5th June 2018

European Central Bank
Directorate General - Market Infrastructure and Payments
Sonnemannstrasse 20, 60314
Frankfurt am Main, Germany

Via Electronic Submission

Re: CYBER RESILIENCE OVERSIGHT EXPECTATIONS (CROE) FOR FINANCIAL MARKET INFRASTRUCTURES

FIA welcomes the opportunity to respond to the public consultation on the draft cyber resilience oversight expectations for financial market infrastructures ("the Guidelines") issued by the European Central Bank (ECB).

FIA is the leading global trade organization for the futures, options and centrally cleared derivatives markets, with offices in London, Singapore and Washington, D.C. FIA's membership includes clearing firms, exchanges, clearinghouses, trading firms and commodities specialists from more than 48 countries as well as technology vendors, lawyers and other professionals serving the industry. FIA's mission is to support open, transparent, and competitive markets; protect and enhance the integrity of the financial system; and promote high standards of professional conduct. As the principal members of derivatives clearinghouses worldwide, FIA's member firms play a critical role in the reduction of systemic risk in global financial markets. Further information is available at www.fia.org.

FIA is a voice for the cleared derivatives industry on cybersecurity issues. In the United States, FIA is a member of the Financial Services Sector Coordinating Council (FSSCC),[1] the Financial Services Information Sharing and Advisory Center (FS-ISAC),[2] and participates in regular public/private sector discussions on cyber security with the US government's Financial Banking and Information and Infrastructure Committee (FBIIC).[3] FIA is a stakeholder in the FSSCC initiative for regulatory harmonization for cyber security regulation based on the National Institute of Standards and Technology (NIST) framework.[4] FIA has also participated in the US Treasury's Hamilton Series of cyber security exercises and has worked with its members to provide business continuity-oriented workshops regarding hypothetical cyber events within the cleared derivatives industry.[5]

Introduction

Financial market infrastructure (FMI)—including trading venues, clearing houses and settlement systems—is increasingly electronic in nature. Electronification has brought many benefits, including increased automation, shorter transaction times, and the ability to conduct business efficiently in a global economy.

Cleared derivatives have increasingly become media for risk management on a global basis, and the infrastructure to support the trading, clearing, and settlement of cleared derivatives has evolved to provide a near 24 x 7 interconnected network of counterparties, trading venues, clearinghouses/central counterparties (CCPs), custodians, and technology providers. Many of these parties have a global footprint and engage in activities across

[1] https://www.fsscc.org/

[2] https://www.fsisac.com/

[3] https://www.fbiic.gov/

[4] FSSCC letter to Mr. Edwin Games, National Institute of Standards and Technology, April 10 2017: https://www.nist.gov/sites/default/files/documents/2017/04/21/2017-04-10_-_fsscc.pdf

[5] FIA MarketVoice - Insight: The Dark Side of Innovation, A message from Walt Lukken, President and CEO, FIA: https://marketvoice.fia.org/issues/2017-12/insight-the-dark-side-of-innovation

many different types of financial services. For example, global investment banks may operate in many jurisdictions and provide many types of services that are regulated by different types of financial oversight authorities. In many financial institutions, the cleared derivatives business may be relatively small and rely on shared services within the institution to provide cyber security and vendor management functions.

While we note that the Guidelines focus on Prominently Important Retail Payment Systems (PIRPS), Other Retail Payment Systems (ORPS), Systemically Important Payment Systems (SIPS) and TARGET-2 Securities (T2S), there is substantial overlap of institutions involved in these functions with those also involved with the trading, clearing and settlement of cleared derivatives on a global basis. As a result, various requirements in the Guidelines may become difficult to apply—notably expectations on the role of senior executives, which may be governed by requirements in firms' home jurisdictions.

FIA questions whether the Guidelines provide sufficient flexibility to accommodate the global nature of financial institutions. We encourage the ECB to issue Guidelines that complement and defer where appropriate to regulatory frameworks in other jurisdictions. In our view, a more principles-based approach to the Guidelines would better foster innovation and resiliency, especially as technology develop with ever-increasing speed and complexity. Prescriptive regulation, by contrast, imposes rigid requirements that may be difficult to adopt for global institutions that provide diverse financial services, risks inhibiting innovation and technological evolution, and requires frequent refresh to avoid becoming outdated.

The proposed Guidelines do not recognize the global nature of FMIs and their participants

FIA believes that regulation should be designed to meet its purpose and be appropriately harmonized with similar regulation from comparable bodies to avoid inadvertent conflict with compliance.

