DEPARTM

Potential Federal Insurance Response to Catastrophic Cyber Incidents

AGENCY: Departmental Offices, U.S. Department of the Treasury.

ACTION: Request for comment.

SUMMARY: Over the past several years, the Federal Insurance Office (FIO) in the U.S. Department of the Treasury (Treasury) has continued its ongoing efforts with regard to both cyber insurance and insurer cybersecurity. Cyber insurance is a significant risk-transfer mechanism, and the insurance industry has an important role to play in strengthening cyber hygiene and building resiliency. FIO has also increased its data collection in this area with regard to the Terrorism Risk Insurance Program (TRIP) and has supported the development of Treasury's counter-ransomware strategy. The Government Accountability Office (GAO) released a report in June 2022 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 critical infrastructure from catastrophic cyber incidents and potential financial exposures warrant a federal insurance response." Both FIO and CISA have agreed to conduct the recommended assessment. FIO is also coordinating with the White House Office of the National Cyber Director on these issues.

In order to inform FIO's future work and the joint assessment, FIO is seeking comments from the public on questions related to cyber insurance and catastrophic cyber incidents.

DATES: Submit comments on or before. [**INSERT DATE 45 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER***].

ADDRESSES: Submit comments electronically through the Federal eRulemaking Portal at *http://www.regulations.gov,* in accordance with the instructions on that site, or by mail to the

Federal Insurance Office, Attn: Richard Ifft, Room 1410 MT, Department of the Treasury, 1500 Pennsylvania Avenue NW, Washington, DC 20220. Because postal mail may be subject to processing delays, it is recommended that comments be submitted electronically. If submitting comments by mail, please submit an original version with two copies. Comments should be captioned with "Potential Federal Insurance Response to Catastrophic Cyber Incidents." In general, Treasury will post all comments to *www.regulations.gov* without change, including any business or personal information provided such as names, addresses, email addresses, or telephone numbers. All comments, including attachments and other supporting materials, are part of the public record and subject to public disclosure. You should submit only information that you wish to make available publicly. Where appropriate, a comment should include a short Executive Summary (no more than five single-spaced pages).

Additional Instructions. Responses should also include: (1) the data or rationale, including examples, supporting any opinions or conclusions; and (2) any specific legislative, administrative, or regulatory proposals for carrying out recommended approaches or options.

FOR FURTHER INFORMATION CONTACT: Richard Ifft, Senior Insurance Regulatory Policy Analyst, Federal Insurance Office, (202) 622-2922, Richard.Ifft@treasury.gov, Jeremiah Pam, Senior Insurance Regulatory Policy Analyst, Federal Insurance Office, (202) 622-7009, Jeremiah.Pam2@treasury.gov, or Philip Goodman, Senior Insurance Regulatory Policy Analyst (202) 622-1170, Philip.Goodman@treasury.gov. Persons who have difficulty hearing or speaking may access these numbers via TTY by calling the toll-free Federal Relay Service at (800) 877-8339.

SUPPLEMENTARY INFORMATION

I. Background

Cyber insurance is an increasingly significant risk-transfer mechanism, and the insurance industry has an important role to play in strengthening cyber hygiene and building resiliency.[1] Through underwriting and pricing, insurers can encourage or even require policyholders to implement strong cybersecurity standards and controls. More generally, cyber insurance "can help policyholders respond to lawsuits and loss, and provide associated mitigation services, arising in a variety of situations such as data loss, cloud outage, distributed denial-of-service attacks, malware, and associated ransomware extortion."[2] Cyber insurance is a growing market, with approximately $4 billion in direct premiums written in 2020.[3]

On June 21, 2022, GAO issued a report, *Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks* (GAO Report).[4] The GAO Report emphasizes three points about the catastrophic risk of cyber incidents. First, cyber incidents impacting critical infrastructure have increased in frequency and severity. The GAO Report cites a 2020 study by CISA that includes an analysis of scenario-based estimates of potential losses from severe cyber incidents that ranged from $2.8 billion to $1 trillion per event for the United States.[5] Second, the GAO Report finds that recent attacks demonstrate the potential for systemic cyber incidents, citing recent cyber attacks that "illustrate that the effects of cyber incidents can spill over from the initial target to economically linked firms—thereby magnifying the damage to the economy."[6] Third, the GAO Report evaluates some of the issues regarding potential risks

---

[1] *See, e.g.*, FIO, *Annual Report on the Insurance Industry* (September 2021), 74-78, https://home.treasury.gov/system/files/311/FIO-2021-Annual-Report-Insurance-Industry.pdf (*2021 Annual Report*).

[2] FIO, *2021 Annual Report*, 74.

