Update on FIO's RFI on a Potential Federal Insurance Response to Catastrophic Cyber Incidents

Advisory Committee on Risk-Sharing Mechanisms

July 26, 2023

FIO's Prior and Current Work on Cyber Insurance

- FIO continues its ongoing efforts relating to cyber insurance and insurer cybersecurity.
- FIO administers the Terrorism Risk Insurance Program (TRIP), and cyber insurance may be written in TRIP-eligible lines of insurance.
    - FIO increased its collection of cyber-related elements beginning with the 2022 TRIP data call. FIO's 2022 *Report on the Effectiveness of the Terrorism Risk Insurance Program* and 2023 *Study of Small Insurer Competitiveness in the Terrorism Risk Insurance Marketplace* included discussions of the cyber insurance results of the expanded data call.
- FIO Annual Reports include information on cyber insurance and insurer cybersecurity.
- FIO coordinates with other Treasury offices and federal agencies, including Treasury's Office of Cybersecurity and Critical Infrastructure Protection (OCCIP) and the White House Office of the National Cyber Director (ONCD).
- FIO is now working on a joint assessment with the Department of Homeland Security's Cybersecurity and Infrastructure Agency (CISA) in response to a GAO Report, *Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks* (June 2022)

GAO Report, *Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks*

- **Findings.** The GAO report noted, among other things:
  - U.S. critical infrastructure faces increasing cybersecurity risks: cyber incidents to critical infrastructure have increased in frequency and severity.
  - Recent attacks demonstrate the potential for systemic cyber incidents.
  - Cyber insurance and TRIP are limited in their ability to cover potentially catastrophic losses from systemic cyberattacks.

- **Conclusion and Recommendation:** The GAO report concluded that a full evaluation of whether there should be a federal insurance response in connection with catastrophic cyber risks would be best addressed jointly 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).

- **Next Steps:** FIO and CISA accepted the GAO Report recommendation and began work on this joint project last summer.
  - FIO sought public comment on questions relating to cyber insurance and catastrophic cyber incidents with a Federal Register Notice (FRN) published on September 29, 2022.

FIO FRN Questions on Catastrophic Cyber Incidents

- **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?

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

- **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?

FIO FRN Questions on Potential Federal Insurance Response

- **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?

- **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?

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

FIO FRN Questions on Potential Federal Insurance Response Structure (continued) and General Question

- **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?
  - This question asks respondents to also address related questions concerning: Potential Models, Participation, Scope of Coverage, Cybersecurity Measures, Moral Hazard, Risk Sharing, Reinsurance/Capital Markets, Funding, Evaluation/Data Collection, and Limitations.
- **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.** Please provide any additional comments or information on any other issues or topics relating to cyber insurance and catastrophic cyber incidents.

National Cybersecurity Strategy

- On March 2, 2023, President Biden released the National Cybersecurity Strategy.
  - Strategic Objective 3.6 is *Explore a Federal Cyber Insurance Backstop*:
  - "The Administration will assess the need for and possible structures of a Federal insurance response to catastrophic cyber events that would support the existing cyber insurance market."
- On July 13, 2023, President Biden released the National Cybersecurity Strategy Implementation Plan
  - Initiative Number 3.6.1 is *Assess the need for a Federal insurance response to a catastrophic cyber event*
  - The Implementation Plan designates Treasury as the Responsible Agency
  - "The Department of the Treasury's Federal Insurance Office, in coordination with CISA and ONCD, will assess the need for a Federal insurance response to catastrophic cyber events that would support the existing cyber insurance market."

RFI Comments Received

- 60 separate RFI comments were submitted (56 unique), including from:
  - Insurers and reinsurers (including specialist cyber insurers),
  - Insurance and reinsurance brokers,
  - An insurance rating agency,
  - Trade associations (insurance, reinsurance and insurance-related),
  - Insurance risk modeling analytics organizations,
  - Insurance think tanks and academic experts,
  - Cybersecurity consultants and cybersecurity product companies, and
  - Organizations representing multiple critical infrastructure sectors.

High-Level Summary of Some Commenter Themes (1 of 3)

1. Broad conceptual support for some type of future federal insurance response

    - Support among most commenters that some kind of federal insurance response should be developed.

    - Some commenters expressed the view that adopting a federal insurance response now would be premature but supported further analysis.

2. General agreement that any federal insurance response should address cyber hygiene

    - A number of responses listed specific cybersecurity controls that commenters suggested should be part of insurer-enforced minimum cybersecurity standards, with some commenters noting that required cybersecurity controls would help mitigate the moral hazard effect of insuring cyber incidents. A few commenters said that access to a new federal insurance response should be explicitly conditioned on the adoption of cybersecurity controls meeting minimum standards.

    - Other commenters noted potential limitations in what can be accomplished by even the best cybersecurity controls, calling for the federal government at most to promote and encourage cyber hygiene best practices in order to help inform private insurer underwriting.

High-Level Summary of Some Commenter Themes (2 of 3)

3. Commenters proposed a range of ideas for the structure of a potential federal insurance response, including:

   - Create a new structure not modeled on any existing government program;
   - Create a new structure loosely modeled on, but separate from, the Terrorism Risk Insurance Act (TRIA) and the Terrorism Risk Insurance Program (TRIP), dedicated to addressing catastrophic cyber risk. Modify TRIP as needed to coordinate programs (e.g., change TRIP's coverage of cyber terrorist attacks to eliminate overlap with new structure);
   - Amend TRIA and expand TRIP to cover catastrophic cyber incidents more generally (i.e., no longer limit it to cyber terrorism incidents);
   - Create a new governmental public-private partnership modeled on the UK's Pool Re;
   - Create a new structure modeled on FEMA's National Flood Insurance Program (NFIP); and
   - Create a new structure through a newly-created government-sponsored enterprise (GSE) analogous to Fannie Mae or Freddie Mac through which the federal government would assume catastrophic cyber risk.

High-Level Summary of Some Commenter Themes (3 of 3)

4. Differing views regarding the adoption of key structural elements from TRIA/TRIP
    - Some commenters noted reservations about a certification process, particularly one with an attribution requirement.
5. Commenters suggested numerous structural elements not featured in TRIA
    - Some commenters expressed preference for a pure financial trigger.
6. Support for considering cross-border scenarios while assessing catastrophic cyber insurance
    - Scenarios raised include losses from a catastrophic cyber incident realized in the United States by a non-U.S. entity, and worldwide protection of a U.S. entity.

Next Steps

- FIO is engaging with various commenters and other public and private sector stakeholders, including our international counterparts.

- This high-level summary of some of the main issues raised by commenters does not suggest FIO endorsement of or agreement with any of the themes summarized.

- However, the themes identified by commenters indicate that FIO and CISA, in coordination with the White House Office of the National Cyber Director (ONCD), need to continue to undertake further analysis and engagement to assess whether a federal insurance response for catastrophic cyber risk is warranted, and if so, what form it should take.