February 23, 2016

CPMI Secretariat
Bank for International Settlements
Centralbahnplatz 2
4002 Basel, Switzerland
**Via Electronic Mail** (cpmi@bis.org)

IOSCO Secretariat
International Organization of Securities Commissions (IOSCO)
C/ Oquendo 12
28006 Madrid
SPAIN
**Via Electronic Mail** (consultation-2015-09@iosco.org)

Re: Comments on CPMI-IOSCO Consultative Report on Guidance on cyber resilience for financial market infrastructures

Ladies and Gentlemen:

The undersigned organizations are operators of Financial Market Infrastructures ("**FMIs**") designated as systemically important financial market utilities under the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (the "**Dodd-Frank Act**").[1] Additionally, some of the organizations operate regulated trade repositories in the U.S. and globally. We appreciate the work of the Committee on Payments and Market Infrastructures ("**CPMI**") and the Board of the International Organization of Securities Commissions ("**IOSCO**") to provide proposed guidance in the form of the recently published consultative report on "Guidance on cyber resilience for financial market infrastructures" (the "**Consultative Report**"), with the intent of supporting the industry's ongoing efforts to enhance FMIs' ability to pre-empt and respond to cyber attacks. We also appreciate the opportunity to comment on the Consultative Report, and hope that our comments will be taken into consideration in finalizing the proposed guidance.

[1] In July, 2012, the U.S. Financial Stability Oversight Council designated, among other entities, (i) The Clearing House Payments Company, L.L.C. (on the basis of its role as operator of the Clearing House Interbank Payments System), (ii) the Chicago Mercantile Exchange, Inc., (iii) The Depository Trust Company, National Securities Clearing Corporation, and Fixed Income Clearing Corporation, all of which are subsidiaries of The Depository Trust & Clearing Corporation, (iv) ICE Clear Credit L.L.C., and (v) The Options Clearing Corporation, as systemically important financial market utilities under Title VIII of the Dodd-Frank Act.

## I. General Comments

The undersigned FMIs recognize the significant work that CPMI-IOSCO has done in preparing the guidance in the Consultative Report. The current Consultative Report builds on prior work done over the past several years by both CPMI and IOSCO, including engaging the industry to analyze how FMIs address cyber security issues in the context of the Principles for Financial Market Infrastructures ("**PFMI**")[2], and the resulting report issued by CPMI in November 2014 entitled "Cyber resilience in financial market infrastructures" (referred to as the "**2014 Cyber Report**").

Recognizing the importance of addressing cyber threats, the group is supportive of these efforts and the value in providing the guidance contained in the Consultative Report. We believe, however, there are certain areas where further clarifications or modifications are warranted, particularly as the guidance is meant to cover all types of FMIs who provide very diverse services, operate in different markets and have different risk profiles.

Accordingly, the group respectfully strongly recommends that the finalized report be clearly identified and construed as high level guidance. Regulators should continue to provide FMIs the flexibility to develop and implement approaches and tools to address cyber security issues in a manner that (i) is appropriate for each FMI's unique risks and circumstances, and (ii) enables FMIs to tailor the use of relevant industry-based recognized best practices to their own programs. Adopting a flexible principles-based approach to regulating how FMIs address cyber threats is critical both because of the evolving nature of cyber threats, and the varied means of response. Recognizing that FMIs often operate across jurisdictions and may be subject to multiple regulatory regimes, it is also important to avoid the risk of requiring compliance with multiple standards or regulations that may result in an overly prescriptive (and potentially conflicting) approach that would neither be cost effective nor necessarily achieve the desired level of protection.

