December 14, 2022

Mr. Steven E. Seitz
Director
Federal Insurance Office
Department of the Treasury
1500 Pennsylvania Avenue, NW
Washington, DC 20220

Re: Request for Comment on Potential Federal Response to Catastrophic Cyber Incidents; https://www.govinfo.gov/content/pkg/FR-2022-09-29/pdf/2022-21133.pdf

Dear Director Seitz:

The Institute of International Finance (IIF)[1] and its insurance member firms welcome the opportunity to respond to the Federal Insurance Office's (FIO) request for comment on a potential Federal insurance response to catastrophic cyber incidents.

We commend FIO's focus on the important role of the insurance industry in facilitating financial risk transfer, strengthening cyber hygiene, and increasing resiliency through the cyber insurance market. We also appreciate FIO's close coordination with the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) on the assessment of the extent to which risks to critical infrastructure from catastrophic cyber incidents and potential financial exposures warrant a Federal insurance response. We note that the IIF has responded to CISA's Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) and our response is attached to this letter for your information.

As FIO notes in its request for comment, CISA has quoted estimates of potential losses from severe cyber incidents that indicate that these losses may range from $2.8 billion to $1 trillion per event for the United States. Moreover, the effects of severe cyber incidents are not limited to the initial target but may spill over to economically linked firms, magnifying the damage to the U.S. economy and severely challenging the ability of the insurance industry to respond with adequate cover. While catastrophic cyber incidents can impact each of CISA's 16 critical infrastructure sectors,[2] our response to FIO's request for comment reflects the views of the IIF's insurance members on the impact of catastrophic cyber incidents and potential Federal insurance program.

[1] The Institute of International Finance (IIF) is the global association of the financial industry, with about 400 members from more than 60 countries. The IIF provides its members with innovative research, unparalleled global advocacy, and access to leading industry events that leverage its influential network. Its mission is to support the financial industry in the prudent management of risks; to develop sound industry practices; and to advocate for regulatory, financial, and economic policies that are in the broad interests of its members and foster global financial stability and sustainable economic growth. IIF members include commercial and investment banks, asset managers, insurance companies, professional services firms, exchanges, sovereign wealth funds, hedge funds, central banks, and development banks.

[2] https://www.cisa.gov/critical-infrastructure-sectors

In response to FIO's threshold question, the IIF believes that there is a need for a further comprehensive study of whether and how the Federal government could and should address various potential catastrophic cyber incidents that are beyond the risk appetite and capacity of the private cyber insurance market before making a definitive judgment as to whether and when a Federal response is appropriate. While the private market for affirmative cyber insurance is still maturing, it has demonstrated to date a risk appetite to cover cyberattacks that may be attributed to a wide variety of actors, with the exception of nation-state initiated or sponsored attacks, for which the private market generally has a lower risk appetite.

The IIF would recommend that FIO consider the following as part of any comprehensive study on a potential Federal insurance program for catastrophic cyber incidents:

Avoid Supplanting the Private Cyber Insurance Market:

Importantly, in considering the design of a Federal program, FIO and its government partners should recognize the important role that cyber insurers and reinsurers already play in providing coverage for cyber risks. This role should not be supplanted by Federal programs, as recourse to the private markets is the first best option for addressing these risks. Cyber (re)insurers have considerable experience in underwriting complex risks and in working with their customers to advance sound risk management practices. As the cyber insurance market continues to mature, insurers are developing more robust cyber hygiene requirements, often as a condition of cover for affirmative cyber risk. Additionally, insurers also support cyber resilience by providing customers with pre-incident services, such as vulnerability testing and reviews of cyber governance, proficiency, and infrastructure. They can also assist their customers post-incident with services to evaluate impacts and help implement response and recovery plans.

While the private cyber insurance market should remain the primary source of cyber risk coverage, there could potentially be extraordinary cyber incidents that rise to the level of a catastrophic exposure that could exceed the risk appetite and capacity of the private market and would warrant a Federal response. A well-crafted Federal response would need to be carefully calibrated such that it neither acts as a ceiling that limits the growth and evolution of the cyber insurance market, nor compels insurers to cover losses that would typically be excluded.[3] A Federal program could be helpful to the extent it provides more certainty to all market participants, while allowing the cyber insurance market to grow organically and provide more insurance capacity through, for example, capital markets solutions such as insurance-linked securities (ILS).

Any potential Federal response should also be designed in a manner that is likely to increase market confidence in cyber insurance solutions by providing certainty as to when and to what extent a Federal program would be implicated and as to the scope and limits of coverage. In particular, coverage limits should be clearly delineated for companies with global operations.

