PRC PAYMENTS RISK COMMITTEE

Sponsored by: FEDERAL RESERVE BANK of NEW YORK

February 22, 2016

Mr. Klaus Löber
Head of the Secretariat of the Committee for Payments and Market Infrastructures
cpmi@bis.org

Mr. Paul Andrews
Secretary General of the Board of the International Organization of Securities Commissions
consultation-2015-09@iosco.org

Dear Messrs. Löber and Andrews,

Please find attached comments by the Payments Risk Committee (PRC) on the Committee for Payments and Market Infrastructures' (CPMI) and the Board of the International Organization of Securities Commissions' (IOSCO) consultative document *Guidance on Cyber Resilience for Financial Market Infrastructures.*

Cybersecurity and its related risks are an important topic for the PRC, to which it has devoted increasing attention over the past years.

The PRC is a private-sector organization sponsored by the Federal Reserve Bank of New York. The PRC's membership, drawn from financial firms, meets at regular intervals to identify and analyze risk issues in payments, clearing, and settlement of financial transactions[1]. The primary goal of the PRC is to foster enhancements to the safety and resiliency of financial market infrastructure, including steps to strengthen the clearing and settlement of financial transactions, and to inform the Federal Reserve Bank of New York about developments, conditions, and practices in payments, clearing, and settlement systems.

The views expressed in this document are the views of the PRC only. Nothing herein reflects official views of the Federal Reserve Bank of New York, the Board of Governors of the Federal Reserve System, or any other entity within the Federal Reserve System.

We appreciate the opportunity to comment on the important issues addressed in this consultation paper and to make recommendations to improve the proposed guidance on cyber resiliency.

The PRC would welcome an opportunity to work with the CPMI and IOSCO to further develop the cyber resilience guidance, to ensure consistent and appropriate guidance and rules to ensure the global financial markets are protected.

Yours sincerely,

David Russo
Chairman, Payments Risk Committee
Chief Operating Officer, Risk Management, Morgan Stanley

[1] The current members of the PRC represent Bank of America N.A., The Bank of New York Mellon, Bank ofTokyo-Mitsubishi UFJ, Citibank N.A., Deutsche Bank AG, Goldman Sachs, HSBC Bank USA, JPMorgan Chase, Morgan Stanley, State Street Bank and Trust Company, UBS AG, and Wells Fargo. More information on the PRC and its members is available at: http://www.newyorkfed.org/prc.

The PRC supports the work of global policymakers to address systemic risk in financial market infrastructures (FMIs), FMIs in general, and CCPs in particular, given their increased systemic importance. We feel that safeguarding FMIs against operational risk issues including cybersecurity risks is very much needed, and therefore this guidance for FMIs is welcomed.

Generally, the PRC found the guidance to be fairly comprehensive in addressing key cybersecurity issues and supports CPMI-IOSCO's proposed guidance on cyber resilience for FMIs. The guidance provides a sufficiently flexible and risk-based approach that is applicable internationally and provides a basis with which FMIs can manage their cybersecurity objectives.

In specific response to the guidance, the PRC would like to offer the following comments and recommendations for your consideration.

1. The PRC supports the intent behind the requirement to enable the safe resumption of critical operations within 2-hours of a cyber disruption, though we understand that this may currently be aspirational and/or exceedingly expensive to achieve in practice. The PRC suggests a discussion and deliberation among stakeholders regarding the costs/benefits and meaning/definition of a 2-hour recovery time objective (RTO), specifically or a prescribed RTO generally following a cyber incident. The requirement to complete final settlement at least by end-of-day is necessary and desirable.

2. The PRC believes that dedicated resources should be available to address cyber resilience issues affecting the financial sector and that FMIs should partner with participants to ensure that dedicated resources are available both within the FMIs and among its participants to effectively address cyber resilience issues.

3. Testing, exercising and coordination should include the wider ecosystem of FMIs. Exercises and testing are well-recognized aspects of good cyber resilience. The document would benefit from additional references to the role that exercising, including the use of sector-wide exercises, can play in strengthening an FMI's cyber resiliency.

4. CPMI-IOSCO should consider developing and incorporating guidelines as to how FMIs can partner, cooperate and share best practices/information with banks to improve collective ecosystem-wide cyber resilience. The PRC agrees that institutions will benefit from active participation in information-sharing groups and collectives, including cross-industry, cross-government and cross-border groups to gather, distribute and assess information about cyber practices, cyber threats, and early warning indicators related to cyber threats.

5. The PRC supports the need for a coordinated effort on the part of regulatory, supervisory and oversight authorities globally and across different markets.

The PRC is open to collaborating with the CPMI and IOSCO on this topic in the future.