February 23, 2016

Committee on Payment and Settlement Systems
Bank for International Settlements
4002 Basel
Switzerland
cpss@bis.org

General Secretariat
International Organization of Securities Commissions
C/ Oquendo 12
28006 Madrid
Spain
fmi@iosco.org

Re: Consultative Report – *Guidance on Cyber Resilience for Financial Market Infrastructures*

Dear Sir or Madam:

The Clearing House Payments Company L.L.C. ("The Clearing House")[1] appreciates the opportunity to provide comments to the Committee on Payments and Market Infrastructures ("CPMI") and the International Organization of Securities Commissions ("IOSCO"), in response to their consultative report titled, *Guidance on Cyber Resilience for Financial Market Infrastructures* ("Guidance"). While The Clearing House is appreciative and supportive of the intent behind the Guidance, there are a number of issues, more fully discussed below, that we believe require further thought and discussion before CPMI-IOSCO finalizes the Guidance.

[1] The Clearing House is a banking association and payments company that is owned by the largest commercial banks and dates back to 1853. The Clearing House Payments Company L.L.C. owns and operates core payments system infrastructure in the United States and is currently working to modernize that infrastructure by building a new, ubiquitous, real-time payment system. The Clearing House is the only private-sector ACH and wire operator in the United States, processing nearly $2 trillion in U.S. dollar payments each day, representing half of all commercial ACH and wire volume. Its affiliate, The Clearing House Association L.L.C. is a nonpartisan organization that engages in research, analysis, advocacy and litigation focused on financial regulation that supports a safe, sound and competitive banking system. Please see The Clearing House's web page at http://www.theclearinghouse.org for additional information.

The Clearing House is also a signatory to, and our comments here are in addition to or supplementary of, the comments in the joint letter submitted by The Clearing House, The Chicago Mercantile Exchange, Inc., ICE Clear Credit L.L.C., The Options Clearing Corporation, and The Depository Trust Company, National Securities Clearing Corporation, and Fixed Income Clearing Corporation, all subsidiaries of The Depository Trust & Clearing Corporation (the "Joint FMI Letter").

Our comments both in the Joint FMI Letter and in this letter are informed by our more than 40 years of experience in operating a large-value funds-transfer system as a significantly regulated entity, including as a systemically important financial market infrastructure designated by the Financial Stability Oversight Council ("FSOC") . We hold leadership positions and are active members of several cyber and financial institution intelligence alliances, including the Financial Services Information Sharing and Analysis Center ("FS-ISAC") and the Financial Services Sector Coordinating Council ("FSSCC"). The Clearing House understands its significant role in promoting a strong and stable financial system, and how cyber resilience is essential for enforcing and maintaining financial stability and economic growth; we take the Guidance seriously and are providing our comments with the hope that they will improve the Guidance in its final form.

I. Executive Summary

The Clearing House recognizes the importance of cyber resilience and the significant risks that cyber-attacks may pose to the financial system if they are not properly managed. We, therefore, strongly support building stronger and more resilient FMIs, and have identified the following set of issues that we believe warrant further analysis and consideration by CPMI-IOSCO before any final guidance is issued:

1. **Proliferation of Standards** – Cyber resilience is a ubiquitous issue that cuts across entities and sectors. Successfully addressing cyber resilience requires actions by individual entities, but equally important it requires coordination and cooperation among and across entities. FMIs, for example, must not only ensure the cyber resilience of their own operations, but also the cyber resilience of their participants, third-party vendors, and others. This requires common taxonomies in order to ensure that all are "speaking the same language" and use of commonly understood yardsticks when it comes to judging the cyber resilience and risks of business partners. The trend, unfortunately, seems to be a proliferation of cyber resilience frameworks, requirements, standards, and guidance. Some are broad baselines, while others are industry or entity-specific. In this instance, the Guidance serves as another industry standard, which in the United States is additive to existing cyber-resilience standards,

such as ISO 27001, NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, FFIEC's *Information Security & IT Handbooks, FFIEC Cybersecurity Assessment Tool* and others.[2]

Given this array of existing standards, it will be important to understand how each relates to the other and whether the Guidance is an independent standard or an "overlay" intended to complement existing standards, . The Clearing House recommends that the Guidance should be limited to only those aspects of cyber-resilience unique to FMIs, while referencing one or more existing standards for "core" requirements common to any entity. Consideration should be given to consolidating standards or improving existing standards, which can help alleviate the complexity associated with how FMIs will prioritize existing requirements, instead of creating an additional standard.