Moral Hazard:

[3] As was noted in the June 2022 GAO Cyber Insurance report, insurance policies generally exclude losses from events with potential catastrophic and systemic effects, such as acts of war or infrastructure outages. Cyber insurers have also been taking steps to reduce their exposure to systemic cyber events through cyber warfare exclusions. https://www.gao.gov/assets/gao-22-104256.pdf

Any Federal response should be designed carefully so as not to inadvertently lead to moral hazard and undue reliance on a Federal program as a substitute for good cyber hygiene, sound risk management practices, and adequate cyber insurance cover. Just as cyber (re)insurers require policyholders to demonstrate good cyber risk management practices, payment of claims under any Federal program should be conditioned on compliance with sound cyber risk management.[4] At the same time, such a program should prioritize a risk-based approach to managing the cybersecurity risks across the digital value chain, taking care not to create duplicate standards that result in additional compliance burdens for policyholders without meaningful improvements to cyber risk management.

Design Considerations for a Potential Federal Insurance Program:

In exploring the design of a potential Federal insurance program, FIO and CISA should be guided in developing a Federal response by lessons learned from the implementation and administration of the Terrorism Risk Insurance Program (TRIP), the National Flood Insurance Program (NFIP), the Paycheck Protection Program (PPP) and the Federal Crop Insurance Program (FCIP) but should not necessarily use these programs as a template for a response to catastrophic cyber incidents. The design of a catastrophic cyber program will differ in terms of its goals, beneficiaries, and key elements and will need to reflect the role of private industry in providing cyber cover.

The following are responses to specific questions raised in the request for comment:

*What types of cyber incidents could have a catastrophic effect on U.S. critical infrastructure?*

We would expect that catastrophic exposures affecting U.S. critical infrastructure broadly, including the financial services sector, would be those associated with significant concentration and accumulation risk, such as an attack on a third-party service provider on which a substantial portion of the financial services sector relies. A catastrophic cyber incident could imperil financial stability through its second-order effects on other industries, individuals, and data integrity, and could weaken confidence in the U.S. financial system. Other sources of catastrophic exposure could arise from attacks on market infrastructure and payment, clearing and settlement systems.

*What cybersecurity measures would most effectively reduce the likelihood or magnitude of catastrophic cyber incidents? What steps could the Federal government take to potentially incentivize or require policyholders to adopt these measures?*

IIF member insurers have been working with their policyholders to improve cyber hygiene, resilience, and security as part of a holistic approach to cyber insurance. Increasingly, cyber coverage is predicated on adherence to cybersecurity practices that meet or exceed certain standards and is priced on the basis of the policyholder's cybersecurity risk profile and its level of sophistication and track record in mitigating those risks. Many insurers base their analysis of a policyholder's cybersecurity profile on a scoring

[4] We note that the Federal Energy Regulatory Commission has proposed to provide incentive-based rate treatments for the transmission and sale of electric energy by utilities that invest in advanced cybersecurity technology and participate in information sharing programs: https://www.federalregister.gov/documents/2022/10/06/2022-21003/incentives-for-advanced-cybersecurity-investment-cybersecurity-incentives. Similar incentives could be built into any Federal program advanced for catastrophic cyber insurance coverage.

mechanism that considers a wide range of factors including the number and types of devices deployed (including the number of devices that are end-of-life or end-of-sale and no longer receiving updates or support), the number of individuals about which the entity stores data, the use of encryption, endpoint detection and response (EDR) and endpoint antivirus protection and the use of multi-factor authentication (MFA). The use of encryption, EDR, endpoint antivirus protection and MFA are often minimum standards that apply as a condition of coverage. The holistic approach also incorporates the development of a roadmap and timetable for continuous improvements of cybersecurity defenses.

A holistic approach that ensures the existence of strong cyber risk management, resilience, and cyber hygiene practices as a condition of coverage should be integrated into any Federal program in order to reduce moral hazard and the risk to the Federal government and taxpayers. The Federal government could encourage private-led initiatives to develop risk-based industry standards for cyber risk management. A harmonized industry standard could make compliance easier to understand and gauge, better enabling insurers to provide detailed examination and assurance. This could help increase the scope of coverage, especially for small and medium-sized businesses that would otherwise have difficulty meeting the requirements needed to obtain cyber insurance. Existing frameworks, including the Financial Sector Profile maintained by the Cyber Risk Institute,[5] could be leveraged to provide assurance regarding a policyholder's cyber risk management practices.

*Is a Federal insurance response for catastrophic cyber incidents warranted?*

The IIF believes that there is a need for a further comprehensive study of whether and how the Federal government could and should address various potential catastrophic cyber incidents that are beyond the risk appetite and capacity of the private cyber insurance market before making a definitive judgment as to whether and when a Federal response is appropriate. The careful design of any Federal program is critical to promoting market confidence and should be coordinated carefully with the private cyber (re)insurance market and other key stakeholders. A well-crafted Federal response could potentially increase market confidence in cyber insurance solutions and help to grow that market with capital markets solutions such as ILS.

As noted above, the private cyber insurance market is and should remain the primary source of cyber risk coverage. Cyber (re)insurers have considerable experience in underwriting these very complex risks and in working with their customers to advance sound cyber risk management practices and improved cyber hygiene, generally as a condition of cover. Insurers are designing bespoke solutions for customers that are designed to reflect the policyholder's particular risk profile and needs.

