



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: CPMI-IOSCO Consultative Report: Guidance on Cyber Resilience for Financial Market Infrastructures

The Securities Industry and Financial Markets Association (“SIFMA”)¹ submits this letter to the Secretariat of the Committee on Payments and Market Infrastructures (CPMI) and the Secretariat of the International Organization of Securities Commissions (IOSCO) in connection with the consultative report regarding guidance on cyber resilience for financial market infrastructures (FMIs) that was released on November 24, 2015.² We appreciate the opportunity to provide our members’ view on this important topic and are strong proponents of the harmonization of guidance and rules as they relate to cybersecurity globally. SIFMA commends CPMI-IOSCO for their leadership on this important topic and looks forward to further collaboration with them and their member agencies as we seek effective, consistent and appropriate guidance and rules to ensure the global financial markets are protected.

We support the work of global policymakers to address systemic risk in FMIs in general, and in CCPs in particular, given their increased systemic importance. The size and required use of CCPs demands careful scrutiny of how those institutions will manage a potential disruption or failure, and whether the risk concentrated in CCPs represents a new single point of failure for the entire system. While clearing members have primarily focused on ensuring high, minimum standards to prevent a default of one or multiple clearing members, we feel that safeguarding

¹ SIFMA is the voice of the U.S. securities industry. We represent the broker-dealers, banks and asset managers whose nearly 1 million employees provide access to the capital markets, raising over \$2.5 trillion for businesses and municipalities in the U.S., serving clients with over \$20 trillion in assets and managing more than \$67 trillion in assets for individual and institutional clients including mutual funds and retirement plans. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA). For more information, visit <http://www.sifma.org>.

² Link to report, <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD513.pdf>

SIFMA Comment Letter on CPMI-IOSCO Consultative Report: Guidance on Cyber Resilience for Financial Market Infrastructures

February 23, 2016

Page 2

CCPs against operational risk issues including cybersecurity risks is very much needed, and therefore this guidance for FMIs is welcomed.

Cybersecurity is a top priority for the financial industry to ensure the security of sensitive information and customer/client data, as well as efficient, reliable operations given the risks of cyber attacks. Our members and the sector as a whole along with its partners invest a tremendous amount of time, money and resources to manage cyber risks. Our members believe taking a risk-based approach enables a covered entity to develop and implement cybersecurity strategies and programs that effectively mitigate their respective technology and cyber risks. There is no one-size-fits-all approach to cybersecurity and it is only one of the many risks that a financial institution and its partners must manage, but can't eliminate.

SIFMA and its members believe that CPMI-IOSCO has and can continue to play a significant role in the future in coordinating and harmonizing guidance and rules that not only influence FMIs but also the wider ecosystem. An effective cybersecurity program starts at the enterprise level with a consistent, risk-based approach that can then be applied across different regions, products, and functions that financial services firms operate within. Creating and applying this consistent approach across the different regulatory bodies that assess firms is vital for the efficient use of limited resources and the establishment of clear, non-conflicted guidance. Further, applying a consistent approach increases the likelihood that cybersecurity will and should always be primarily rooted in risk management.

In specific response to the consultative report we submit the following general and specific recommendations and comments which we hope will be useful in further enhancing the guidance.

General Recommendations:

As stated above we view effective and consistent cybersecurity principles, guidance and regulation as catalysts to enable a covered entity to develop a cybersecurity strategy and program that is tailored to its specific situation. Regulations should encourage covered entities to take a risk-based approach, which is tailored to the threats they face and takes into account the covered entity's business model and available resources. This approach, which is less prescriptive, should provide covered entities the flexibility they need to determine how they mitigate the risk and address the regulation through the development and implementation of appropriate policies, process, and technology.

Overall SIFMA believes that the principles articulated in the consultative report create an effective foundation for FMIs to organize and manage their cybersecurity strategy, programs, and resiliency and recovery objectives. In addition, the paper provides a number of good examples and recommendations that can be leveraged by firms of all sizes and types as they consider how to improve existing cybersecurity programs. The topics covered within the paper

are comprehensive and we feel that all major items covered are appropriate to be included in a cybersecurity program.

