Dino Kos
Head of Global Regulatory Affairs

CLS Bank International
Financial Square
32 Old Slip, 23rd Floor
New York, NY 10005

Tel: +1 212 510 4548

February 23, 2016

Via Email

IOSCO Secretariat
C/ Oquendo 12
28006 Madrid
Spain
Email: consultation-2015-09@iosco.org

CPMI Secretariat
Bank for International Settlements
Centralbahnplatz 2
4002 Basel
Switzerland
Email: cpmi@bis.org

Re: CPMI-IOSCO's Consultative report: Guidance on cyber resilience for financial market infrastructures

Dear Sirs/Mesdames,

CLS Bank International ("CLS"), the operator of the CLS settlement system (the "CLS System"), appreciates the opportunity to comment on the Committee on Payments and Market Infrastructures' ("CPMI") and the Board of the International Organization of Securities Commissions' ("IOSCO") Consultative report: Guidance on cyber resilience for financial market infrastructures ("FMIs") (November 2015) (the "Proposed Guidance" and once finalized the "Final Guidance").

I. Background

CLS is an Edge Act corporation organized under the laws of the United States of America and is regulated by the Board of Governors of the Federal Reserve System and supervised by the Federal Reserve Bank of New York (collectively, the "Federal Reserve"). It operates the world's largest multicurrency cash settlement system for mitigating settlement risk associated with FX transactions, and currently provides a payment-versus-payment settlement service for payment instructions in 18 currencies. Additionally, the 18 central banks whose currencies are settled in the CLS System have established the CLS Oversight Committee, organized and administered by

the Federal Reserve.[1] The CLS Oversight Committee operates in accordance with the Protocol for the Cooperative Oversight Arrangement of CLS.[2] As a systemically important FMI, CLS is subject to the April 2012 CPSS-IOSCO *Principles for financial market infrastructures* (the "PFMI") as applicable to payment systems. CLS has also been designated a systemically important Financial Market Utility by the United States Financial Stability Oversight Council.

II. Comments on the Proposed Guidance

CLS would like to express its broad support for the Proposed Guidance for FMIs on the enhancement of their cyber resilience. This effort follows the CPMI-IOSCO's creation of a working group on cyber issues, and its November 2014 publication, *Cyber resilience in financial market infrastructures* ("2014 CPMI-IOSCO Publication"), which CLS includes in its consideration of cyber risk. CLS agrees with the CPMI-IOSCO that cyber risks faced by FMIs and their level of readiness to effectively deal with worst-case scenarios should be considered a priority by FMIs and authorities alike. For this reason, CLS is focused on enhancing its risk management framework to take into account evolving threats and responding rapidly and effectively to cyber issues.

The Proposed Guidance, in the Executive Summary, provides that it is supplemental to the PFMI, and is not intended to impose additional standards on FMIs beyond those set forth in the PFMI. It also provides that it is intended to be principles-based, as tactical measures that are effective today may quickly become ineffective in the future. (Proposed Guidance, Section 1.2.2). CLS supports the maintenance of consistent high-level standards across jurisdictions and, subject to its comments below, agrees with the high-level principles contained in the Proposed Guidance, as they are prudent and consistent with well-known control frameworks.

A. Implementation

1. Uniform Adoption

The Proposed Guidance states that "relevant regulatory, supervisory and oversight authorities, in carrying out their responsibilities, are urged to implement the guidance within the context of the legal framework of the relevant jurisdiction." (Proposed Guidance, Section 1.3.6). CLS urges the relevant authorities to approach implementation of the Final Guidance prudently and with a focus on uniform adoption whenever possible, both across borders and amongst various domestic agencies that may oversee FMIs within a given jurisdiction. Lack of uniform implementation creates the potential for inefficiencies associated with complying with multiple standards, as well as challenges regarding clarity and adequacy of compliance. This is particularly relevant to an international FMI like CLS, which is subject to standards in multiple jurisdictions. Therefore, careful uniform implementation is encouraged.

2. High Level Guidance and Control Frameworks

In addition, CLS recommends that when relevant regulatory and supervisory authorities implement the Final Guidance, they clarify that it is meant to provide high-level enduring

---

[1] In addition to the European Central Bank, the CLS Oversight Committee also includes five other Eurosystem central banks, bringing the total to 23 central bank members.

[2] See http://www.federalreserve.gov/paymentsystems/files/cls_protocol.pdf.

principles, which should then be supplemented by other control frameworks[3] such as the International Organization for Standards (ISO) 27001 and 27002, the SANS Institutes' Critical Security Controls, and the National Institute of Standards and Technology's (NIST) Framework for improving infrastructure cybersecurity. CLS recommends that the Final Guidance is practical and not overly prescriptive as (i) cyber risk management is a rapidly changing area where threats are evolving,[4] and (ii) FMIs have unique architectures, business processes and ecosystems, depending on the services they perform and markets they serve, and therefore there is no one-size-fits-all approach to cyber risk prevention.

