laws and regulations and is appropriate for its size, complexity, interconnectedness and risk profile." We agree that the third line of defense, or a firm's internal audit function, has an important role in assessing a firm's cyber risk management. The third line of defense must have an effective, independent reporting line to senior and board level governance bodies. Internal audit activities, conducted in line with auditing standards, may provide assurance that first and second line of defense processes are adequately and effectively applied against defined business and risk management objectives to meet the standards set by applicable laws and regulations.

Audit plans should take into account risk assessments and other information to include appropriate coverage of a firm's security lifecycle. Testing the entire security lifecycle in every audit plan would likely yield limited benefits and would divert attention and resources away from higher risk, sector critical functions. Developing a risk based audit plan, however, would allow internal audit to test the effectiveness of the first and second lines of defense.

C. Risk Based Management of Internal and External Dependencies

Internal and external dependency management standards should continue to be risk based. An entity's cyber risk management strategies should be focused on business assets, including an entity's workforce and technology,[18] upon which the entity depends to deliver core, critical services. The overall strategic risk management plan should guide decisions regarding where to focus efforts to address an entity's own business assets.

The ANPR discusses both a continuous monitoring standard implemented on an enterprise wide basis to "ensure" entities identify cyber risks, and maintaining "current" and "complete" awareness of "all" internal and external assets and business functions. Within this

[17] *See* Regulation SCI, 79 Fed. Reg. at 72,299-303 (SEC adopting a flexible approach regarding best practices and standards).

[18] The ANPR discusses the scope of business assets including a firm's workforce, technology and its data. While a firm's workforce and technology are themselves capable of actions that might either mitigate or contribute to cyber risk, data is the representation of information within a system. Data may be the focus of efforts made by actors, utilizing technology, but it is itself not capable of action. Risk management plans may discuss the role of different business assets in protecting data, but there should not be the expectation that the data itself engages in different mitigating efforts.

context, it discusses continuous application and monitoring of appropriate controls. Firms employ systems of controls to address their inherent risks, and we agree that they should continue to apply appropriate controls on a regular basis and to a reasonable degree. An effective system of controls will likely employ evolving controls specifically designed to manage external dependencies. A firm should take opportunities, for example during contract renewals, to review its management of external dependencies.

Like other related efforts and in line with current regulatory requirements, however, the application and testing of controls should be risk based.[19] Complex, global firms often operate multiple logically and physically separate systems that support different infrastructures within which not all functions are of equal importance. The ability to create segregated sector-critical systems and apply organization resources and controls to these systems may increase the effectiveness of risk management and controls by scoping risk and compliance activities to critical infrastructure. As a result, continuous monitoring of every control as applied to every asset is not required for a firm's overall risk management strategy to be effective.

No control regime will be able to completely mitigate every cyber risk, exception or policy violation. Focusing on critical systems allows both firms and regulators to prioritize efforts in a way that addresses the risks that have the most potential to cause operational issues for systems that support systemically important services. A risk based approach therefore has the best chance of improving the resilience of the overall financial system. The agencies should make clear that it is their intent, in line with current regulatory requirements, to continue to support risk based management of cyber risk through appropriately applied controls.

Similarly, the agencies should clarify that it is also their intent that firms be expected to understand dependencies to a reasonable degree, not that firms attempt to map or test every possible contingency. We agree that evaluating the criticality of different business assets or external dependencies to the functionality of a firm's services is a common practice that enables effective risk management practices. Even without taking into account cyber risk, there are practical limitations on the degree to which firms are able to map dependencies. For example, regardless of how thorough testing and development work may be, implementing changes in the production environment may result in unintended consequences. These unforeseen situations are often the combined result of the change coupled with other technical circumstances that trigger applications to react in new ways.

---

[19] *See generally* FFIEC, SUPERVISION OF TECHNOLOGY SERVICE PROVIDERS, IT EXAMINATION HANDBOOK (Oct. 2012), *available at* http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_SupervisionofTechnologyServiceProviders(TSP).pdf; DIVISION OF BANKING SUPERVISION AND REGULATION, DIVISION OF CONSUMER AND COMMUNITY AFFAIRS, BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, GUIDANCE ON MANAGING OUTSOURCING RISK (2013), *available at* https://www.federalreserve.gov/bankinforeg/srletters/sr1319a1.pdf; *and* OFFICE OF THE COMPTROLLER OF THE CURRENCY, OCC BULL. NO. 2013-29, THIRD PARTY RELATIONSHIP RISK MANAGEMENT GUIDANCE (2013), *available at* https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html.

