AMERICAN ACADEMY of ACTUARIES

Objective. Independent. Effective.™

May 16, 2022

Attn: Richard Ifft
Senior Insurance Regulatory Policy Analyst
U.S. Department of the Treasury
Federal Insurance Office

Re: 2022 TRIP Effectiveness Report Comments
Docket ID: TREAS-TRIP-2022-0010-0001

To Whom It May Concern:

The Department of the Treasury ("Treasury") has requested comments regarding the following factors to consider in the 2022 Report on the Effectiveness of the Terrorism Risk Insurance Program. The Cyber Risk Task Force of the American Academy of Actuaries[1] offers the following comments to these cyber-related questions regarding the Terrorism Risk Insurance Act of 2002 (TRIA), as amended:

> *5. The current state of the cyber insurance market, including the scope of coverage available, the availability and affordability of such coverage, and the effect of ransomware-related losses on the market;*
>
> *6. Terrorism risk insurance issues presented by cyber-related losses, and the impact of TRIP in connection with such exposures, including views on cyber-related terrorism losses that are included within TRIP and those losses outside of TRIP;*
>
> *7. Any potential changes to TRIA or TRIP that would encourage the take up of insurance for cyber-related losses arising from acts of terrorism as defined under TRIA, including but not limited to the modification of the lines of insurance covered by TRIP and revisions to the current sharing mechanisms for cyber-related losses;*

A. The Current State of the Cyber Insurance Market

With regard to the cyber insurance market, the Loss & Defense and Cost Containment (DCC) ratios remain at an elevated level in 2021 and 2020 for stand-alone U.S. cyber insurance coverage compared

[1] The American Academy of Actuaries is a 19,500-member professional association whose mission is to serve the public and the U.S. actuarial profession. For more than 50 years, the Academy has assisted public policymakers on all levels by providing leadership, objective expertise, and actuarial advice on risk and financial security issues. The Academy also sets qualification, practice, and professionalism standards for actuaries in the United States.

with prior years' loss ratio experience. See below for the U.S. direct loss ratio and DCC[2] experience by year as reported to the National Association of Insurance Commissioners (NAIC). There was a significant increase in the loss ratios in 2020 and 2021 compared with 2015 through 2019.

U.S. Cyber Insurance Stand-alone, Direct Loss & DCC ratios:[3]

- 2015—48%
- 2016—43%
- 2017—35%
- 2018—34%
- 2019—47%
- 2020—72%
- 2021—65%

When analyzing these loss ratios, it is important to consider the premium rate increases that were experienced by policyholders in 2021 that were notably driven by ransomware losses. The following table shows year-over-year premium rate increases experienced by Aon and Marsh insureds in 2021. The Aon results are for Errors and Omissions (E&O) / Cyber insurance pricing whereas the Marsh results are presented as Cyber insurance.

Year-over-Year Rate Change Increases (For example Q4 2021 is comparing to Q4 2020)

Quarter	Aon Reported Premium Rate Increases[4]	Marsh Reported Premium Rate Increases[5,6]
Q1 2021	January—22.8% February—23.3% March—28.1%	35%
Q2 2021	April—37.5% May—38.5% June—58.2%	60%
Q3 2021	July—71.6% August—100.9% September—103.8%	101%
Q4 2021	October—105.2% November—105.1% December—137.3%	130%

Cyber insurance premium rate increases have continued as notable cyber insurers reported achieving premium rate increases of between 80% and 100% over Q1 2022 on their cyber insurance books of business.

A stable cyber insurance market provides a means for companies and individuals to transfer a portion of their financial exposure to insurance markets, reducing the costs associated with a cyber event. Cyber insurance can also provide companies expert assistance in improving cyber security as

[2] Direct loss and DCC as percentage of direct earned premium
[3] https://www.fitchratings.com/research/insurance/us-cyber-insurance-sees-rapid-premium-growth-declining-loss-ratios-13-04-2022
[4] https://publications.aon.com/eo-and-cyber-market-review/loss-and-pricing-trends
[5] https://www.marsh.com/us/services/cyber-risk/insights/cyber-insurance-market-overview-q4-2021.html
[6] https://www.marsh.com/us/services/international-placement-services/insights/us-gimi-q4-2021.html#:~:text=Cyber%20pricing%20increased%20130%25%2C%20affected,pay%2Douts%20from%20ransomware%20events.

well as managing the recovery from an attack. The American Academy of Actuaries Cyber Risk Task Force is not opining on the scope of coverage or the availability / affordability of cyber insurance coverage. However, these pricing changes and corresponding loss experience across the industry should be continually monitored. Clearer and/or additional industry reporting requirements within the NAIC annual statement blank filings could assist with the tracking of industry cyber insurance trends. The Academy acknowledges that the NAIC annual statement blank does require a supplemental filing related to cyber insurance.