## II. Specific Comments

### 1. Implementation

The introduction (1.1.4)[3] states that the document is intended to provide "supplemental guidance" to the PFMI regarding cyber resilience, principally in the context of principles 2 (Governance), 3 (Framework for the comprehensive management of risks), 8 (Settlement finality) 17 (Operational risk) and 20 (FMI links), focusing on measures FMIs *should* undertake to enhance their cyber resilience capabilities. While the guidance is intended to be principles-based (1.2.2), in a number of areas it provides quite detailed guidance that may overlap or conflict with existing national regulation

[2] Issued by the Committee on Payment and Settlement Systems (the former name of the CPMI) and IOSCO in April, 2012.
[3] All number references refer to numbered sections in the Consultative Report.

applicable to one or more types of FMIs. At the same time the draft recognizes that "requiring specific measures today may quickly become ineffective in the future." (1.2.2)

Section 1.3.6 provides that oversight authorities are urged to "implement the guidance in carrying out their responsibilities within the context of the legal framework of the relevant jurisdiction." Given the mix of high-level recommendations with significantly detailed directions in a number or areas, however, it is unclear whether CPMI/IOSCO intends the guidance to be self-effectuating by setting standards to be applied by the FMI's supervisory authorities in interpreting and applying the PFMI (or the locally enacted equivalent), or if the detailed guidance should be implemented nationally through local specific regulations. Many jurisdictions have already done significant work in the area, adopting or proposing regulations specifically designed to address systems and cyber resiliency, including by requiring the adoption of industry best practices or generally accepted standards.[4] If the goal is to have a baseline level playing field, then the guidance should be modified to focus on high level principles that can be applied in a risk-based non-conflicted manner across the diverse universe of FMIs, as the threat landscape, industry standards and the technological tools to address cyber threats evolves.

2. Governance issues

The proposed guidance is presented in chapters that outline five primary risk management categories and three overarching components "that should be factored across an FMI's cyber resilience strategy and framework." (1.2.1) Under the governance category, FMIs are directed to have a clear and comprehensive cyber resilience strategy (2.1-Preamble) and framework that "prioritizes the security and efficiency of the FMI's operations and supports financial stability objectives." Further, the proposed guidance suggests an FMI's Board should ratify the strategy, which should be "closely aligned with, and complementary to, the resilience framework, ensuring it is capable of achieving its strategic objectives and outcomes." (2.2.1)

What is unclear from the discussion that follows is whether an FMI's cyber framework is intended to be a separate document (and one internally adapted to the FMIs' specific risks and infrastructure), or rather is guiding FMIs to apply and adopt one or more existing industry-based cyber resilience frameworks (2.2.6), such as the National

[4] See, for example, in the United States: Regulation Systems Compliance and Integrity, adopted by the U.S. Securities and Exchange Commission ("**SEC**") (SEC Release No. 34-73639, 79 F.R. 72252 (December 5, 20014), referred to as "**Reg SCI**", and the adopting release as the "**Reg SCI Release**"); U.S. Commodity Futures Trading Commission ("**CFTC**") rule proposal clarifying existing systems safeguards testing requirements for Derivatives Clearing Organizations (80 F.R. 80114 (December 23,2015)), and rule proposal for clarifying existing systems safeguards testing requirements for Designated Contract Markets, Swap Execution Facilities and Swap Data Repositories (80 F.R. 80140 (December 23, 2015)), respectively (referred to collectively as the "**Proposed System Safeguard Rules**"). See, also Regulation HH (Risk Management Standards for Designated Market Utilities) adopted by the Board of Governors of the Federal Reserve System (the "**FRB Board**"), 12 CFR 234 (and 234.3(a)(17), in particular) (79 F.R. 65543 (November 5, 2014)), effective December 31, 2014 (referred to as "**Regulation HH**").

Institute of Standards and Technology's (NIST) *Framework for improving critical infrastructure cybersecurity* (February, 2014), the Federal Financial Institutions Examination Council's (FFIEC) *Information Security Handbook*, or the International Organization for Standardization (ISO) *ISO/IEC 27001* standard.