3. The FMI's Risk Management Framework

In Section 1.1.3, the Proposed Guidance notes that "cyber risks are unique," while also acknowledging that they should be managed as part of an FMI's overall risk management framework. CLS agrees with both points, and as for the latter, would highlight that most FMIs have comprehensive risk management frameworks in place, as required by the PFMI. Therefore, the most efficient approach would be to embed appropriately into those existing risk management frameworks the Final Guidance and applicable control frameworks, and not segregate them into separate frameworks and documents unless there is a practical reason for doing so.

The Proposed Guidance in various sections appears to refer interchangeably to the "cyber resilience strategy and framework" (Proposed Guidance, Preamble 2.1), the "cyber resilience framework" (id,) and the "resilience framework" (Proposed Guidance, Section 2.2.1). Consistent with the paragraph above, the Final Guidance should clarify that while FMIs should appropriately manage cyber risks and have clear roles, responsibilities, and accountability for developing strategy and managing cyber incidents, these concepts can be contained in the FMIs' existing frameworks and documents wherever practicable, and that there are no prescribed titles for particular risk management documents, assuming such documents, taken as a whole, achieve the objectives of the Final Guidance.

B. Two Hour Resumption of Critical Services

In several sections, the Proposed Guidance refers to a two hour timeframe during which an FMI must resume its critical operations if its critical services are disrupted. (Proposed Guidance, Sections 1.1.5, 6.2.2, 6.2.3, 6.3.1, and Glossary (definition of "resume")). CLS recognises that FMIs are vital to the global financial system and should endeavor to return to full operational capacity as quickly as possible if a disruption occurs. CLS also understands the value of having target resumption times and best practices in place to drive the industry toward a common understanding of the significance of resuming critical services. CLS further appreciates that the Proposed Guidance provides that the resumption requirement should be tiered, as it references "critical" operations.

However, consistent with other guidance,[5] the Final Guidance should consider the challenges associated with a two hour resumption period in extreme but plausible circumstances, as there

---

[3] CLS suggests that the term "control frameworks" or a similar term be specifically referenced and/or defined to clarify this point and distinguish such frameworks from the Final Guidance.

[4] It may also be advisable to review and update, as needed, the Final Guidance more frequently than the PFMI.

[5] See 2014 CPMI-IOSCO Publication, at 1 ("FMIs consider a two-hour recovery time objective (2h-RTO*) in the context of an extreme cyber event to be challenging . . ."); see also PFMI, Section 3.17.14 ("[a]n FMI should *aim* to be able to resume operations within two hours following disruptive events") (emphasis added)).

are threats that may be presently unknown, and FMIs cannot test an infinite number of scenarios or certify or guarantee that critical services will be resumed within a certain time period in every case. In some cases, resumption should be balanced against the necessity to preserve data and contain corruption. This approach is consistent with the direction in the Proposed Guidance that "an FMI should resume critical services as soon as it is safe and practicable to do so without causing unnecessary risk to the wider sector or further detriment to financial stability." (Proposed Guidance, Glossary (definition of "resume"); see also Section 6.4.2). The Final Guidance should also take into account that there may be disruptions that could involve multiple institutions, and that resumption, in such cases, would require coordination. To effectively manage an incident of this scale, advanced coordination and planning should be considered.

Further, the pace of the implementation of cyber risk reduction technology, regardless of its potential, should always be properly balanced against pragmatic and appropriately phased implementation, as new solutions meant to decrease resumption time may comport their own risks. Thus, when applying the Final Guidance toward a two hour resumption period, it is essential that the FMI be permitted to set appropriate timeframes for implementation.

Finally, there is some ambiguity around how the two hour resumption period should be calculated and when the period should apply, depending on the incident and the type of FMI. A cyber threat may be present for some time before it is discovered, and partial resumption may be sufficient under certain circumstances. For CLS, settlement of FX payment instructions and associated funding occurs within a five hour period on business days, and thus priorities in terms of resumption of the service would also vary according to whether they fall into or just prior to this window.

C. Stakeholder and Third Party Considerations

1. Scope

In several Sections, the Proposed Guidance acknowledges that FMIs have "linkages and interdependencies" in the financial system, and that adequate cyber resilience is dependent not only on the resilience of a single FMI, but also on that of interconnected FMIs, service providers and participants. (Proposed Guidance, Section 1.3.3). In other Sections, the Proposed Guidance references the FMI's "ecosystem," and also states that, "[i]n particular, an FMI's cyber resilience framework should consider how the FMI would regularly review and actively mitigate the cyber risks that it bears from and poses to its participants, other FMIs, vendors, vendor products and its service providers, which are collectively referred to in this document as an FMI's ecosystem." (Proposed Guidance, Sections 2.2.5, 3.3; 6.4.2, and Glossary (definition of "ecosystem")).