One general area for improvement would be the organization of the guidance so that it can be more readily mapped to existing standards and frameworks used around the globe, ensuring consistency. Rather than creating another model or framework that covered entities should organize around, we suggest it would be useful to re-align this guidance, and any future CPMI-IOSCO requirements regarding cybersecurity, with the NIST Cybersecurity Framework³. The NIST Framework is a preferred mechanism for illustrating how the various components of a cybersecurity program interact and for communicating across the firm with both cybersecurity experts and non-experts who have input into and oversight over the program. While we acknowledge that the NIST Framework is maintained by a US-based standards organization; we believe that NIST has done an excellent job of trying to align the Framework to international standards such as ISO/IEC 27001 and ANSI/ISA-62443. We continue to encourage NIST to expand their international outreach that has already started with the focus on including more countries and standards bodies in the long-term ownership and management of the Framework, so its use can continue to evolve per the requirements of the financial services industry as well as many other industries that we rely on via key relationships.

Furthermore we suggest CPMI-IOSCO encourage their member agencies to do the same when they release guidance or regulations as this would help to align and harmonize policy and regulatory oversight, as well as drive efficiency in the multiple examinations that covered entities are often subject to each year. Coordination is essential to enhance the harmonization of regulatory guidance and ensures the most effective use of limited resources. The proliferation of different definitions, frameworks and methods, which in general tie back to a set of common standards (NIST 800-53, ISO 27001, COBIT 5, etc.), creates confusion and fosters an environment that makes communication and coordination more difficult to achieve. Regulators can also benefit from sharing solutions to similar compliance problems and leveraging knowledge across agencies. Consistent regulatory guidance creates an environment in which all parties can benefit as we seek the same goal of protecting the sector.

Specific Recommendations:

1. Section 3.2 – Identification and Classification, Section 8.2 Cyber Threat Intelligence & Section 8.3 – Information Sharing: Threat intelligence, situational awareness and the communication of that awareness should be included in the Identification phase of a cybersecurity program. In addition to merging content and more tightly-aligning with the NIST Framework, it eliminates the need for a separate Situational Awareness section within the paper’s suggested framework. This approach also shifts the focus of the identification process from the “keys to the castle” approach of asset discovery and

³ Link to the National Institute of Standards and Technology Cybersecurity Framework, <http://www.nist.gov/cyberframework/>

classification to the “what are they after” approach of identifying threat actors and potential vectors of attack. This change would encourage the three areas to be more tightly coupled. This is particularly important for most FMIs, which should have a different and more specific focus on availability and ensuring the integrity of data and systems, than on data confidentiality (personal data, payment card data), which currently make most of the headlines around cybersecurity issues in the financial sector. For FMIs, the threat of an operational disruption is much more relevant, and the choice of specific assets to target is less important than disrupting any of the many interconnected links that would result in an outage or market instability. To that end, if FMIs apply a risk-based approach to the problem, identification efforts should be focused on identifying threat actors, tools, and methods so defenses may be properly positioned and tested and critical assets can be highlighted based on this information.

