May 8, 2026

Attn: Richard Ifft
Lead Management and Senior Insurance Policy Analyst
Terrorism Risk Insurance Program
Federal Insurance Office
U.S. Department of the Treasury

Re: 2026 TRIP Effectiveness Report

To Whom It May Concern:

On behalf of the Casualty Practice Council's Committee on Cyber Risk (the Committee) of the American Academy of Actuaries[1], we appreciate the opportunity to offer comments on the 2026 Report on the Effectiveness of the Terrorism Risk Insurance Program. In response to the Department of the Treasury ("Treasury") request for comments, the Committee offers comments on the following cyber-related topics regarding the Terrorism Risk Insurance Act of 2002 (TRIA), as amended:

> *5. Terrorism risk insurance issues presented by cyber-related losses, and the impact of TRIP in connection with such exposures, including your views on cyber-related terrorism losses that are included within TRIP and those losses outside of TRIP;*
>
> *6. 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 potential modification of the lines of insurance covered by TRIP and revisions to any of the current sharing mechanisms for cyber-related losses, such as, for example, the individual insurer deductible or the federal share percentage.*
>
> *7. The availability of reinsurance or capital markets support for cyber-related losses arising from acts of terrorism as defined under TRIA;*

5. Cyber-related Losses and their Impact on Terrorism Risk Insurance

Certain cyberattacks may be labeled as acts of cyber-related "terrorism." However, only those that are deemed a "certified act of terrorism" by the Secretary of the Treasury as defined by the law are eligible for coverage under TRIA.[2] To date, there has yet to be a

[1] The American Academy of Actuaries is a 20,000-member professional association whose mission is to serve the public and the U.S. actuarial profession. For 60 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.

[2] "Certified Act of Terrorism", IRMI, accessed May 7, 2026.

certified act of terrorism for reimbursement, from any cause of loss, under the Terrorism Risk Insurance Act (TRIA). An additional source of complexity for Terrorism Risk Insurance is that acts committed as part of the course of war declared by the Congress are not to be certified by the Secretary as an act of terrorism.[3] The potential for state-sponsored cyber terrorist groups adds another layer of complexity to the determination around applicability of TRIP coverage.

Cyberattacks and bad actors continue to operate across geographic borders and have varying motivations ranging from financial to ideological to state-sponsored. The following commentary comes from the Committee's January 2021 comment letter to Treasury,[4] and it still is relevant in today's environment. The most notable world-wide cyber event is still the NotPetya attack, which began in June 2017. While originating in Ukraine, the impact of the NotPetya attack spread across Europe, Asia, and the Americas.[5] The following excerpt is from the Committee'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.*

The current cyber threat actor environment is constantly evolving. Political conflicts will likely continue to deploy kinetic and non-kinetic warfare. Terrorist and nation-state related activity are relevant topics of discussions when discussing how TRIA would respond to a cyber incident. As previously discussed with NotPetya, the potential for a catastrophic cyber event to originate in a given region of the world yet spread significantly across the world is a realistic scenario. Additionally, other recent cyber incidents such as CrowdStrike, Change Healthcare, and CDK in 2024 or Jaguar Land Rover in 2025 have all had significant downstream impacts originating from a single initial target or event.

The Committee's January 2021 commentary below highlights some of the nuances and difficulty associated with event attribution and payment triggers. Further guidance surrounding attribution and timely payout triggers would assist the broader insurance market in evaluating the financial protection received from TRIA.[6]

> *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*

[3] "Terrorism Risk Insurance Act (TRIA) – Consolidated Statute", U.S. Department of the Treasury, 2015
[4] "Cyber Risk and the Terrorism Risk Insurance Program", American Academy of Actuaries, January 2021
[5] "Statement from the Press Secretary", The White House (Archived), Feb. 25, 2019
[6] IBID

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.

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

Prior commentary provided by the Committee to the Treasury in May 2022[7] regarding the impact of included and excluded coverages surrounding "Professional Errors and Omissions Liability Insurance" remains pertinent. Many organizations that provide technology-based services purchase a blended Technology Errors & Omissions and Professional Liability policy to protect their financial interests from cyber and technology-related incidents. However, the 2016 guidance from the Treasury explicitly states that "Professional Errors and Omissions Liability Insurance" is excluded from TRIP.[8] This explicit omission from TRIP presents a gap in coverage for organizations who may present the largest aggregate exposure for a cyber catastrophe. The Committee recommends further exploration and potential expansion of the coverage lines included within TRIA given this potential gap.

7. Reinsurance Availability and Capital Market Support for Cyber Insurance

As of the April 1, 2026, reinsurance treaty renewals, the cyber reinsurance market remains buyer-friendly to cyber insurers within the U.S. The supply of reinsurance capital for cyber risk is outpacing the demand by insurers, which has led to an overall excess capacity and corresponding rate competition as seen in the April 1, 2026, reinsurance renewals.[9] At the January 1, 2026, renewals, the non-proportional cyber reinsurance rates decreased 32% on a risk-adjusted basis, per Gallagher Re.[10] The rate reduction is driven by both favorable loss experience and strong interest by reinsurers to write the coverage. Proportional (quota share) reinsurance ceding commissions increased by approximately 1% to 1.5% for many purchasers at the January 1, 2026, renewals, per Howden Re.[11]

In addition to traditional reinsurance, catastrophe bonds and insurance linked securities (ILS) continued to renew over the course of 2025 and into 2026. In December 2025, there were two

[7] "Academy Comment Letter to FIO on TRIP", American Academy of Actuaries, May 16, 2022
[8] "Guidance Concerning Stand-Alone Cyber Liability Insurance Policies Under the Terrorism Risk Insurance Program", Federal Register, Dec. 27, 2016
[9] "Softer Cyber Reinsurance Pricing Expected to Persist", *The Insurer*, April 28, 2026
[10] "Gallagher Re Cyber Risk Adjusted Rating (RAR) Index – 2026 Update", Gallagher Re, 2026
[11] "Cyber Reinsurance Buyers Benefit from Favourable Supply Dynamics at 1/1: Howden Re", *Reinsurance News*, 2026

cyber risk catastrophe bonds issued by Beasley[12] and Chubb.[13] Additionally, Hanover Re's Cumulus Re 2026-1 cloud outage catastrophe bond was issued in March 2026.[14]

Thank you for the opportunity to comment on the 2026 report, including further considerations of addressing TRIA coverage concerns for cyber risk. We look forward to working with you and Treasury staff to explore this important topic and help resolve these various questions. If you have any questions or would like to discuss these comments further, please contact Rob Fischer, policy project manager, casualty (fischer@actuary.org, 202-785-7865).

Sincerely,

Samuel Tashima, MAAA, FCAS, MBA
Chairperson, Committee on Cyber Risk

[12] "Polestar Re Ltd. Series 2026-1", Artemis, 2026
[13] "East Lane Re VII Ltd. Series 2026-1", Artemis, 2026
[14] "Cumulus Re Series 2026-1", Artemis, 2026