We suggest that the discussion be clarified to make clear that CPMI-IOSCO is *not* mandating adoption of a particular industry-based framework, but rather intends that FMIs benchmark their own frameworks against the best practices and generally accepted standards best suited for each FMI's unique risks. Internal "frameworks"—that is, the relevant collection of policies, procedures and controls addressing cyber security risks – should be designed utilizing the PFMI principles-based approach and tailored to the specific risk profile and environment of each FMI. The guidance should leave the manner and form in which the strategy and framework is documented and implemented to the FMI, which may take into account the FMI's existing legal and governance structure, and its overall risk management framework. The guidance should also be clear that it is not the intent of CPMI-IOSCO to prescribe a particular form and approach to the framework, provided the risk categories and relevant components are appropriately addressed, and draw upon one or more generally accepted industry benchmarks and guidance.[5] We believe that clarity here is key to avoid potential compliance risk for FMIs that are subject to multiple regulatory regimes and regulators fail or are unable to coordinate and align on a common set of guidelines or standards in this area.

3. Identification: Interconnections and coordination

Among the key focuses of the guidance is interconnectedness risk. The introduction notes that "[g]iven the extensive interlinkages and interdependencies in the financial system, adequate cyber resilience is dependent not only on the resilience of a single FMI, but also on that of interconnected FMIs, of service providers and of the participants." (1.3.3) Collaboration, cooperation and information sharing among the FMI's key stakeholders, linked parties and vendors (described as the FMI's "ecosystem") are stressed as a means to improve resiliency. At numerous points throughout the Consultative Report, FMIs are directed to take (or require) actions in coordination with various stakeholders or entities within their own ecosystems: for example, in the design and implementation of their resilience efforts (3.3); to require "appropriate action" among their participants, service providers or other stakeholders, to support the implementation of the FMI's resilience objectives (1.3.3); in the area of exercises to test response, recovery and resumption plans (7.3); and with respect to information sharing regarding cyber threats, early warning indicators, and in the event of an incident (8.3).

[5] We also note the guidance suggesting that FMIs should be encouraged to use relevant metrics and maturity models to assess and measure the effectiveness of their cyber security programs. The use of commercially available metrics and maturity models may be confusing to the industry if there are multiple measurement programs and metrics that do not coalesce or align with each other.

The group is fully supportive of improving effective cooperation and information sharing, but cautions that the proposed guidance could lead, in practice, to overlapping and conflicting demands and obligations on FMIs. That is, every FMI is likely to be part of multiple "ecosystems"—the determination of who is (or is not) part of an ecosystem is always a matter of the viewer's perspective, and each FMI will be the center of its own ecosystem. Linked FMIs will be part of each other's orbit, and participants increasingly seek to treat the FMIs in which they participate as service provider/vendors.

Accordingly, the guidance should be clear that it should be the FMI who (i) determines who is within its respective "ecosystem", and (ii) sets the boundaries of what types of information is appropriate to share, and the means by which information such as threat vectors, etc., is shared. To minimize overlapping demands and requirements, FMIs should be encouraged to leverage existing industry groups and trusted networks as the means to promote cooperation and information sharing. FMIs should consider sharing information regarding identified threats and vulnerabilities via secure and confidential channels.[6] We address issues with respect to third party vendors in more detail below.

4. Protection: Controls, Vendor Management and Insider Threats

The group agrees with the emphasis on strong controls and designing for resilience. The guidance notes (4.2.1) that "[p]rotective controls should be proportionate to and consistent with the FMI's risk tolerance, its threat landscape and its systemic role in the financial system." While not attempting to be prescriptive, the draft nevertheless

- provides that FMIs should have a process that *ensures* that " *all* software, network configurations and hardware. . .are subject to rigorous testing against related security standards" [emphasis supplied](4.2.2),[7] and

- emphasizes that FMIs should have a comprehensive change management process that explicitly considers cyber risks both prior to and following any change. (4.2.3.b)

We believe this is overbroad, and that in promoting this perspective, the guidance should be revised to make clear that FMIs' control processes can utilize a risk-based approach to identify those applications, configurations and hardware, and systems changes that are critical or material, and then apply controls proportionate to the risk presented.

Similarly, in the discussion of service providers, the guidance provides that, "at a minimum" FMIs should "ensure" their service providers "meet the same high level of

[6] However, vulnerabilities identified within an FMI's internal systems would not be appropriate to share, but rather should be timely identified and mitigated.

