wiley

ALERT

Should Federal Government Insure "Catastrophic Cyber Incidents"? Comments due November 14, 2022

October 14, 2022

On September 29, 2022, the Federal Insurance Office (FIO) of the Department of the Treasury published a Request for Comment (RFC) related to cyber insurance and catastrophic cyber incidents. The RFC is intended to "inform FIO's future work and the joint assessment," and it specifically notes that "FIO intends to assess potential federal insurance responses that are outside" the current Terrorism Risk Insurance Program (TRIP) and to "consider how potential responses could interact with, or be part of, TRIP." Comments to the RFC are due by Monday, November 14, 2022.[1]

The RFC is in response to a June 2022 Report by the Government Accountability Office (GAO) recommending that FIO and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) conduct a joint assessment to determine "the extent to which risks to the critical infrastructure from catastrophic cyber incidents and potential financial exposures warrant a federal insurance response." As the RFC explains, "[b]oth FIO and CISA have agreed to conduct the recommended assessment," and "FIO is also coordinating with the White House Office of the National Cyber Director on these issues."

With the RFC, the FIO is seeking "public comments as to whether a federal insurance response to 'catastrophic' cyber incidents may be warranted, as well as how such an insurance response should be structured and other related issues." To that end, FIO specifically seeks comments on a wide range of topics.

Authors

Edward R. Brown
Partner
202.719.7580
erbrown@wiley.law

Leslie A. Platt
Partner
202.719.3174
lplatt@wiley.law

David H. Topol
Partner
202.719.7214
dtopol@wiley.law

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Practice Areas

Insurance

Privacy, Cyber & Data Governance

Catastrophic Cyber Incidents

1. What type of cyber incidents could have a catastrophic effect on U.S. critical infrastructure, and how likely are such incidents?
2. Are any sectors of U.S critical infrastructure more susceptible to such incidents?
3. How should the federal government and/or the insurance industry address the potential for cascading, cross-sector impacts from a cyber incident?
4. What type of potential "catastrophic" cyber incident could justify the creation of a federal insurance response?
5. What data and methodologies could the federal government and/or the insurance industry use to predict, measure, and assess the financial impact of catastrophic cyber incidents?
6. What amount of financial losses should be deemed "catastrophic" for purposes of any potential federal insurance response?
7. How should FIO measure and assess potential insured loss from catastrophic cyber incidents?
8. What cybersecurity measures would most effectively reduce the likelihood or magnitude of catastrophic cyber incidents?
9. What steps could the federal government take to potentially incentivize or require policyholders to adopt these measures?

Potential Federal Insurance Response for Catastrophic Cyber Incidents

1. What insurance coverage is currently available for catastrophic cyber incidents? What are the current limitations on coverage for catastrophic cyber incidents?
2. What rationales have been (or may be) used to deny coverage for catastrophic cyber incidents?
3. Is the private market currently making available insurance for catastrophic cyber incidents that is desired by policyholders, in terms of the limits, the scope of coverage, and the type and size of businesses seeking coverage?
4. What data do you collect that you would be willing to share with FIO and/or CISA to consider in their assessment of catastrophic cyber incidents and cyber insurance?
5. What other information regarding catastrophic cyber incidents and cyber insurance should FIO and CISA consider?
6. What data should FIO and/or CISA consider collecting to help inform this assessment and their ongoing work?
7. Is a federal insurance response for catastrophic cyber incidents warranted? Why or why not?
8. How might a federal insurance response affect the availability and affordability of cyber insurance across the entire insurance market? What would be the effect on any part of the cyber insurance market that would remain outside the parameters of a federal insurance response?

Potential Structures for Federal Insurance Response

1. *Potential Models*. What structures should be considered by FIO and CISA for a potential federal insurance response for catastrophic cyber incidents? Should an existing federal insurance program (e. g., NFIP or TRIP) or other U.S. or international public-private insurance mechanism serve as a model for, or be modified to address, catastrophic cyber incidents?
2. *Participation*. If there were a federal insurance response, should all cyber insurers be required to participate? Should there be other conditions surrounding participation, whether for cyber insurance or policyholders?
3. *Scope of Coverage*. What should be included in the scope of coverage? For example, should it be limited to certain critical infrastructure sectors, size(s) of policyholder permitted to participate, policyholder retentions or deductibles, any required coverages, limits, deductibles, etc.? Should coverage be limited to or differentiate whether a firm is U.S.-based or the infrastructure is located within the U.S.?
4. *Cybersecurity Measures*. Should cybersecurity and/or cyber hygiene measures be required of policyholders under the structure? If so, which measures should be required?
5. *Moral Hazard*. What measures should be included to minimize potential moral hazard risks (e.g., the possibility that either insurers or policyholders might take undue risks in reliance upon a federal insurance response or fail to implement cybersecurity controls)?
6. *Risk Sharing*. How should any structure involving private insurance address risk sharing with the government and the private insurance sector?
7. *Reinsurance/Capital Markets*. To what extent should reinsurance arrangements, including capital markets participation, be included in any potential insurance response? How would a potential federal insurance response affect the reinsurance and capital markets?
8. *Funding*. How should the structure be funded (e.g., should it be pre- or post- funded)? What might the costs be to the federal government and thus the potential impact on taxpayers?
9. *Evaluation/Data Collection*. How should any structure and its program administration be evaluated on an ongoing basis, whether by policymakers and/or administrators, including whether there should be reporting requirements to Congress or other authorities (and on what topics) and data collection (and which information to collect)?
10. *Limitations*. What catastrophic risk exposures might insurers be unwilling to insure even if a federal insurance response supporting such coverage were adopted? Should limitations exist between cyber and physical incidents (e.g., causes or impacts)?

There also is a "catch all" request for "any additional comments or information on any other issues or topics relating to cyber insurance and catastrophic cyber incidents."

For next steps, following receipt and review of all comments, FIO and CISA will provide Congress a joint assessment of whether a federal insurance response to catastrophic cyber incidents is warranted. This may lead to regulations impacting cyber insurers and the cyber insurance marketplace.

Wiley's Insurance and Privacy, Cyber & Data Governance teams are currently working with industry stakeholders in connection with this RFC. Please reach out to any of the authors with questions or to discuss the potential submission of comments.

[1] November 14, 2022 is also the deadline for submitting comments related to the development of proposed regulations required by the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA"). Among other things, that statute directs the Cybersecurity and Infrastructure Security Agency ("CISA") to develop and oversee implementation of regulations requiring covered entities to submit to CISA reports detailing covered cyber incidents and ransom payments. More on this rulemaking can be found here.