January 7, 2021

Via Federal Regulatory Portal

Re: 2019 TRIA Reauthorization Proposed Rules Comments
Docket ID: TREAS-TRIP-2020-0022

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

To Whom It May Concern:

The Department of the Treasury ("Treasury") has requested comments regarding changes to previous Treasury cyber coverage guidance on the following:

> *(a) Whether cyber events outside the United States can inflict cyber-related losses within the United States that qualify as "damage within the United States" for purposes of TRIA;*
>
> *(b) To the extent such cyber events can be said to inflict losses that qualify as "damage within the United States," whether such losses may also be subject to compensation under the terrorism risk insurance pools or arrangements of other jurisdictions; and*
>
> *(c) How Treasury could evaluate such losses representing "damage within the United States" from a certification standpoint, particularly if the causative cyber events in question take place outside the United States.*

The Cyber Risk Task Force of the American Academy of Actuaries[1] offers the following comments to regarding Terrorism Risk Insurance Program (TRIP) proposed rule changes.

Background and Solution

A stable cyber insurance market provides a mechanism for companies and individuals to transfer a portion of their financial exposure to insurance markets, reducing the costs associated with a cyber event. In this regard, any additional clarity and an appropriate scope of the Terrorism Risk

[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.

Insurance Act (TRIA) would further increase the stability of the cyber insurance market.

Cyberattacks are a real threat in today's ever-evolving cyber risk landscape. The COVID-19 pandemic is forcing organizations to accelerate digital transformations already underway. E-commerce is booming, while schools and offices have adopted and adapted to online distance learning classes and remote working. This rapid transformation has further increased systemic vulnerabilities to cyberattacks. Various scenarios estimating catastrophic damage from cyber events have ranged from tens of billions to hundreds of billions of dollars. The treatment of cyber coverage under TRIA has enabled more robust participation among insurers and reinsurers due to the mitigation of losses under some extreme scenarios.

The cyber threat landscape is continually changing and evolving as attackers develop new tools and discover new attack vectors. Machine learning and artificial intelligence are being increasingly used by both attackers and defenders, and the importance of these tools is likely to increase in the future. Modern computer networks are complex systems and a weakness in any component of the system could render the entire system vulnerable.

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.

To date, the costliest cyberattack is the 2017 NotPetya attack, with total costs estimated as high as $10 billion.[2] The attack began in Ukraine but quickly spread to countries around the world. Later investigation revealed that the attack had begun with the servers of a Ukrainian software company that produced a piece of accounting software used widely within that country. The worm spread with incredible speed, taking down the networks of several large Ukrainian companies in less than 60 seconds from the time the first computers in those networks were infected. It spread quickly beyond Ukraine, impacting companies in a wide range of locations and industries. Two of the most heavily impacted companies were Merck and FedEx, each of which lost hundreds of millions of dollars due to the attack.

At Merck, the attack reportedly may have crippled more than 30,000 laptop and desktop computers, as well as 7,500 servers. Sales, manufacturing, and research units were all hit. By the end of 2017, Merck's initial estimate of the malware damage was $870 million. This initial estimate has increased over time.

An act with consequences similar to NotPetya—creating significant damage that would meet other coverage triggers and requirements under TRIA—should not be outside the scope of TRIA just because it was initiated outside the U.S.

[2] "The Worst Hacks of the Decade"; *Wired*; Dec. 23, 2019.

Other Issues of Concern

One concern in regard to TRIA had been a lack of clarity regarding non-standalone cyber coverages. The Treasury proposed rule of November 10, 2020,[3] would seem to alleviate that concern by stating "that the National Association of Insurance Commissioners (NAIC) had recently identified, for state purposes, an insurance product called 'Cyber Liability' within the general scope of the Other Liability line of insurance, which is generally subject to the Program." The intention of coverage for this type of policy indicated by the Treasury statement would help address some of the concern for other types of policies that may contain cyber damage coverage. It would also address the concern in regard to the need for clarity about what was meant by the Treasury's reference to NAIC[4] sub-lines of insurance and TRIA-covered lines (the 2016 Treasury Cyber Guidance had originally identified standalone cyber liability insurance, for reporting purposes, a sub-line of insurance within Other Liability).

In the Academy's letter[5] of June 1, 2020, to the U.S. Government Accountability Office, we shared other issues that the December 2016 Treasury guidance did not address. Additionally, some areas could use more clarity to reduce uncertainty about the program and its intention. As the various challenges around the current coronavirus pandemic indicate, attempting to address any uncertainties after a large-scale event may prove to be much more difficult and will create additional stress in the financial system. Addressing the following two issues would contribute to greater confidence and stability in the cyber insurance market:

- 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.

The American Academy of Actuaries Cyber Risk Task Force appreciates that 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 in advance of a real-life test of the law.

---

[3] "Terrorism Risk Insurance Program; Updated Regulations in Light of the Terrorism Risk Insurance Program Reauthorization Act of 2019, and for Other Purposes"; *Federal Register*; Nov. 10, 2020.

[4] Cyber Guidance, 81 FR 95313; see NAIC, Uniform Property & Casualty Product Coding Matrix (effective Jan. 1, 2020), 10, https://www.naic.org/documents/industry_pcm_p_c_2020.pdf.

[5] https://www.actuary.org/sites/default/files/2020-06/GAO_Comment_Letter_TRIA_and_Cyber.pdf

If you have any questions about this letter or seek additional information from the Academy, contact Devin Boerm, deputy director for public policy, at 202-785-8196 or boerm@actuary.org.

Sincerely,

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