2. **Risk-Based Approach** As each FMI has a different risk profile, the Guidance should allow each FMI to incorporate the requirements based on its own risk profile. A risk-based approach would allow appropriate prioritization of the requirements and the efficient allocation of resources based on each FMI's risk profile.

3. **Development of a Common Baseline** – The Guidance must provide a consistent way to communicate common baselines and maturity posture levels with stakeholders, as each FMI may interpret controls differently. Communication of common baselines and maturity posture levels is essential given the increasing connectedness of the global financial system.

4. **Utility Analysis** –An additional set of standards without a clear nexus to or relationship with existing standards may add additional complexity, administrative burdens, impose additional resource constraints and layer on additional costs that outweigh any benefits from the standard. Before the Guidance is finalized, we believe CPMI-IOSCO should more thoroughly assess the benefits of the proposed guidance through a survey, quantitative impact assessment or other mechanism. A clear understanding of the value added by the Guidance given the plethora of existing standards is needed.

[2] The Federal Financial Institutions Examination Council is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Consumer Financial Protection Bureau (CFPB), and to make recommendations to promote uniformity in the supervision of financial institutions.

To address these issues, The Clearing House recommends that:

1. CPMI-IOSCO fully evaluate the need to add another standard to the existing plethora of standards.
2. The Guidance should provide a clearer perspective on how the Guidance aligns with or complements other industry standards. The Guidance should serve as an overlay template for FMI specific cyber resilience standards, references, applicability, and control sets, instead of serving as an entirely new industry standard.
3. The Guidance should adopt a risk-based approach allowing FMIs to prioritize those aspects of the Guidance that should be considered critical controls versus aspirational controls within the context of the FMI's specific risk profile.
4. The Guidance should provide a consistent and easier way to communicate common baselines and maturity posture level with other stakeholders.
5. The Guidance should be able to be easily incorporated into an FMI's existing enterprise risk management structure.

II. Discussion

Proliferation of Standards

It is not clear whether the Guidance is intended to complement/overlay existing standards with more specific, unique FMI requirements (the overlay concept) or serve as an independent set of requirements for FMIs in addition to the requirements of other standards. Absent such clarification, additional standards result in additional controls and requirements, which only complicate architecture and engineering without adding real value.[3]

[3] The following seven points summarize the main factors regarding how the Guidance diverges from current NIST and FFIEC cyber frameworks:

1. **Lack of Process -** Unlike the NIST and FFIEC frameworks the Guidance does not provide a process for determining how to move toward the desired state.
2. **Lack of Tools to Set a Baseline**– the Guidance s lacking definition of any maturity targets or levels such as those found in NIST and FFIEC standards . Baselines and aspirational targets would show and FMI how far the FMI is from the more advanced requirements in the Guidance.
3. **Definitional Differences** - The Guidance defines fairly complex items such as the "FMI Ecosystem", "Interconnections" and "Situational Awareness" broadly and without consistency to definitions in other frameworks.
4. **Prescriptive in Certain Areas -** The specification of technical control methods and business continuity measures (see 2 hour recovery and Gold disk recovery requirements as examples) makes

An overlay is a set of interpretative statements that further define broader controls or give the controls specific context within a set of business-specific requirements. The Guidance should serve as an overlay template for cyber resilience standards, references, applicability, and control sets unique to FMI business processes, instead of serving as an entirely new standard. Furthermore, the Guidance as an overlay should provide sufficient flexibility that it could be administered within an FMI's existing overall risk management framework. For example the US Office of Management and Budget (OMB) and Federal CIO provide all Federal Government departments with the ability to apply broad guidance in the NIST 800-53 controls and Cyber Security Framework in the context of an "overlay" to their requirements. These overlays are then documented and published to allow each organization to tailor the guidance to their own specific business processes and risks, and to serve as an explanation of the organization's view of the more general controls. The overlay serves as a tool, instead of a prescriptive solution, a model that should be followed here.