2. Section 7.2 – Comprehensive Testing Program: This section provides a complete and comprehensive set of tests that can be run to address cyber resilience. We agree with the non-prescriptive approach that has been designed and the independence these tests should have from the regulatory agencies that may be evaluating the results or the actions taken as a result. Firms should maintain the flexibility to design and run tests specific to their situation and regulators should refrain from imposing one-size-fits-all approaches that test firms in the same way. Regulatory agencies currently developing detailed testing requirements, such as the US Commodity Futures Trading Commission, should support approaches to operational assessment (including penetration testing and vulnerability assessment) that are safe, globally scalable and risk-based, so as to reduce negative impacts on operations and avoid creating new risks. The mandatory use of specific external parties for penetration testing and other forms of operational assessment may introduce additional risks, which regulators ought to understand and seek to mitigate. Language to this effect could be included in the CPMI-IOSCO guidance.
3. Section 6.2 – Incident Response, Resumption and Recovery: The general premise of operational impairment and recovery is well-addressed in existing guidance and regulation where recovery time objectives are appropriately and adequately considered. Although we understand that this guidance should be in line with Principle 17 (Operational Risk) of the Principles for Financial Market Infrastructures (PFMIs) and although we support the intent behind the requirement for two-hour recovery following a cyber disruption, we would like to emphasize that this may be unrealistic and/or exceedingly expensive to design and achieve in practice. For the purpose of cybersecurity-specific guidance, the notion of resumption in a set time period and specifically within two hours is exceedingly complicated and warrants further discussion amongst stakeholders to clarify what it is exactly and what can be achieved in a two-hour window.

While there are common processes and considerations that can be shared and applied for both kinetic events and cyber events, the actual decisions made and actions taken will differ greatly between the two event types. The scenarios that this paper considers, as

highlighted in section 1.1.3 (cyber risks are unique), make it near impossible to quantify recovery time objectives. We do acknowledge though that completing final settlement at least by end-of-day should be of the utmost importance for FMIs.

4. Section 6.2.3 – Contingency Planning: Another area of concern is the notion of “manual processing” discussed in section 6.2.3. The idea that an FMI (or any firm of significant size and scale) should be processing transactions manually seems unrealistic, and may only be a solution in very rare situations. Technology is central to the handling and routing of transactions, the surveillance of the networks that handle those transactions and the overall risk management and compliance programs to inform decision making. FMIs and firms alike have been working for years to eliminate the manual processing of transactions in order to reduce operational risk and drive consistency. We believe that operating a manual process during or after a crisis event could create further risk for the FMI and the firms that rely on and participate in the venue they operate.

The lack of necessary controls, the possibility that the usual set of data and information is not available and the reduced confidence in the system to operate as designed should be a significant set of factors in driving FMIs to instead re-establish production or leverage back-up systems supported by a minimum set of technology. SIFMA suggests that CPMI-IOSCO and other regulators start using the term “alternate systems or alternative systems” which could be technology options that may have less functionality or lower capacity to execute and process transactions but still have minimum levels of control, surveillance and reporting.

One final point for consideration is that when a large technology outage or cyber attack occurs it may be a better and safer option for FMIs and their participants not to operate as opposed to adding risk to an unresolved situation in the markets. This is an issue that merits further discussion amongst stakeholders.

5. Section 4.2.3 – Strong ICT Controls: This section wisely does not attempt to be comprehensive around ICT controls as each firm needs to determine what is most critical to it based on a risk assessment, the threats faced and the resources available. However, the specific examples cited seem to communicate a prioritization of controls. We are not sure if that was the intention, but based on a review of the section that appears to be the case. Based on this, the four examples chosen can be improved upon in our opinion or language should be added to note these are just illustrative of what should be considered. All are important where appropriate, but should not consume the majority of examination, statute, or intent since they do not take context and exposure into account. Other ICT controls we suggest for consideration as possibly more important for an FMI include.
 - a. Access Control: Documented, repeatable and audited processes should be in place governing the process from requesting through granting and recertifying access to sensitive systems or data.