B. Terrorism Risk Insurance Issues Presented by Cyber-related Losses

As noted in the task force's January 2021 comment letter to Treasury,[7] cyberattacks do not always respect geographic boundaries and can expand across many nations. As such, foreign events that cause damage to an organization within the United States such as 2017's NotPetya attack should be considered for inclusion under TRIA. The following excerpt is from the task force's January 2021 comment letter to Treasury:

> *Cyberattacks do not adhere to geographical boundaries. This may lead to many scenarios where a cyberattack outside the United States would lead to substantial damage and losses within the United States. In general, providing coverage under TRIA for damage inside the United States from a foreign event would be best considered as a type of loss that was envisioned to fall under the umbrella of coverages under TRIA. We believe that foreign events such as those contemplated in Treasury's inquiry would meet the intent of covered damage under TRIA and as such should be covered. A clear example of how an attack with specific targets in one country can quickly become a global catastrophe is the 2017 NotPetya attack.*

Further, attribution surrounding cyberattacks is a difficult topic, but it is a key topic when analyzing the interaction between TRIA and cyber insurance given that a requirement is to understand which terrorist group caused the cyberattack. The following excerpt from the task force's January 2021 commentary succinctly articulates two key issues and considerations that would assist the insurance market in providing additional guidance around how cyberattacks would be attributed and deemed to trigger payouts under TRIA:

> *Given the nature of cyberattacks, often the exact source, timing, and motivation are not clear, at least for some period of time. Additionally, an attack on a particular target may unintentionally spread the damage to others. The NotPetya attack is an example. Specific guidance on which types of attacks are considered terrorism, and the relevance of the involvement of foreign governments in determining whether an act is considered terrorism or "war," would provide needed clarity. It would be valuable to examine various scenarios and consider which types of events would be covered under TRIA and which would not.*
>
> *TRIA includes several requirements to trigger the payout of federal funds. One of these is a public finding by the Treasury that an event was caused by nongovernmental terrorists. The difficulty of identifying the origin of a cyberattack, the likely ambiguity about the status of the attackers, and the length of time that it may take to get a public declaration about the identity of the attackers all suggest that there will be a great deal of uncertainty about the application of TRIA in the event of a major cyberattack. Consequently, we believe that a different standard for cyberattacks should be considered—one that does not require the identification of the attackers.*

[7] https://www.actuary.org/sites/default/files/2021-01/Cyber_TRIA_Academy_Comment_Letter.pdf

With regard to cyber war and cyber terrorism, the task force has updated its Cyber Risk Toolkit[8] in February 2022, and a section titled War, Cyberterrorism, and Cyber Insurance was added. This section addresses some of the critical issues related to cyberattacks, attributing the attacks, and the interaction between general war exclusions as well as TRIA within cyber insurance policies.

C. Potential Changes to TRIA or TRIP that would Encourage Take up of Insurance for Cyber-related Losses

When looking at potential changes to TRIA, the Academy's Cyber Risk Task Force recognizes the coverages included within TRIA are property and casualty insurance as defined under Part 50 subpart A[9] as noted below. These definitions are also reiterated in the June 2021 proposed definitional changes to TRIA[10].

> *(1) Means commercial lines within only the following lines of insurance from the NAIC's Exhibit of Premiums and Losses (commonly known as Statutory Page 14): Line 1—Fire; Line 2.1—Allied Lines; Line 5.1—Commercial Multiple Peril (non-liability portion); Line 5.2—Commercial Multiple Peril (liability portion); Line 8—Ocean Marine; Line 9—Inland Marine; Line 16—Workers' Compensation; Line 17—Other Liability; Line 18—Products Liability; Line 22—Aircraft (all perils); and Line 27—Boiler and Machinery; a stand-alone cyber liability policy falling within Line 17—Other Liability, is property and casualty insurance, so long as it is not otherwise identified for state reporting purposes as a policy that is not property and casualty insurance, such as professional liability insurance.*

It is important to note that professional liability insurance is still explicitly excluded from coverage under TRIA. Given that organizations may protect themselves from cyber incidents by utilizing terms and endorsements within professional liability insurance policy forms, this is a potential area of exploration regarding the modification of the lines of insurance covered within TRIA, especially as it relates to cyber-related losses.

The American Academy of Actuaries Cyber Risk Task Force appreciates that the Department of the Treasury is further considering concerns on TRIA coverage for cyber risk. We look forward to working with you and Treasury staff to explore this topic and help resolve these various questions.

If you have any questions about this letter or seek additional information from the Academy, contact Rob Fischer, casualty policy analyst, at fischer@actuary.org.

Sincerely,

Norman Niami, MAAA, FCAS, Affiliate IFoA
Chairperson
Cyber Risk Task Force

[8] https://www.actuary.org/sites/default/files/2022-02/CyberRiskToolkit.Feb22.pdf
[9] https://www.ecfr.gov/current/title-31/subtitle-A/part-50/subpart-A/section-50.4
[10] https://www.federalregister.gov/documents/2021/06/09/2021-12014/terrorism-risk-insurance-program-updated-regulations-in-light-of-the-terrorism-risk-insurance#citation-14-p30538