The ANPR discusses a proposed requirement that covered entities "identify and manage real-time cyber risks associated with external dependencies, particularly those connected to or supporting sector-critical systems and operations." The continuous monitoring of these dependencies is not feasible.

While firms may reasonably monitor connection points to external dependencies and understand their own dependency on external vendors or services, requiring firms to have a "current, accurate, and complete awareness of...all external dependencies and trusted connections enterprise-wide" may have unintended consequences.[20] First, firms often rely on services available only from power and telecommunications utilities providers that are considered critical infrastructure. Real time monitoring of their control environments by numerous external firms would create security concerns for utilities that provide services not only to the U.S. financial system, but to other critical sectors, and even the U.S. federal government. Second, as noted above in the discussion of vendor services, the Agencies should make clear that SIFMUs should not be considered external dependencies for which covered entities would need to conduct external dependency management. Requiring covered entities to attempt to conduct continuous monitoring of SIFMUs would create security concerns and would be at best a duplicative exercise. Third, by creating regulatory requirements addressing external dependency management that cannot by their nature be met, firms may be forced to rely far less on external service providers. Some firms may be pressured to seek out external service providers that may be able to meet the regulatory requirement but cannot offer the same level of the core, operational service. Other firms may forego technical advances offered by external service providers or vendors that could provide an overall improvement in their cyber resilience because they cannot meet unnecessarily high regulatory standards. Fourth, certain services, like cloud services, may be important to several systemically important firms and better provided to the industry as a whole by external firms. If multiple firms must develop those services internally, instead of allowing each firm to avail itself of the best expertise and capabilities, some firm's internally developed capabilities will not meet the same standard.

Understanding a firm's dependencies and developing resiliency are complementary exercises. Firms should plan to mitigate to a reasonable degree inevitable technical issues, regardless of whether they are caused by cyber threats. The practical realities discussed above illustrate why internal and external dependency management cannot on their own address a firm's inherent cyber risks. Developing a firm's own resiliency, including by testing back-ups and other forms of redundancy, is a key and complementary way of mitigating inevitable technical issues. Systemically important firms regularly engage many different types of testing to improve their resiliency, including back-up testing and disaster recovery exercises.

---

[20] The Agencies also requested input on the impact that a two hour recovery time objective ("RTO") would have on third party service provider utilized by a covered entity to provide critical systems. For similar reasons as discussed here, the enforcement of a two-hour RTO may remove the ability to the covered entity to use certain vendors or other industry-best technology services.

The ANPR discusses that the agencies are considering requiring identification and periodic testing of alternative solutions in case an external partner fails to perform as expected. Some scenarios involving the unavailability of an external partner may be taken into account when firms address geographic dispersal disaster recovery requirements, but it would be unrealistic or even potentially destabilizing in certain situations to attempt to unilaterally identify viable alternative solutions in case a common industry external partner fails to perform. Cyber exercises like the Hamilton Exercises sponsored by the U.S. Department of the Treasury allow industry participants and government bodies to discuss potential cross sector impacts, and the roles and responsibilities of different entities. Entities like FS-ISAC and FSARC promote related industry wide dialogue. The Agencies should seek to promote additional participation in such exercises and information sharing organizations to foster cross sector dialogue in lieu of attempting to require each firm on its own to attempt to identify alternative service providers.

D. Incident Response, Cyber Resilience and Situational Awareness

Strong and tested incident response capabilities must be part of every firm's cyber risk management strategy. Situational awareness and threat analytics are an important part of a firm's overall cyber defense posture.

Every day, firms operate their critical business functions and successfully defend against cyber-attacks. Not every cyber threat or attack has the potential to cause the same level of operational disruption. While most threats or attacks are manageable, the Agencies should not expect that firms will be able to "reliably predict" every change in its operating environment.[21] There may be escalated threat scenarios when firms should consider whether halting operations is preferable to prematurely performing certain business functions. For example, a sophisticated actor might successfully exploit a zero day vulnerability present in the systems of multiple firms and attempt to destabilize U.S. markets by causing cross sector data integrity issues. In such a scenario, firms may decide that it is preferable to confirm the integrity of data and develop a patch to the vulnerability before completing certain processes. Likewise, if the power or telecommunications utilities were operationally impacted by cyber-attacks, in an extreme scenario each firm may decide that it is preferable to temporarily pause operations and disengage from its external connections rather than also falling victim to a sophisticated and orchestrated attack that would cause long term damage to its operations or the marketplace.

