Summary of Comments on Request for Comment: Federal Insurance Response to Catastrophic Cyber Incidents

Presentation to the Federal Advisory Committee on Insurance
March 29, 2023

Federal Insurance Office

Background

- 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."
- FIO began evaluating this issue last year, when Treasury (in coordination with CISA) published a Request for Comment (RFI) on a Potential Federal Insurance Response to Catastrophic Cyber Incidents (87 Fed. Reg. 59161).
- 59 separate RFI comments were submitted (55 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), will need 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.