However, there could be extraordinary cyber incidents that rise to the level of a catastrophic exposure that could exhaust the capacity of the private market and may warrant a Federal response. Some of the types of incidents that could potentially exhaust private market capacity are outlined in our response to the first question above and FIO and CISA should consider, with input from stakeholders, the full range of potential cyber incidents that could be characterized as catastrophic, as part of the design of any Federal program.[6]

[5] https://cyberriskinstitute.org/the-profile/

[6] One possible design could involve a realistic cap on private market exposure augmented by a Federal government payment, with both private and Federal coverage conditioned on the insured's adherence to minimum cyber risk management standards.

*What structures should be considered by FIO and CISA for a potential Federal insurance response for catastrophic cyber incidents?*

If it is determined that a Federal solution is warranted, FIO and CISA should be guided in developing a Federal response by lessons learned from the implementation and administration of the TRIP, the NFIP, the PPP and the FCIP but should not necessarily use these programs as a template for a response to catastrophic cyber incidents. The design of a catastrophic cyber program will differ in terms of its goals, beneficiaries and key elements and will need to reflect the role of private industry in providing cyber cover. A Federal response should be designed carefully so as not to inadvertently lead to moral hazard and undue reliance on a Federal solution as a substitute for adequate cyber insurance cover and sound risk management practices.

FIO and CISA should also consider the experience of other governments and non-government organizations in establishing public-private partnerships, including initiatives developed specifically to expand the cyber risk insurance market and address its various risks. The design of any Federal response should integrate best practices from such partnerships.[7] Additionally, international coordination efforts, such as those displayed during the recently concluded Washington, D.C. meeting of the International Counter Ransomware Initiative (CRI),[8] highlight the need for borderless solutions to cyber risk and ransomware. Participants from 36 countries plus the European Union (EU), along with more than a dozen private sector entities, agreed to set up an Australia-led International Counter Ransomware Task Force, create an investigations toolkit, publish joint advisories about ransomware, and share information about cryptocurrency addresses and techniques used by ransomware gangs. Such policies and established partnerships can help provide greater certainty for private market participants to increase cyber coverage.

Importantly, industry input, as well as input from a broad range of stakeholders, should be received before FIO and CISA considers establishing a program and before the agencies refine any Federal insurance response for catastrophic cyber incidents. In designing their cyber (re)insurance offerings, the U.S. (re)insurance industry has considerable data and expertise that could help the authorities avoid unproductive approaches and assist in creating a more efficient and cost-effective solution.

Reinsurance solutions have been critical in the private sector responses to cyber risk and should be reflected in any Federal solution. While capital markets solutions to cyber risk are not as well developed as solutions for other risks (e.g. natural catastrophe risks), we believe that the potential for alternative capital sources to augment existing cyber risk solutions should be more fully explored by both the public and private sectors. A joint public-private task force designed to assess opportunities for attracting market-based sources of capital could be considered.

---

[7] Programs include terrorism risk insurance and reinsurance programs, as well as cyber-specific risk programs such as:

- Gestion de l'Assurance et de la Reassurance des risques Attentats et actes de Terrorisme (GAREAT) in France (GAREAT's website provides a useful link to a broader range of relevant pools and organizations)
- The Netherlands Terrorism Risk Insurance Programme (NHT)
- Pool Re (terrorism risk reinsurance) in the U.K.
- Cyber risk programs such as the Cyber Risk Management project from the Monetary Authority of Singapore, which is led by the Nanyang Technological University's Insurance Risk and Financial Research Centre

[8] https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/01/international-counter-ransomware-initiative-2022-joint-statement/

Sufficient flexibility should be built into program design to allow for an iterative approach to future refinement. Any program should be subject to ongoing monitoring and review to allow for continuous improvement, albeit on a schedule that does not impede program efficiency and cost-effectiveness. Private stakeholders should have a role in the review process, given the significant expertise they can bring from day-to-day involvement in the cyber (re)insurance market and in cyber risk management.

IIF insurance members believe that methods to ensure the existence of minimum cybersecurity and cyber hygiene standards and practices across the digital value chain would benefit the U.S. government, (re)insurers and policyholders alike and would reduce moral hazard risks. As noted above in response to FIO's question regarding effective cybersecurity measures, harmonizing the minimum standards that are expected of policyholders across the board could be of value. Other (or additional) standards may be appropriate based on policyholder risk profiles. In addition, careful consideration and clear communication of the circumstances under which Federal coverage would apply and the limits of, and conditions on, Federal coverage would help to both reduce moral hazard and to reduce the risk of market failure.

We appreciate the opportunity to submit a response to this request for comment. We would be pleased to discuss our response in greater detail with you and your staff and colleagues at CISA.

Respectfully submitted,

Mary Frances Monroe