Committee on Payments and
Market Infrastructures

BANK FOR INTERNATIONAL SETTLEMENTS

Press release

Press enquiries: +41 61 280 8188
press@bis.org
www.bis.org

Ref no: IOSCO/MR/44/2015

24 November 2015

CPMI-IOSCO consultative paper
Guidance on cyber resilience for financial market infrastructures

The Committee on Payments and Market Infrastructures (CPMI)[1] and the Board of the International Organization of Securities Commissions (IOSCO)[2] today released the consultative paper *Guidance on cyber resilience for financial market infrastructures* ("the Cyber Guidance").[3]

Financial market infrastructures (FMIs) play a critical role in promoting the stability of the financial system. Thus, the cyber risks faced by FMIs and their level of readiness to effectively deal with worst case scenarios have been considered top priorities by industry leaders and authorities alike. The Cyber Guidance aims to add momentum to and instil international consistency in the industry's ongoing efforts to enhance FMIs' ability to pre-empt cyber attacks, respond rapidly and effectively to them, and achieve faster and safer target recovery objectives if they succeed.

Key concepts built into the Cyber Guidance include the following:

- Board and senior management attention is critical to a successful cyber resilience strategy.
- The ability to resume operations quickly and safely after a successful cyber attack is paramount.
- FMIs should make use of good-quality threat intelligence and rigorous testing.
- Cyber resilience requires a process of continuous improvements.
- Cyber resilience cannot be achieved by an FMI alone; it is a collective endeavour of the whole "ecosystem".

The Cyber Guidance builds on previous studies conducted in this area by both the CPMI and IOSCO.[4] When finalised, the Cyber Guidance will not establish additional standards for FMIs beyond those already set out in the Principles for Financial Market Infrastructures (PFMI). Instead, the document is intended to be supplemental to the PFMI, primarily in the context of governance (Principle 2), the

framework for the comprehensive management of risks (Principle 3), settlement finality (Principle 8), operational risk (Principle 17) and FMI links (Principle 20).

The proposed Cyber Guidance sets out the preparations and measures that FMIs should undertake to enhance their cyber resilience capabilities with the aim of limiting the escalating risks that cyber threats pose to individual FMIs and thereby to financial stability. It also provides authorities with a set of internationally agreed guidelines to support consistent and effective oversight and supervision of FMIs in the area of cyber risk.

The Cyber Guidance is primarily intended to create meaningful shifts in the FMI industry towards greater cyber resilience. In this regard, Mr Benoît Cœuré, Chairman of the CPMI, stated: "This is an important report because cyber attacks in the financial sector have the potential to create widespread financial instability. Nobody should assume they will be able to prevent cyber attacks in all circumstances. Therefore, the Cyber Guidance addresses the need for an FMI to resume its operations quickly and safely after an attack has occurred. This is not an easy task and may require innovative thinking that goes beyond the traditional approaches to operational resilience."

Mr Greg Medcraft, Chairman of IOSCO, added: "The proposed Cyber Guidance is the culmination of extensive collaboration between IOSCO and the CPMI. It reflects an urgency to address the increasing risks that cyber threats pose to FMIs and financial stability, as well as the need for a coordinated approach. At the FMI level too, cyber resilience cannot be achieved by individual institutions alone in our highly interconnected financial sector. The broader 'ecosystem' needs to work in unison. The Guidance calls upon the ecosystem to do just that. We hope to collaborate with all stakeholders to meaningfully enhance the cyber resilience of our financial system as we refine these proposals and later implement them."

The consultative report is available on the websites of the Bank for International Settlements (www.bis.org) and IOSCO (www.iosco.org).

Comments on the report should be submitted **by Tuesday 23 February 2016 via e-mail** to **both** the CPMI Secretariat (cpmi@bis.org) and the IOSCO Secretariat (consultation-2015-09@iosco.org).

All comments may be published on the websites of the Bank for International Settlements and IOSCO unless a commenter specifically requests confidential treatment.

Notes

1. The CPMI promotes the safety and efficiency of payment, clearing, settlement and related arrangements, thereby supporting financial stability and the wider economy. The CPMI monitors and analyses developments in these arrangements, both within and across jurisdictions. It also serves as a forum for central bank cooperation in related oversight, policy and operational matters, including the provision of central bank services. The CPMI is a global standard setter in this area. The CPMI secretariat is hosted by the

BIS. More information about the CPMI, and all its publications, can be found on the BIS website.

2. IOSCO is an international policy forum for securities regulators. Its objective is to review major regulatory issues related to international securities and futures transactions and to coordinate practical responses to these concerns.

3. The Cyber Guidance was prepared for the CPMI and IOSCO by a working group comprising representatives from CPMI central banks and IOSCO securities commissions. The working group is co-chaired by Coen Voormeulen (Director, Cash and Payments Division, Netherlands Bank) and Hern Shin Ho (Executive Director, Specialist Risk Department, Monetary Authority of Singapore).

4. Please see also CPMI, *Cyber resilience in financial market infrastructures*, November 2014; and IOSCO, *Cyber-crime, securities markets and systemic risk*, Staff Working Paper, July 2013.