Risk-based Approach

Given limited time and resources, and the complexity of cyber resilience issues, it is critical that a risk-based approach be taken in applying any guidance or other requirements. While financial market infrastructures typically have similar risk appetites, they can vary significantly with regard to their risk profiles and consequently where they should focus their attention. In this regard, the Guidance provides little direction or sense of how it should be applied given such risk differentiation. For instance, it is unclear as to whether the Guidance is simply establishing aspirational goals, adding new requirements, or providing a FMI-specific interpretation of broader frameworks such as ISO 27001, NIST's *Framework for Improving Critical Infrastructure Cybersecurity,* FFIEC's *Information Security Handbook*, or others. Because each FMI has a different risk profile, the Guidance should allow each FMI to incorporate the Guidance based on

---

the Guidance prescriptive and does not appear to allow for compensating security controls by the FMI. Both NIST and FFIEC standards are designed to welcome compensating controls and risk management.

5. **Focus on Single Means to an End –** As an example, the concept of detection in the Guidance is based on behavioral factors where both NIST and FFIEC see it as one of a number of factors leading to understanding unauthorized activity.
6. **Separate, Rather than Integrated Processes:** The Guidance brings out situational awareness as its own function, describing it as an information sharing capability whereas both NIST and FFIEC standards regard it as an integral component of other processes.
7. **Addition of Advanced Features without a Current Baseline of Control:** The Guidance adds the recommendation for prediction of cyber threats - an advanced ability. The most common method of prediction compares incoming threat data with an established set of security controls. The Guidance, however, does not provide a way to assess current controls; the use of an outside framework will be required.

its own risk profile, risk-based priorities and applicable risk management frameworks. CPMI-IOSCO should consider and clarify how the Guidance should be applied within a risk-based context and explicitly state where aspects of the Guidance are aspirational, new requirements, or a FMI-specific interpretation of other existing cyber resilience frameworks.

The Guidance notes that it is intended to be "principles-based" and recognizes that "the dynamic nature of cyber threats requires evolving methods to mitigate these threats." Guidance, §1.2.2. Given the evolutionary nature of cyber threats, the Guidance further notes that "requiring specific measures today may quickly become ineffective in the future." Id. This appears to suggest the very risk-based approach that The Clearing House is advocating. However, in numerous instances, the Guidance deviates from this risk-based approach and appears to impose a specific approach to risk mitigation. Examples include proposed standards relating to security analytics (§ 4.4.1), changes in employment status (§ 4.4.2), continuous monitoring (§ 5.2.1), resumption within two hours (§ 6.2.2), data integrity (§ 6.3.2), data sharing agreements (§ 6.4.1), red team tests (§ 7.2.2) and predictive capacity (§9.2.3). Rather than impose specific standards in these areas, CPMI-IOSCO should limit the guidance to high-level principles that establish an overall resiliency objective and allow individual FMIs the latitude to achieve that objective as appropriate in relation to the FMI's risk profile and existing cyber frameworks.

The requirements set forth in 6.2.2 and 6.3.2 are particularly troubling. Section 6.2.2 seeks to impose a prescriptive standard whereby FMI's must "design and test its systems and processes to enable the safe resumption of critical operations within two hours of a disruption and to enable itself to complete settlement by the end of the day of the disruption, even in the case of extreme but plausible scenarios." Imposing a flat two-hour window for the resumption of operations is problematic for a number of reasons. First, it is unclear from what time the recovery point is calculated. Cyber operations, unlike natural disasters, may not always be easy to detect and a disruption, depending on how defined, may go unnoticed for some period of time.

Further, the standard has the potential to subject the FMI to inconsistent goals. Rather than a flat two-hour standard, the FMI's greatest concern should be resuming critical operations in a safe and sound manner, which, depending on the nature of the cyberattack and the state of the FMI's forensic investigation may or may not be possible in two hours. If a flat, two-hour window is imposed, FMIs run the risk of hastily applying short-term or ineffective solutions. While we believe a two-hour recovery period and the completion of settlement by the end of day is feasible on a fail-forward basis, FMIs should have the flexibility to determine the best recovery time based on the magnitude of the threat, the FMI's current business needs, and the availability to participants of substitute vectors and alternative providers in the market.