By way of example, financial institutions in the United States may be overseen by multiple regulators, including the US Treasury, the Office of the Comptroller of the Currency (OCC), the Federal Reserve, the Federal Deposit Insurance Corporation (FDIC), the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC), the National Futures Association (NFA) and the Financial Industry Regulatory Authority (FINRA), as well as many state regulators such as the New York State Department of Financial Services. In the last few years US regulators have issued many cyber security requirements that have duplicated each other and caused financial institutions to spend unnecessary time ensuring compliance with conflicting regulation rather than concentrating on the protection of their systems. Indeed, FSSCC has led an initiative on cyber security regulatory harmonization in response to these conflicting requirements.[6]

FIA is a proponent of principles-based cyber security regulation that leverages industry standards and best practices (such as those referenced in section 1.2 of the Guidelines). Overly prescriptive requirements from a specific authority may inhibit the ability of a global business to implement technology, and potentially lead to "ring-fencing" of technology and systems for the same financial services offered globally due to conflicting requirements in different jurisdictions. "Ring-fencing" in this manner may lead to operational inefficiencies and higher operating costs across different jurisdictions and cause global businesses to withdraw their services when those costs become difficult to justify.

Accordingly, FIA believes that the Guidelines should be more flexible regarding how ECB expects global FMIs and their participants operating within the Eurosystem to implement similar practices across their global businesses. Practices that are tailored to the nature of an institution will also be more effective when implemented than rigid rules that may not consider the operational reality of that institution's business.

---

[6] Testimony of Christopher F. Feeny on behalf of The Financial Services Roundtable before the US Senate Committee on Homeland Security & Government Affairs hearing entitled "Cybersecurity Regulation Harmonization": https://www.hsgac.senate.gov/imo/media/doc/Testimony-Feeney-2017-06-21.pdf

We encourage ECB to review its Guidelines with similar requirements in other jurisdictions, and particularly the lessons learned from their implementation—some of which may predate the CPMI/IOSCO guidance on cyber resilience for FMIs published in June 2016.

Prescriptive cyber resilience expectations may impact the ability to innovate

The cleared derivatives industry has thrived through its ability to innovate, particularly through its use of technology to expand services across the world. FIA is particularly concerned that over-prescriptive regulation around cyber resilience may inhibit the ability for the industry to adopt—and adapt—emerging technology to improve operational efficiency.

Cyber security and resiliency are critical to a safe global financial system, yet it is also important to ensure that firms implement processes that are proportionate to the size of their business globally. We have observed that financial institutions increasingly outsource technology functions and solutions to third-party providers, and a key factor to onboarding a new provider is how the provider meets the cyber security requirements of the procuring firm.

FIA appreciates that the Guidelines address different levels of maturity of FMIs—notably baseline, intermediate and advanced – and sets expectations accordingly, without requiring all FMIs to meet a standard level of compliance from when the Guidelines take effect. However, potential "top-down" or "one-size-fits-all" regulation when an FMI or its participants are identified at an advanced maturity level—particularly with regards to change and patch management, supplier and third-party security management, and testing—may impact the ability for an FMI or its participants to quickly adopt new technology solutions.

As we have noted previously, practice that is appropriately tailored to the sophistication of the nature of an institution and its business units is often more effective, and instead of detailing expectations, the Guidelines should encourage FMIs and their participants—regardless of their maturity level—to adopt industry standard frameworks such as ISO 27001 or perform risk assessments of their own systems and those of their technology partners using ISO 27005.

Conclusion

FIA supports encouraging cyber security and resilience across the global financial industry. The cleared derivatives industry is global in nature, and FIA believes that FMIs and their participants should focus on cyber security practice best suited for their sophistication and scale globally, rather than having to adapt or "ring-fence" practices to local requirements such as those proposed in the Guidelines.

While we support the aim of ECB to ensure that there is appropriate cyber resilience within the Eurosystem and the recognition that FMIs and their participants may be of different levels of maturity, we strongly question whether the Guidelines should prescribe practices around every level of governance, identification, protection, detection, response and recovery, testing, situational awareness, and learning and evolving. As the Guidelines note in their introduction, industry standards and frameworks for best practices already exist and should be adopted by businesses as part of their policies and procedures. These standards and best practices will continue to evolve together with technological innovation.

To that point, we suggest that ECB adopt a more principles-based approach that encourages best practice and allows businesses to implement cyber security frameworks appropriate to their size, sophistication, and global reach. This will allow FMIs, their participants, and other stakeholders to focus on their actual resilience rather than their regulatory compliance.

Respectfully submitted,

Greg Wood
Senior Vice President of Global Industry Operations & Technology