[3] FIO, *Effectiveness of the Terrorism Risk Insurance Program* (June 2022), 62, https://home.treasury.gov/system/files/311/2022%20Program%20Effectiveness%20Report%20%28FINAL%29.pdf.

[4] GAO, *Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks (2022),* https://www.gao.gov/products/gao-22-104256.

[5] *See* GAO Report, 25 (citing CISA, *Cost of a Cyber Incident: Systematic Review and Cross Validation* (2020), 14, https://www.cisa.gov/sites/default/files/publications/CISA-OCE_Cost_of_Cyber_Incidents_Study-FINAL_508.pdf).

[6] *See* GAO Report, 16 (identifying the May 2021 attack on the Colonial Pipeline Company, the July 2021 attack on Kaseya, and the February 2022 attack on Viasat, Inc.).

presented by cyber incidents to critical infrastructure in the United States.[7] (Market participants, including insurers and reinsurers, have similarly highlighted the risks presented by catastrophic and/or systemic cyber incidents with regard to the cyber insurance market.[8]) The GAO Report also identified potential issues in creating a federal insurance cyber backstop within the scope of the Terrorism Risk Insurance Program (TRIP).[9]

The GAO Report concludes that a full evaluation of whether there should be a federal insurance response in connection with catastrophic cyber risks would be best addressed by FIO (given its statutory authorities, including monitoring of the insurance sector and assisting the Secretary of the Treasury with administration of TRIP) and CISA (given its expertise in connection with cyber and physical risks to U.S. infrastructure) in a joint assessment to be provided to Congress.[10] Both FIO and CISA accepted the GAO recommendation to conduct such a joint assessment, as reflected in letters attached to the GAO Report.

---

[7] *See* GAO Report, 9-12.

[8] *See, e.g.*, Chubb, *Catastrophic Cyber Risks – A Growing Concern* (2021), 6, https://www.chubb.com/content/dam/chubb-sites/chubb-com/us-en/global/global/documents/pdf/2021-10.21_17-01-0286_Cyber_Systemic_Risks_whitepaper.pdf; Carnegie Endowment for International Peace, *Systemic Cyber Risk: A Primer* (March 7, 2022), https://carnegieendowment.org/2022/03/07/systemic-cyber-risk-primer-pub-86531; Geneva Association and the International Forum of Terrorism Risk (Re)Insurance Pools, *Insuring Hostile Cyber Activity: In search of sustainable solutions* (January 2022), 16-20, https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/cybersolutions_web.pdf.

[9] The GAO Report was originally mandated in the 2019 reauthorization of the Terrorism Risk Insurance Program, which was enacted as part of the Further Consolidated Appropriations Act, 2020, Pub. L. No. 116-94, section 502, 133 Stat. 2534, 3027 (2019). *See* GAO, *Cyber Insurance* (2022), 3. Specifically, the Terrorism Risk Insurance Program Reauthorization Act of 2019 directed GAO to provide Congress with a study and report that shall:

> (1) analyze and address—
>
> > (A) overall vulnerabilities and potential costs of cyber attacks to the United States public and private infrastructure that could result in physical or digital damage;
> >
> > (B) whether State-defined cyber liability under a property and casualty line of insurance is adequate coverage for an act of cyber terrorism;
> >
> > (C) whether such risks can be adequately priced by the private market; and
> >
> > (D) whether the current risk-share system under the Terrorism Risk Insurance Act of 2002 (15 U.S.C. 6701 note) is appropriate for a cyber terrorism event; and
>
> (2) set forth recommendations on how Congress could amend the Terrorism Risk Insurance Act of 2002 (15 U.S.C. 6701 note) to meet the next generation of cyber threats.

Pub. L. No. 116-94 at sec. 502(d).

[10] GAO Report, 33.

As a threshold matter, "insurance responses" can take many forms. Most insurance in the United States is provided through private insurance companies that are regulated at the state level. However, there are a large number of programs and mechanisms, both at the state and federal level, where insurance coverage may be provided or mandated by state or federal requirements. These arrangements have typically been put into place when the private market has failed to make available affordable insurance to policyholders. At the state level, many states have created residual market funds that ensure all policyholders can obtain coverage (with those obligations spread across the industry as a whole in some fashion) in areas such as workers' compensation, automobile, and property insurance.[11] There are also several federal programs in this area, including TRIP,[12] the National Flood Insurance Program,[13] the Federal Crop Insurance Program,[14] and others.