- b. **Intrusion Detection and Visibility:** Networks that are used for critical functions and thus likely to be targeted in attacks must have appropriate instrumentation and be monitored for suspicious activity and abuse.
 - c. **Internet Egress:** Discretionary content filtering must be in place to dynamically identify malicious web sites and block access from employee and data center systems.
 - d. **Web Application Security:** Where Internet-based connectivity to internal systems is present, network-based systems independent from web servers must have visibility into traffic and the ability to identify and block malicious activity.
 - e. **Network Segmentation:** A default-deny philosophy should be enacted via the use of firewalls and access control devices that prohibit unnecessary communication among systems.
 - f. **Remote Access:** Internet-based remote access for employees must require multi-factor authentication to nullify the value of credential capture.
6. **Section 4.3 – Interconnections:** This section operates under the premise that service providers have elevated access to sensitive systems and thus tasks FMIs with the incredibly difficult task of ensuring service provider security reaches the same level of control as the internal program of an FMI. A more realistic approach to vendor and partner risk is to categorize and prioritize the FMI’s external links, segment networks, minimize access outright and monitor the residual vectors of access closely. Focus should be on treating external connections similarly to connections with the Internet, terminating them outside the network perimeter, only allowing specific required and approved protocols and sources, and monitoring the resulting traffic with behavioral analytic tools.
7. **Section 6.3.2 – Data Integrity:** Different FMIs falling under CPMI-IOSCO guidance will have different applications and methods of integrity checking and re-establishment of a baseline if they are affected. For some FMIs and in some scenarios, recording participant intent and replaying it will be appropriate; for many others, however, the only tenable path is to establish a point of reliability loss, invalidate transactions submitted after that point and return to a previous checkpoint to resume processing. Flexibility needs to be afforded to FMIs to determine what is appropriate not only for the business they operate and market function they support but for the specific scenario and the impacts that are being managed as they attempt to resume normal operations. Additionally, in many cases the participants at an FMI may be the only entities properly positioned to conduct and/or support reconciliation activity. Tasking FMIs with “independent reconciliation” is prescriptive and dangerous and may not produce the correct outcome, especially when participants may on a regular basis and during normal operations already successfully be driving and informing reconciliation requirements directly.
8. **Section 6.2.4 – Planning and Preparation and Section 7.3 – Coordination:** Exercises and testing are well-recognized aspects of good cyber resilience that can enhance coordination and resiliency. The guidance document would benefit from additional

SIFMA Comment Letter on CPMI-IOSCO Consultative Report: Guidance on Cyber Resilience
for Financial Market Infrastructures

February 23, 2016

Page 7

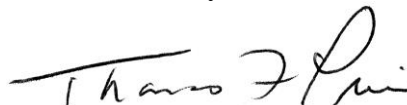
references to the role that exercising can play in strengthening an FMI's cyber resiliency. This would also be helpful in better understanding impacts on the ecosystem. Appropriate language could be included within Planning and Preparation (section 6.2.4) and Crisis Communication (section 6.4.3) and the relevant language on exercises in Testing (section 7) could also be broadened. Added language on exercising could also stress the value of sector-wide exercises, specifically within Coordination (section 7.3), as a means to improve sector resiliency.

9. Section 8.3 – Information Sharing: We are supportive of the inclusion of guidance on information sharing though as currently phrased this section lacks a perspective on the value of sharing information in order to prevent incidents from occurring. Information sharing needs to take place prior to, during and after an incident to be effective and practiced. This section should be amended to highlight the value of information sharing beyond incident response, i.e. to emphasize how FMIs may share cyber threat information with one another and other stakeholders (vendors, law enforcement and national governments) in the ecosystem to prevent incidents.
10. Section 4.4 – Insider Threats: A call for analytics and screening on employees seems appropriate for FMIs given their importance and the focus on protecting critical systems from external threats. While the topic of insider threats has often been associated to access controls in the past we agree that individuals with elevated permissions should be monitored closely as attacks concerning destruction or destabilization will have far reaching consequences. As a global principles document that applies to FMIs that operate in many countries around the world, there may be some challenges in meeting this requirement as a result of the country specific laws regarding monitoring, privacy and the screening of employees. We suggest that this be noted in the section as a challenge that needs to be assessed as the FMIs' policies are developed.

* * *

SIFMA appreciates the consideration that CPMI-IOSCO has given to these issues and the concerns that have been raised above. If you have any questions or require further information, please contact me at (212) 313-1260 (tprice@sifma.org) or David Strongin at 212-313-1213 (dstrongin@sifma.org).

Sincerely,



Tom Price
Managing Director