Thomas Murray
Data Services

Thomas Murray Data Services,
No. 1 Farriers Yard, Assembly London,
77-85 Fulham Palace Road,
London W6 8JA,
England

Letter submitted by e-mail to consultation-2015-09@iosco.org; and cpmi@bis.org.

Subject line of email: "Consultative report: guidance on cyber resilience for financial market infrastructures," text in Microsoft WORD format

Comment may be made publicly available.

Reference: "Consultative report: Guidance on cyber resilience for financial market infrastructures"

Rohini Tendulkar,
Senior Economist
IOSCO Secretariat
IOSCO
Calle Oquendo
28006 Madrid
Spain

19th February 2016

Dear Rohini,

The firm of Thomas Murray wishes to thank IOSCO for the opportunity to comment on guidance on cyber resilience for financial market infrastructures. Cyber security is at the top of the list of IOSCO's risk concerns, a perspective we share based upon our analyses of hundreds of financial institutions, feedback from our clients, and equally the safety and inviolability of the firm's own extensive information bases.

We appreciate IOSCO setting the framework for this consultation in the context of the Principles for Financial Market Infrastructures ("PFMIs"), which this firm uses extensively for organising information on infrastructures. The PFMIs are rapidly becoming a reference work of the highest importance for our clients. The report sets out the stakes for increasingly worrisome problems, *perhaps not even loudly enough*. In our experience in conversation and correspondence, IT security has a parallel to thinking

about global warming: it is a subject that is familiar to all, always on the radar screens, but somehow a problem for another day.

This firm underscores the significance of CPMI-IOSCO's point on boards of directors' leadership on cyber security. In practice, from our research on FMIs, we see infrastructures addressing risk questions far more than pre-2007-2009, but then the financial system has also grown proportionately more dependent on IT – with increasing vulnerability to its flaws, and to those who would probe its weaknesses for disruptive, and possibly illegal purposes. Physical plant and the integrity of systems and data bases are central to that heightened focus. There is much more awareness of testing and back-up sites in reserve, budgeting, the training and hiring of senior suite risk managers and IT strategists – and yet resistance at the board level for meaningful discussion, which in our view is true of IT generally. Few directors have enough practical experience of IT to speak fluently to their peers – it is an uncomfortable subject relative to the dependency of corporations in 2016. The obverse is also true: too few IT and risk managers have enough experience of general management issues to get appointed to boards of directors.

The firm

Thomas Murray was founded 22 years ago as a private firm registered in the United Kingdom. It is owned by 90 individual investors; with no institutional ties of any kind, this position assures the independence of viewpoint that is essential for credible analytical and advisory services.

Uniquely, the firm's business is devoted solely to capital markets infrastructure institutions, and its analyses cover 430+ such establishments in more than 100 marketplaces. 75 persons work for the firm, and we endeavour to provide current, detailed information to our clients. The question that led to the founding of Thomas Murray was global custody, and from there the business coverage spread by geography and line of business. Today the firm's analytical coverage includes central securities depositories, custodians (global, national, and sub-custodian), settlement houses, clearing houses, transfer agents, cash correspondents, as well as registrars.

It has been clear since the 2009 G20 Pittsburgh summit that the policy expectations in terms of capital markets risk management were changing considerably with respect to infrastructures, notably in the clearing field as a solution to OTC derivatives valuation and counterparty risk mitigation.

Thomas Murray believes that its extensive knowledge of financial market infrastructures, generally and globally, may give weight to the comments that follow.

Comments on the current consultation

<u>Principle 2: Governance</u>

Following on immediately from Principle 1, with its focus on law, we find that during our collaboration with infrastructures on their PFMI self-assessments, there is a carry-over conversation with a focus on the proper powers, responsibilities, and authorisations and processes of board governance. These are often adequate for the key considerations, so we tend to stop there. It is right to maintain the strong focus on law, which is fundamental to securities markets.

But in 2016, that is no longer enough – we are dealing with a more complex environment. Risks of various general sorts do come up, but only tangentially, at least in our experience.

Whilst on the subject of governance, Thomas Murray would recommend that boards establish cyber security committees, as they now frequently have for audit, nomination or remuneration. This would take the board's focus on cyber security to another level, rather than having the heads of IT or the chief risk officer provide regular reports to the board. Cyber security must become of the board, not to the board.

As part of directors' induction to their responsibilities of leadership, they must become fluent in the firm's risk model *in all its complexity*.

Principle 3: Framework for the comprehensive management of risks

As the headline of Principle 3 indicates, FMIs face many risks throughout the day. From the 2012 publication of these Principles, the term "cyber security" was actually missing from the laundry list of "legal, credit, liquidity, operational and other risks." This must be revised. Even in the short lapse of time since the first editing of the PFMIs, the risks that must be navigated on a daily basis have evolved.