The agencies should not ask each covered entity to unilaterally identify and mitigate the cyber risks they pose through interconnectedness to sector partners and external stakeholders to prevent cyber contagion. It is well known that cyber warfare directed at the United States is not limited in its scope to only government systems. Cyber threat actors can include

[21] Such a standard may be difficult to meet and a challenge to interpret. It is not clear how a reliability standard would be consistently measured, especially taking into account the unique challenges of managing cyber threats.

sophisticated, well-funded multi-national organizations or even other nation states. Industry exercises, and organizations like FS-ISAC, FSARC and others, provide forums that can help identify such connections and dependencies and give firms needed information to enable them to mitigate threats.

The ANPR anticipates a proposal to require entities to transfer business to another entity or service provider within prescribed time frames and with minimal disruption. It discusses implementing defined data standards in order to increase the substitutability of third party relationships to reduce recovery times for systems impacted by a significant cyber event, and implementing data recovery point objectives. DCOs and DCAs are already required by existing regulations to be able to address the failure of their largest clearing member, and SIFMUs must meet a higher standard. SIDCOs, through their own rules, are capable of transferring certain clearing member business to another firm. Each DCO or DCA's staff is best qualified to understand its systems, confirm system integrity and provide for operational continuity. Historically, regulatory attempts at defined data standards, especially regarding formatting, have soon become outdated and have created burdens on financial firms that do not yield commensurate benefits.[22] Attempting to implement data recovery point objectives would be challenged by the inconsistencies in the clearance and settlement processes across the equities, derivatives and banking sectors. The agencies should instead focus on incident response planning and situational awareness developed in part through information sharing.

VI. RTO Standards for Sector-Critical Systems of Covered Entities

The ANPR discusses a proposal to require covered entities to establish a two hour RTO for sector-critical systems, validated by testing. It notes that the scope of the application of the proposal may extend beyond core clearing and settlement organizations. The CPMI-IOSCO Guidance on Cyber Resilience for Financial Market Infrastructures recently published guidance on FMI cyber security resiliency, including significant discussion of the two hour recovery time objective.[23] CPMI has previously recognized that, given the infinite variety of possible scenarios (including the potential of state actors), it is not possible to confirm that a two hour RTO could be met in every situation. Further, a two hour RTO is not necessary for all types of FMIs. The focus instead should be on the ability to resume operations as quickly as possible consistent

[22] Firms do, however, have current record keeping regulatory requirements.

[23] *See* CPMI-IOSCO, GUIDANCE ON CYBER RESILIENCE FOR FINANCIAL MARKET INFRASTRUCTURES (2016), *available at* https://www.iosco.org/library/pubdocs/pdf/IOSCOPD535.pdf (recognizing that, given the infinite variety of possible scenarios, including the potential of state actors, it is not possible to confirm that a two hour RTO could be met in every situation, and that a two hour RTO is not necessarily for all types of FMIs). FMIs should be able to continue to prioritize their systems and processes in terms of criticality, with longer lead times for services that would not immediately impact critical market activities.

with safe and sound operations.[24] FMIs should be able to prioritize their systems and processes in terms of criticality, with longer lead times for services that would not immediately impact critical market activities.

In comments to the CPMI-IOSCO guidance, the SIFMUs noted that with respect to cyber disruptions the RTO is properly a concrete goal in designing BCM policies and procedures, and not an inflexible regulatory requirement that must be met in all recovery circumstances irrespective of the nature or extent of the disruption. The original recovery discussion in the PFMI was focused on physical disruptions. Unlike cyber events, physical events have a known starting point and, in most cases, an easily predictable and dimensional impact.

Cyber recovery, on the other hand, is fundamentally different. A cyber event will not always lead to an outage or disruption. To apply a two hour RTO necessarily implies the determination of a "recovery point" from which the recovery time would be measured. In the case of a disruption, that could only reasonably commence after the point of detection and identification, which often doesn't happen for an extended period of time. For example, the median time between a data breach and its detection is over 146 days.[25] Effective recovery may depend on taking reasonable steps to prevent inadvertently leaving weaknesses in place that adversaries might immediately exploit again. Elimination and containment failures might allow portions of a compromise to remain on the organization's systems, causing further damage without the adversary even acting.[26] Further, FMIs were required to incorporate the use of secondary sites with IT systems designed to enable resumption of operations within 2 hours following disruptive events. The means by which most FMIs have addressed this requirement is by utilizing geographically diverse sites with systems replicating processing data and instructions. While this facilitates timely resumption of operations following physical events, the structure may make recovery and resumption following a cyber-event more challenging.