[7] We note that the guidance tends to overuse terms such as "ensure", which appears at least 23 times in the document. This creates a level of expectation that we believe is neither practical nor warranted in many of the places in which the term is leveraged.

cyber resilience they would need to meet if their services were provided by the FMI itself." (4.3.1.b). This approach seems to treat all vendors as equal sources of risk, irrespective of the nature of service, the provider (for example, whether the provider is a common carrier such as a utility, or government provider, where the ability to obtain detailed information may be limited), and the connection interface. We believe the use of the term "ensure" in this context is not appropriate. A more realistic approach to addressing such risk would be to

- prioritize focus on outsourced services, where there is existing guidance (such as the FFIEC handbook on Risk Management of Outsourced Technology Services) on the approach to govern and manage these relationships, and

- minimize risk by segmentation and restricting or minimizing system access to specified vectors/communication interfaces, as regards providers generally.

Further, we believe that the use of consistent tools for vendor due diligence (such as standardized audit reports) should be supported to avoid duplicative review and auditing of the systems and capabilities of common service providers. Finally, the issue of who is deemed a service provider is also important—as with the view of an FMI's ecosystem, there is the risk of differing and overlapping views of who is a service provider to whom—including FMIs with link arrangements to other FMIs. FMIs are also increasingly viewed as service providers to their own participants, which risks having conflicting and overlapping requirements on security controls and related disclosure. A focus on outsourcing should help reduce potential overlap.[8]

With respect to insider threats (4.4), the guidance calls for screening and analytics on employees. We question whether mandating a baseline of profile activity for employees and anomaly detection may be overly aggressive if applied to all of an FMI's employees, and note that effective commercial monitoring technology in this area is still evolving. The guidance should also recognize that some form of background checks may not be permissible under privacy laws in a number of jurisdictions.

5. Recovery time objectives

While the group understands the context within which the recovery time objective is stated—that is, the discussion under PFMI 17 of business continuity management[9]—the final guidance needs to make clear that with respect to cyber disruptions the recovery time objective is properly a concrete goal in designing BCM policies and procedures, rather than a hard and fast regulatory requirement that needs to be met in all recovery circumstances irrespective of the nature or extent of the disruption.

[8] In this context, we believe that for highly regulated FMIs, market participants in conducting systems safeguards related due diligence should be able to take into account that those entities are regularly examined and are the focus of heightened scrutiny.
[9] Key Consideration 6 of PFMI 17 (Operational Risk).

The original recovery discussion in the PFMI was focused on physical disruptions. To mitigate the effect of these, the Operational Risk discussion in Principle 17 directs FMIs to incorporate 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.

Physical events have a known starting point and, in most cases, an easily predictable and dimensional impact as well as a standard path for failing over to alternate sites and staffing. Cyber recovery, on the other hand, is fundamentally different. CPMI-IOSCO concedes this point (1.1.3). Mitigation of cyber events requires:

- Identification/notification—this encompasses the need to identify the source/issue of the cyber event, which, unlike physical events, can have a multitude of permutations the examination of which can take significant time
- Containment—the need to prevent spread or contagion of the event, including to participants in the FMI's ecosystem
- Eradication
- Recovery, and
- Resumption of services

A cyber event will not always, or even necessarily, lead to a processing outage or disruption; in such cases applying the recovery time frame is not necessary or always sensible. On the other hand, to apply a two hour recovery objective 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.

Further, recovery is not the same as resumption.[10] 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, done 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.[11]

[10] These terms tend to be used interchangeably in the draft. As noted in the Glossary to the Consultative Report, recovery is a technology term that refers to the availability of technology in a new environment. Resumption is a business term that means the ability to now conduct business on the new/recovered technology.

[11] The feasibility of fail-forward approaches (where uncompleted transactions from a certain specified point forward are deemed cancelled and processing resumes anew utilizing new instruction input) may depend upon the volume of transactions processed by an FMI and the nature and length of the applicable transaction processing life cycle.

Some of the suggested means to address recovery and resumption in the Consultative Report are impractical, particularly the consideration of manual processing as a fall back, or at the other end of the spectrum maintaining a wholly separate and differentiated processing architecture that would enable parallel processing. Both would introduce significant operational risks of their own into the infrastructure and as to the latter, may foreseeably raise considerable costs to build and operate on an ongoing basis.