In our experience with chief risk officers and their staff, a great deal of effort has been put into summarising enterprise risks into a single neat chart. Whilst that can focus the mind for some, that exercise can be mind-numbing for others. In the course of PFMI reviews, chief risk officers have smiled back silently when we have inquired as to whether the board of that infrastructure would be able to take those summary charts and present them to their fellow directors with some fluency. As the headline of Principle 3 suggests, cyber risk is not explicitly flagged. In inspections, we spend a great deal of time on various infrastructure risks, because this is the firm's historic field of expertise for banks and asset managers in respect of asset custody and other post-trade transaction administration.

As an example, during an inspection of a central securities depository, we review in detail numerous risk topics: liquidity, counterparty, asset safety, asset servicing, finances, operations, and governance and transparency. In these areas, cyber security does get raised, but again only tangentially and in a way that crosses several other risk areas. In our view, by 2016 cyber security needs to be addressed as a topic of its own.

For the PFMI inspections, we speak with heads of infrastructure risk management, and are finding that there are more and more chief regulatory officers, trained and occupying senior executive positions. Like internal audit, they usually have good access to the boards of directors. The risk charts which are produced are often summations, getting the key ideas in a complex configuration on one page. When pressed further, in our role as inspectors we get some admissions that the boards know they need to have these risk charts, but their knowledge of them is still of the superficial, tick-list variety.

At one G20 country infrastructure, one chief risk officer highlighted that his risk chart had to cover multiple kinds of risk, of which a critical one is cyber security. Like IT generally, risk questions are on the must-do list of the infrastructures we research, including when assisting with the PFMI self-assessments, but these are not areas where boards are as at ease with the topic as they need to be.

Principle 8: Settlement finality

We understand why CPMI-IOSCO highlights this particular principle in the context of cyber security, because risk of any kind to payment disruptions is a top concern for any marketplace. But in our experience, the focus of the conversation has been on the legal basis of irrevocable payment, and how enforceable that basis is in local law and regulation. We do not recall a cyber security question being raised in this context.

Principle 17: Operational risk

It is in the context of Principle 17 that the conversations with FMIs come closest to the main objective of this public comment, and in our work a great deal of the focus is on resilience and recovery of operations, including visiting back-up sites when security allows. Scalability, testing, working from the back-up sites, these are common parts of the conversations. It would be somewhat less common for the conversation to come around to prevention of attacks, shielding the infrastructure from constant probing, though that topic is invariably reviewed. We would suppose the focus has become resilience and recovery, because there is an implicit acknowledgment that there is something inevitable about the attacks in the first place.

In the firm's work on monitoring sub-custodian banks, cyber security is becoming increasingly important. Indeed, the sub-custodian banks have begun to add more of their own detailed questions to generate better information on this subject. We find the same trend in our work with prime brokers, and the questionnaire we circulate for their clients.

CPMI-IOSCO may consider adding a more explicit key consideration for the extent and frequency of staff training in cyber security risks and appropriate responses. This key consideration should include details on penetration testing, frequency of review, and processes for implementing changes to enable the infrastructure to keep ahead of this threat. Operational risks are otherwise well covered in Principle 17. A more explicit and robust Principle 17 is the logical staff counterpoint to greater focus on cyber security at the board level.

Principle 20 – FMI links

As with so much about the PFMIs, most of our conversations relative to this Principle and its Key Considerations have revolved around law and regulation – this work does come from CPMI-IOSCO, after all. We also review the simple practicalities of how they interconnect. It is our supposition that in raising Principle 20 in this context, the concern could be weaknesses in the chain when a transaction passes from one FMI to another, and at that moment a cyber penetration could be introduced into a weak link in the chain, bringing everyone down.

In our view, a more practical bent - *in addition to but not instead of* - law and regulation would lead to a welcome rebalancing of this Principle and the Key Considerations underpinning it.

Conclusion

This firm reads this consultative paper as a wake-up call to raise the level of awareness of the importance of cyber security in our ongoing conversations with infrastructures, and equally in the weightings we give them in our risk assessments. The firm's reports go to hundreds of buy- and sell-side institutions that place a daily reliance on the proper functioning of the world's financial infrastructures. A heightened sense of awareness would be a contribution to the responses the financial services industry must make, and this firm is adapting its assessments in this direction, too.

IOSCO and CPMI are to be commended for the good sense shown in leading the debate, and in these practical proposals for training. Awareness, back-ups, and rehearsal for responding to failures or attacks will all ease the ever more acute sense of vulnerability that managers of FMIs feel.

We remain respectfully yours for questions you may have,

Sincerely,

Thomas Krantz

Senior Advisor Capital Markets

Alex Harborne

Senior Analyst

CC: Simon Thomas, Jim Micklethwaite, Janet Wynn, Ana Giraldo, Steve Merry, Luis Nino, TM