February 28, 2023

Ms. Petra Hielkema
Chairperson
European Insurance and Occupational Pensions Authority (EIOPA)
Westhafenplatz 1
60327 Frankfurt am Main
Germany

Re: EIOPA Consultation on Methodological Principles of Insurance Stress Testing – Cyber Component

Dear Ms. Hielkema:

The Institute of International Finance (IIF) and its insurance members are pleased to respond to EIOPA's consultation on the methodological principles of insurance cyber stress testing. We appreciate EIOPA's keen interest in this topic and its efforts to enhance its stress testing capabilities. The IIF has been actively engaged in thought leadership and advocacy on cyber resilience and cyber underwriting for the insurance and broader financial services sector for several years and we recognize the importance of active dialogue on these subjects.

Comments Related to Cyber Stress Testing in General

We encourage EIOPA to adopt a focused, proportionate and practical approach to stress testing that recognizes the need for flexibility and appropriate simplifying assumptions. We also welcome continued stakeholder involvement in the development of specific scenarios, as the industry and insurance industry experts are well placed to collaborate with EIOPA in order to identify the most material cyber risk exposures and, thus, the most meaningful stresses and scenarios to analyze. Consultation with industry groups on proposed scenarios and stress test specifications could help to refine exercises and produce more decision-useful results for both supervisors and firms.

We appreciated the flexible approach to simplifications and approximations that EIOPA demonstrated in the latest round of liquidity stress testing and we welcome a similar approach to cyber stress testing. We encourage EIOPA to allow for simplifications and approximations as the state of the art of cyber stress testing evolves and improves. Given the evolving state of cyber risk management, data may not be available at the level of granularity that is ideal for EIOPA and we encourage the recognition that firms may use estimates, proxies and approximations and submit higher level, less granular information until the robustness of data improves over time.

The choice of a group or solo approach should be determined by the insurer based on the structure of the firm, its information technology and risk management architecture and how the risk is managed internally. We encourage EIOPA to offer flexibility to firms to determine whether a group or solo approach is appropriate. EU-headquartered companies should liaise with their group supervisors to discuss any issues related to stress testing at the group versus solo level, rather than with individual jurisdictional supervisors. With respect to groups headquartered outside of the EU, EIOPA should limit its requirements to the EU-based operations.

Given the sensitivity of the data that would be provided to EIOPA in cyber resilience and cyber underwriting stress testing exercises, we note the need for strict protocols to ensure the security and confidentiality of this information. We encourage the release to supervisors of high-level, aggregated and anonymized data absent a clear supervisory need for more granular information regarding an insurer.

Additional Comments Related to Cyber Resilience Stress Testing

Large global insurers are running multiple cyber resilience scenarios for various regulators and supervisors as well as internal scenarios for risk management purposes. Consideration should be given to allowing firms to supply internal analyses in lieu of supervisory exercises in cases where materially equivalent outputs would be available. This flexibility would reflect the bespoke, decision-useful information that firms use in their day-to-day risk management and strategic planning and would have the added benefit of incentivizing insurers to improve their internal stress testing and scenario analysis capabilities. Internal scenarios would also better reflect the conditions that would have the greatest impact on the firm.

We encourage a primary focus on the impact (to the insurer) rather than on the cause of the incident (as reflected in Paragraph 80 of the Discussion Paper with respect to disruptions caused by an interruption of services by a third-party provider). The characterization of an incident as malicious does not translate into a necessarily greater impact on the insurer. However, we realize that there may be some benefit to identifying and separately analyzing malicious incidents as contrasted with operational errors for the assessment of insurers' own cyber resilience, as malicious incidents will have different threat agents, frequency and duration. We agree that the consideration of regulatory fines and legal judgments against an insurer arising from a cyber incident would unduly complicate the analysis.

Recognizing that the development of broader operational resilience testing is out of the scope of the Discussion Paper, we encourage EIOPA, to the extent feasible and practicable, to align its cyber resilience stress testing to the requirements of the Digital Operational Resilience Act (DORA) and to avoid duplication with any analyses conducted in the implementation of DORA. Moreover, the implementation of measures in accordance with DORA should be given full credit in determining compliance with EIOPA's cyber resilience stress testing framework and factored into companies' risk assessments.

Insurers employ a range of mitigating measures to reduce the potential incidence and impact of cyber risks, one of which is the purchase of cyber insurance. EIOPA's stress testing framework should explicitly acknowledge and account for the benefit of cyber insurance coverage.

Additional Comments Related to the Underwriting of Cyber Risks

For purposes of the cyber underwriting exercise, EIOPA should recognize and reflect in its request for data the differences in access to data between direct insurers and reinsurers. We also reiterate our more general comments regarding data availability, which may vary among stress test participants and necessitate the use of estimates and proxies.

In designing a stress test, EIOPA may find it helpful to consider the lessons learned from the cyber underwriting stress test exercises conducted by a number of national supervisors, including the U.K. PRA, the Singapore MAS and the National Bank of Belgium.

We appreciate the opportunity to respond to this important consultation and welcome avenues for dialogue on these issues, which are of critical importance to the IIF's global insurance members.

Respectfully submitted,

Mary Frances Monroe, IIF