CPMI recognized in its 2014 Cyber Report 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.[12] 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 with safe and sound operation.[13] 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.

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.[14] Accordingly, the group believes that the guidance should be revised to take a consistent approach.

---

[12] See the 2014 Cyber Report at 3-4, and 10-12.

[13] Section 6.4.5 of the guidance (Forensic readiness) illustrates the inherent tension between safely resuming operations with the ability to properly identify the source and mitigate a cyber issue, and the focus on a two hour RTO. While noting that forensic analysis may need to be postponed, the guidance nevertheless provides that "FMIs should ensure that investigations can still be performed post-event to the extent possible, eg through preservation of necessary system logs and evidence." If the expectation is for resumption to take the highest priority in a limited timeframe, then additional time and effort cannot be exerted around evidence preservation and collection. The focus will be on replacing systems quickly, regardless of what evidence may be lost in the process. More important, the FMI must be able to perform sufficient analysis to ensure the ability to recover to a stable state, so as to avoid merely recovering systems to the vulnerable state which had permitted the attack to succeed in the first place. A more balanced approach would, we believe, better promote safety and soundness.

[14] See, for example, the SEC's Reg SCI Release, *supra* at note 4 (79 F.R. at 72294-96). The regulation as originally proposed would have required entities, including U.S. registered clearing agencies and trading venues (as entities deemed "Reg SCI Entities"), to maintain policies and procedures, including business continuity and disaster recovery plans with backup and recovery capabilities designed "to ensure next business day resumption of trading" for trade venues, and required two hour resumption of "clearance and settlement services." In response to numerous comments, the proposal as finally adopted was modified. The Reg 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." Id. In support of this modification, the SEC cities the U.S. Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial Systems, SEC Rel No. 47638 (April 7, 2003), 68 F.R. 17809, 17812, which provides 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."
See, also the CFTC's Proposed System Safeguard Rules (*supra* at note 4). For derivatives clearing organizations ("**DCOs**"), the proposal 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," or in the case of a systemically important DCO, its business continuity and disaster recovery plan "*shall have*

*  *  *  *  *  *

We appreciate the opportunity to comment on the Consultative Report and your consideration of the views expressed in this letter. We recognize that many of the matters addressed are complex, and we would 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,


The Clearing House Payments Company L.L.C.
/s/ Parthiv Shah
Senior Vice President and Chief Information Security Officer
parthiv.shah@theclearinghouse.org

Intercontinental Exchange, Inc.
/s/Jerry Perullo
Chief Information Security Officer
jerry.perullo@theice.com

CME Group Inc.
/s/ Gil Vega
Managing Director and Chief Information Security Officer
Gil.vega@cmegroup.com

The Options Clearing Corporation
/s/ Daniel DeWaal
First Vice President, Security Services and Chief Security Officer
ddewaal@theocc.com

The Depository Trust & Clearing Corporation
/s/ Stephen Scharf
Managing Director and Chief Security Officer
sscharf@dtcc.com


---

*the objective of enabling"* the DCO to recover its operations and resume daily processing, clearing and settlement no later than two hours following the disruption [emphasis supplied]. (80 F.R. at 80135-36) For trade repositories, the proposal provides that swap data repository's business continuity/ disaster recovery plan and resources generally should enable resumption of swap data repository's operations and resumption of ongoing fulfillment of the swap data repository's duties and obligations during the next business day following the disruption. (80 F.R. at 80187).

The FRB Board, in adopting Regulation HH, made a similar observation and modification:

> In areas where threats and technology are evolving, such as is the case for certain extreme cyber attacks, the Board recognizes that it may not be possible at this time for the designated FMU to recover within two hours. In such cases, the Board will work with the designated FMU through the supervisory process to identify reasonable approaches to preparing for and recovering from such attacks. The Board is revising proposed [section (a)(17)(vii)(B) of the regulation] to indicate this intent.

*Supra* at note 4, 79 F.R. at 65552.