EBF_019611

19 February 2016

CPMI Secretariat
by e-mail: cpmi@bis.org

IOSCO Secretariat
by e-mail: consultation-2015-09@iosco.org

TARGET Working Group comments on the CPMI/IOSCO Consultative Report on Guidance on cyber resilience for financial market infrastructures

The TARGET Working Group (TWG) would like to thank the CPMI/IOSCO for the opportunity to comment on the above report. The TWG represents the European payments industry in discussions with the ECB and Eurosystem on issues relating to the TARGET 2 system and its interfaces with other market infrastructures.

The TWG fully recognises the growing threat to critical market infrastructures from cyber risk and believes that this report will be useful to FMIs. However, whilst we agree with the various recommendations when considered in isolation from each other, we are concerned that taken together they may inadvertently cause problems. We explain our concern in more detail below.

Section 1.3.6 states that relevant regulatory, supervisory and oversight authorities, in carrying out their responsibilities, are urged to implement the guidance within the legal framework of the relevant jurisdiction. Whilst at first sight this statement may appear innocuous, it gives rise to two potential issues, namely:

- participants connected to an FMI and affected by the FMI's decisions may be located in different jurisdictions and thus subject to different law and /or regulation.
- in our experience, competition law in particular may have unintended effects.

We believe that these issues are likely to become increasingly important as jurisdictions attempt to counter cybercrime in a variety of sectors including banking. For example, we have read with interest the European Parliament's Press Release dated 7 December 2015 entitled "MEPs close deal with Council on first ever EU rules on cybersecurity".

We also have recent experience of a security problem to which we believe interpretation of European competition law has contributed. Whilst this is only one example, it seems reasonable to assume that similar issues could arise elsewhere in the world although we hasten to add that we have no hard evidence to support this assumption. We note that:

- section 2.2.5 of the report refers to the need to mitigate the cyber risks an FMI poses to its participants.
- section 4.3.1 states that an FMI's participation requirements should be designed to ensure that they adequately support its cyber resilience framework.
- the "Broad relevance" part of the Executive summary states that the markets' overall cyber resilience is dependent not only on the resilience of a single FMI, but also on that of interconnected FMIs, of service providers, and of participants. Furthermore, the Collaboration section makes the point that effective solutions may necessitate collaboration between FMIs and their stakeholders.

The problem that has arisen is that an FMI has insisted that a token is used by participants for security purposes when sending messages to the FMI with one reason given being that European competition law doesn't allow differentiation between competing network providers notwithstanding that one of the providers is SWIFT which is used by many banks for a large number of high value messages but where the message security does not involve use of a token. From a participant point of view, quite apart from the need to differentiate between different types of SWIFT traffic, the greater concern is potential conflict with both internal and possibly regulatory requirements which may mean that such a token is not immediately available in the event of an emergency switch to a contingency site. Needless to say, we have raised this issue with the FMI concerned but we believe it illustrates the wider issue of potential conflict between legal and regulatory requirements.

We do, of course, recognise that CPMI/IOSCO cannot override applicable law and regulation. However, we suggest that an additional section(s) is added to the report, including the Executive summary, drawing attention to the possibility of such conflict and recommending discussion with all stakeholders to seek to ensure any such conflict is identified and addressed in advance of implementation. We have deliberately referred to "all stakeholders" since when dealing with interconnected FMIs and institutions, the effect may spread beyond those most closely connected to the FMI.

Whilst recognising that section 1.2.2 of the report makes it clear that the Guidance is principles based, nevertheless a number of our consultees have expressed surprise about the lack of more specific technical guidance. Our attention has also been drawn to the large number of standard setting bodies and codes with slightly different agendas ranging from the National Institute of Standards and Technology (NIST) in the USA to the CBEST framework in the UK with its emphasis on controlled, bespoke, intelligence – led cyber security tests. In such a fast moving area as cyber security, we do of course recognise that a global publication of this nature has, of necessity, to be high level. Nevertheless, the TWG believes that it would be useful to add a prominent note drawing readers' attention to the need to comply with all applicable laws and regulatory requirements including those related to detailed technical standards.

Finally, we believe that section 6.2.2 would benefit from clarification about what happens when the failure occurs within 2 hours of the normal end of day. To achieve this, we would suggest deleting from "and to enable itself" to the end and substituting "The FMI should also have plans in place to enable itself to complete settlement by the end of the day of the disruption even where the failure occurs within 2 hours of the normal end of day. Whether this is achieved by extending the end of day or other means is a matter for the FMI."

(We also wondered about any DNS systems which may still not settle at the end of the calendar day but we assume the phrase "end of the day" is considered to cover such a scenario.)

We hope that you will find these comments useful and look forward to seeing the final report.

Yours sincerely,

Roger Jones
Chairman
TARGET Working Group

Denisa Mularova
Secretary
TARGET Working Group