Dear Madame/ Sir,

Thank you for the opportunity to comment on the draft guidance on cyber resilience for financial market infrastructures. We have found it very useful and important as for cyber resilience issues. It reflects relevant security issues, that should be addressed somehow either in the supervisory or oversight framework. We think that this guidance fills a gap in the current oversight practice because FMI's security policies and authorities' oversight/supervisory activities still mostly focusing on physical and logical protection and only partly on cyber issues.

The oversight team of Magyar Nemzeti Bank (the central bank of Hungary) has collected some general and specific issues regarding the guidance, please find below:

1. One of the main aim of PFMI was to collect and merge all the relevant standards and recommendations relating to FMIs in one set of principles which contributes to the harmonised application of them. What is the plan with the current guidelines? Are you planning to build them into the PFMI (updating the original 2012 document) or we should it be applied independently?
2. Is it planned to publish an assessment methodology that includes key considerations and assessment questions?
3. When do you expect the first assessment against cyber risk to be done (what is not included in Principle 17)?
4. To which standards refers the report when speaks about 'leading-practice cyber resilience standards'? It is also a question relating to this issue, that which body (authority or standard maker) will keep the list of these standards up to date (see 4.2.1 in the guidance)?
5. We think that cyber resilience is an issue for the whole banking sector not only for FMIs and the measures taken by them can be applicable also for the FMI. It is not investigated in the report how the existing practice and standards from the banking sector could be taken over by FMIs.
6. Who provides the mandate for FMIs or authorities (overseers) to have full access to the information necessary to assess the cyber risk arising from the service provider if it is a cross-border entity, especially a non-EU service provider? How should the cyber risk recommendations be incorporated into the contractual arrangements already in place (especially if it is a monopole service provider )? (eg. How can we assess as an overseer of the Hungarian FMIs that an India-based service provider comply with the requirements of cyber risk?). (see 4.3.1 in the guidance)
7. Was it considered while preparing this guidance that the cyber risk sensitivity of an FMI using open communication channels (internet-based solutions) is very much different from those using closed communication channels like SWIFT or own proprietary networks?
8. How can overseers assess whether an FMI is already prepared for the' vulnerabilities that are not yet publicly known' (see 5.2.2 in the guidance)?
9. According to our reading FMIs should gather and analyse cyber threat intelligence information. We think that proper arrangement between FMIs and national intelligence bodies would be more effective because it requires specialised knowledge and practices (see 8.2 in the guidance).

Best regards,

Cecília Pintér

The Central Bank of Hungary
**CECÍLIA PINTÉR**
Senior analyst