The provisions regarding data integrity are similarly troubling. Section 6.3.2 provides that "FMIs should "design and test their systems and processes to enable timely recovery of accurate data following a breach" and suggests, by way of example, that "FMIs' systems and processes could be designed to maintain an uncorrupted 'golden copy' of critical data." The section goes on to state that an "FMI's cyber resilience framework should include data recovery measures, such as keeping a copy of all received and processed data…."

The Clearing House understands and is supportive of the desire to ensure data integrity. However, The Clearing House believes that this proposed standard fails to take into consideration the complexities and trade-offs that can arise in this area. Specifically, with regard to payments systems and the corruption of data there is likely to be only one "golden copy" of transactional data and that golden copy is uniquely the participants' data. Any other data set is equally subject to corruption and, unless validated against the participants' data, resort to an external "golden copy" is only likely to introduce more complexity and potential for data corruption into the system. Keeping a copy of all received and processed data may actually increase opportunities for data theft and compromise. Any proposed standard for data integrity must allow FMIs to develop a risk-based approach that takes into consideration the complexities present in this area and the likely trade-offs and balancing of risks that need to be considered.

Development of Common Baseline and Reciprocity

The Guidance should provide a consistent way to communicate common baselines and maturity posture levels relative to Guidance expectations and desired outcomes. Without such a baseline, each FMI may interpret their level of compliance with the Guidance differently. Currently, the Guidance does not clearly outline maturity scoring mechanisms (or clearly dovetail with existing frameworks that do provide such scoring mechanisms), making it impossible for FMIs to compare results with one another or communicate results to stakeholders in a common manner. In addition, other entities affecting the FMI's cyber resiliency (e.g., third-party vendors or participants) may be using a different framework and scoring mechanisms to evaluate their cyber resilience, making it difficult if not impossible for the FMI to aggregate and assess its risks from external parties.

In light of the interconnectedness of the global financial system, we believe that CPMI-IOSCO should consider how the Guidance can provide a baseline for ensuring reciprocity. For example, CPMI-IOSCO could consider adopting a maturity scoring mechanism that is a component of a widely accepted framework.

Utility of Benefits

An additional set of standards without a clear nexus to or relationship with other existing standards will add an additional level of complexity and substantial administrative burden to a FMI's cyber resilience program. In particular, it will be an additional draw on critical resources that, ideally, should be focused on proactively preventing and addressing actual cyber issues as opposed to administering and mapping various frameworks. In addition, to the extent that the Guidance is not risk-focused, excessive costs may be borne by FMIs addressing issues that pose less risk in the context of an FMI's specific risk profile.

To ensure that the Guidance adds distinct utility to the industry, CPMI-IOSCO should more thoroughly assess the perceived benefits of the Guidance in light of existing standards.[4] In that any benefits that would be added by the Guidance are directly proportional to how well the Guidance dovetails with existing standards, CPMI-IOSCO should further study through a survey, quantitative impact assessment or other mechanism the gaps, if any, in existing standards and the need for further Guidance.

We hope that these comments have been helpful. We appreciate the opportunity to provide our input, and look forward to future opportunities to do so. If we can help to facilitate further discussions with you on these matters or assist you in any other way, please do not hesitate to contact me at 336.769.5314 or Rob.Hunter@theclearinghouse.org.

Sincerely,

/S/

Robert C. Hunter
Executive Managing Director & Deputy General Counsel

[4] A primary example of cost exceeding benefit in multiple layers of guidance is found in the ten-year progression from the Federal Information Security Management Act (FISMA) inception in 2002 to the reduction of multiple frameworks to a single "Risk Management Framework (RMF)" in 2012. Though RMF was conceptualized by NIST in the United States as early as the late 1990's, it was not fully implemented until March 2014, when both the defense and civil portions of the United States government began to normalize around RMF instead of their own, unique information assurance frameworks. Between FISMA, DIACAP, NIACAP, and other frameworks, the General Accounting Office, Office of Management and Budget, and the Inspector General's Office determined that multiple frameworks were not efficient, and recognized the need to tailor a combination of a basic framework, a common maturity model, and a smaller set of directions that "overlaid" the mission or business needs of the receiving organization.