FIO, in association with CISA, seeks public comments as to whether a federal insurance response to "catastrophic"[15] cyber incidents may be warranted, as well as how such an insurance response should be structured and other related issues. FIO intends to assess potential federal insurance responses that are outside of TRIP, but will also consider how potential responses could interact with, or be part of, TRIP. State and federal governments have responded in a variety of ways to situations in which the private market is unable to provide sufficient or

---

[11] *See* FIO, *Annual Report on the Insurance Industry* (2021), 66-67, https://home.treasury.gov/system/files/311/FIO-2021-Annual-Report-Insurance-Industry.pdf.

[12] Terrorism Risk Insurance Act of 2002, Pub. L. No. 107-297, 116 Stat. 2322 (2002), as amended, 15 U.S.C. 6701 note. The operation of TRIP is described in FIO's most recent report addressing the effectiveness of the Program. *See* FIO, *The Effectiveness of the Terrorism Risk Insurance Program* (June 2022), 5-8, https://home.treasury.gov/system/files/311/2022%20Program%20Effectiveness%20Report%20%28FINAL%29.pdf.

[13] *See generally* "Flood Insurance," FEMA, last updated March 9, 2022, https://www.fema.gov/flood-insurance.

[14] *See generally* "Crop Insurance: Keeps America Growing," National Crop Insurance Services, https://cropinsuranceinamerica.org/.

[15] FIO also seeks information on possible definitions of what constitutes a "catastrophic" cyber incident, but in this context the term is generally related to the magnitude of the loss, its dispersion among multiple entities, and the degree of critical services affected.

affordable insurance, and FIO seeks input on a wide range of options and potential response structures.

Among other things, FIO is seeking comment on issues concerning the risks of catastrophic cyber incidents to critical infrastructure,[16] the potential quantification of such risks, the extent of existing private market insurance protection for such risks, whether a federal insurance response is warranted, and how such a federal insurance response, if warranted, should be structured.

II. Solicitation for Comments

FIO seeks comments on each of the following topics:

Catastrophic Cyber Incidents

1. **Nature of Event.** What type of cyber incidents could have a catastrophic effect on U.S. critical infrastructure? How likely are such incidents? Are particular sectors of U.S. critical infrastructure more susceptible to such incidents? How should the federal government and/or the insurance industry address the potential for cascading, cross-sector impacts from a cyber incident? What type of potential "catastrophic" cyber incident could justify the creation of a federal insurance response?

2. **Measuring Financial and Insured Losses.** 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? What amount of financial losses should

[16] As noted above, the GAO Report recommends a joint assessment on the extent to which the risks to the nation's *critical infrastructure* from catastrophic cyber attacks, and the potential financial exposures resulting from these risks, warrant a federal insurance response. CISA has previously identified those critical infrastructure sectors whose "assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." CISA, "Critical Infrastructure Sectors," https://www.cisa.gov/critical-infrastructure-sectors. FIO also seeks comment (see Question 8, below) about the potential effects of a federal insurance response that distinguishes between risks to critical infrastructure and non-critical infrastructure.

be deemed "catastrophic" for purposes of any potential federal insurance response? How should FIO measure and assess potential insured loss from catastrophic cyber incidents?

3. **Cybersecurity Measures.** 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?

Potential Federal Insurance Response for Catastrophic Cyber Incidents

4. **Insurance Coverage Availability.** What insurance coverage is currently available for catastrophic cyber incidents? What are the current limitations on coverage for catastrophic cyber incidents? What rationales have been (or likely would be) used to deny coverage for catastrophic cyber incidents? 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?

5. **Data and Research.** 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? What other information regarding catastrophic cyber incidents and cyber insurance should FIO and CISA consider? What data should FIO and/or CISA consider collecting to help inform this assessment and their ongoing work?

6. **Federal Insurance Response.** Is a federal insurance response for catastrophic cyber incidents warranted? Why or why not?

7. **Potential Structures for Federal Insurance Response.** What structures should be considered by FIO and CISA for a potential federal insurance response for catastrophic cyber incidents? In your answer, please address:

- ***Potential Models.*** 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?

- ***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?

- ***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.?

- ***Cybersecurity Measures.*** Should cybersecurity and/or cyber hygiene measures be required of policyholders under the structure? If so, which measures should be required?

- ***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)?

- ***Risk Sharing.*** How should any structure involving private insurance address risk sharing with the government and the private insurance sector?

- ***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?

- ***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?

- ***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)?

- ***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)?

8. **Effects on Cyber Insurance Market.** 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?

Other

9. Please provide any additional comments or information on any other issues or topics relating to cyber insurance and catastrophic cyber incidents.

Steven E. Seitz,
Director, Federal Insurance Office.

Billing Code 4810-AK-P

[FR Doc. 2022-21133 Filed: 9/28/2022 8:45 am; Publication Date: 9/29/2022]