As it is not necessary, practical or possible to regularly review and actively mitigate risks associated with every member of the ecosystem, FMIs must be permitted to take a tiered, risk-based approach to address third party risk. Therefore, in order to avoid confusion and promote compliance, it is important that the Final Guidance define terms such as "ecosystem," "linkages" and "interdependencies" appropriately in light of the context and allow for flexibility.[6] For example, "ecosystem" should be defined, at a high level, with reference to an FMI's "interconnected information infrastructure" and "other persons, processes, data, and information and communications technologies, along with the environment and conditions that influence those interactions," rather than generally in a way that would include parties with no link to or effect on

[6] This is particularly true in cases where such terms are already ascribed a meaning associated with financial contagion or other connections that may not be relevant to cyber risk (e.g., in the PFMI).

the FMI's information infrastructure. Once these terms have been defined on a high-level, since FMIs are unique in terms of architecture, business processes, and types of connections and dependencies, each FMI should be tasked with defining its ecosystem, taking a tiered and risk-based approach.

2. Assurances and Testing

In addition to defining its linkages, CLS recognizes that an FMI should gather information from third parties and verify and test assumptions associated with cyber and other types of resilience. Ultimately the FMI should be responsible for clearly defining third party risks and how they are mitigated, and should take a risk-based approach when making these determinations.

CLS notes that the Proposed Guidance calls for rigorous testing of "[a]ll elements of a cyber resilience framework," (Proposed Guidance, Sections 7.1 and 7.2.1), and "all software network configurations and hardware." (Proposed Guidance, Section 4.2.2). In certain cases, confirmations, table-top exercises, attestations and other types of assurances from key partners and/or vendors may be the appropriate means of verification. This may include requesting attestations and other assurances from members of the ecosystem, such as operators of real-time gross settlement systems, with respect to their systems and business processes.

3. Entry Points

At Section 1.1.3, the Proposed Guidance states that "there is a broad range of entry points through which an FMI could be compromised," and provides examples of such points, including linked FMIs, service providers, vendors and vendor products. However, the entry points will vary for each FMI depending on its structure, segregation and architecture, and therefore it should not be assumed that there is a "broad range" of entry points through which an FMI can be compromised. Each FMI should be considered separately when relevant regulatory authorities consider risks of entry.

4. Information Sharing and Use

In Section 1.3.3, the Proposed Guidance underscores the importance of FMIs promoting among their participants, service providers and other relevant stakeholders, an understanding of their resiliency objectives, and requiring appropriate action to support their implementation. Moreover, the Proposed Guidance supports the sharing of information associated with realized risks. (Proposed Guidance, Sections 6.4.4, 8.3.1, and 8.3.2).

While information sharing serves important objectives, the Final Guidance should acknowledge that there may be legal and practical impediments to sharing information, both with industry participants and governmental actors. These impediments include actual or potential conflicts with privacy and competition laws, as well as concerns about other types of liability, the protection of intellectual property, and the exposure of an FMI's weaknesses to third parties. Concerns associated with legal liability are particularly pronounced for an international FMI such as CLS that is subject to several legal regimes. Therefore, the Final Guidance should clarify that information sharing should only be undertaken in compliance with applicable law, and should be balanced against the risk of sharing sensitive or protected information.

CLS also notes a general paucity of channels for international information sharing, in comparison with domestic channels, although the threats contemplated are not constrained by national borders. Understandably, national laws and security and other interests pose challenges to cross-border information sharing. However, for an FMI like CLS, with information assets and interests in

more than one jurisdiction, a more streamlined method of global information sharing is encouraged.

The Proposed Guidance also references security analytics (Proposed Guidance, Sections 4.4.1 and 5.2.5.), as well as screening/background checks on new employees. (Proposed Guidance, Section 4.2.2). While access to and review of this information may be prudent, it may also present legal (e.g., data privacy and protection) or other issues and must be undertaken carefully by an FMI depending on which jurisdictions' laws apply.

D. Log Maintenance

In Section 3.2.2, the Proposed Guidance states that an FMI should "identify and maintain a current log of both individual and system credentials to know the access rights to information assets and their supporting systems." In the absence of an appropriately crafted definition for interconnectedness that takes into account cyber risk, this should be subject to the FMI's internal review and a tiered approach.

* * * *

Please do not hesitate to contact us if you have any questions regarding this letter.

Yours sincerely,

Dino Kos

cc:

Alan Marquard, *General Counsel, CLS Group*
Naresh Nagia, *Chief Risk Officer, CLS Bank International*
Thomas Zschach, *Chief Information Officer, CLS Bank International*
Vas Rajan, *Chief Information Security Officer, CLS Bank International*
Andrea Gildea, *Assistant General Counsel, CLS Bank International*