Regulatory authorities that have confronted recovery issues have recognized these difficulties and appropriately acknowledged that the recovery time objective is properly a goal, rather than a requirement to be met in all circumstances. Equally important, they have also recognized the appropriateness of prioritizing recovery time objectives in terms of critical systems. For example, the SEC in Regulation SCI required two hour resumption of "clearance

---

[24] *See supra* note 24, at 2 ("Notwithstanding this capability to resume critical operations within two hours, FMIs should exercise judgment in effecting resumption so that risks to itself or its ecosystem do not thereby escalate, while taking into account that completion of settlement by the end of day is crucial.").

[25] *See* MANDIANT®, M-TRENDS 2016: A VIEW FROM THE FRONT LINES 1 (2016), *available at* https://www.fireeye.com/current-threats/annual-threat-report.html.

[26] *See* NIST SP8010-184 (DRAFT) Guide for Cybersecurity Event Recovery (June 2016), 593-597.

and settlement services."[2] The Regulation SCI Release notes: "The Commission has carefully considered commenters' views and is revising this provision from the proposal to: (i) specify that the *stated recovery timeframes in Regulation SCI are goals, rather than inflexible requirements* [emphasis supplied]; and (ii) provide that the stated two-hour recovery goal applies to critical SCI systems generally." Similarly, the CFTC's system safeguards testing regime requires that they have business continuity and disaster recovery plans with a recovery time "objective" of "no later than the next business day following the disruption." Finally, the Federal Reserve, in adopting Regulation HH, made a similar observation and recognized that it may not be possible at this time for the designated FMU to recover within two hours.

Finally, recovery is not the same as resumption. The capability to resume processing includes any data reconciliation required to address the potential data loss caused by the event, which may be across jurisdictions and time zones. In many cases reconciliation is, or would need to be, performed in concert with the FMI's participants and/or trading platforms in order to re-establish not only data, but specific transactions from a given failure point forward. In such a scenario, data integrity and validation may be competing priorities with the 2 hour RTO.

VII. The Quantification of Cyber Risk

The agencies are seeking to develop a consistent, repeatable methodology to support the ongoing measurement of cyber risk within covered entities. No such consistent, industry wide defendable and agreed upon methodology exists today. Current methods used to measure cyber risks contain both qualitative and quantitative measurements used to estimate the impact that threats may have to the firm's networking environment and business operations. Cyber risk management may provide the business with services to support discussion of the possibility and severity of business impacts by: 1) defining those cyber security risk areas that need to be managed in order to effectively manage risk; 2) aligning the controls required for the delivery of the service; and 3) developing metrics that inform the business how it is managing the risk in the service area. These measurements are often more art than science. The same risk factors that make each organization unique (i.e. size; complexity of operations; sensitivity of data; products and services; and market interconnectedness) limit, if not remove, the feasibility of a pure quantification of cyber risk.

A requirement to quantitatively measure the degree to which a firm reduces the aggregate residual cyber risk of their systems may also likely detract from the effective communication of cyber risks both to a firm's governance bodies and to regulators. Quantitative discussions often have the unintended effect of focusing attention on numerical

---

[2] *See* Regulation SCI, 79 Fed. Reg. at 72,294 (Regulation SCI requiring two hour resumption of "clearance and settlement services") (citing Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System, 68 Fed. Reg. 17,809, 17,812 (Apr. 11, 2003) (providing that "[r]ecovery-time objectives provide concrete goals to plan for and test against. They should not be regarded as hard and fast deadlines that must be met in every emergency situation.")).

representations themselves instead of the substantive risks that the numbers intend to communicate. Measuring adherence to defined processes and controls is not the same as effectively describing cyber risks. A firm might adhere strictly to their processes, but if their design does not adequately address underlying cyber risks, quantitative reporting might detract from important substantive concerns. Senior management should use risk assessment and controls testing evidence to illustrate broader points to a firm's governing bodies, but assessment or test results provided without context or discussion are far less likely to support effective governance. Finally, quantitative measure of cyber risks will also result in examiners and other regulators comparing firms against inconsistent, firm specific standards. Discussion of best practices is a more consistent, productive way for regulators to engage with industry to assess the individual strength of firm's cyber security frameworks.

VIII. Conclusion

We appreciate the opportunity to comment on the ANPR and your consideration of the views expressed in this comment letter. Together with the regulatory community we share the goal of promoting the stability of the U.S. financial system, including by prioritizing cyber risk management. We welcome the opportunity for further discussions and engagement on the topics raised in this letter. If you have any questions or need further information, please contact the undersigned at the contact information provided.

Sincerely,

CME Group Inc.
/s/ Gil Vega
Managing Director, Chief Information Security Officer

The Depository Trust & Clearing Corporation
/s/ Stephen Scharf
Managing Director, Chief Security Officer

The Options Clearing Corporation
/s/ Jason Stradley
Vice President, Deputy Chief Information Security Officer