June 1, 2020

Hon. Gene Dodaro
Comptroller General
U.S. Government Accountability Office
441 G St. NW
Washington, DC 20548

Re: Cyberattack and the Terrorism Risk Insurance Program

Dear Comptroller General Dodaro:

We understand that the Government Accountability Office (GAO) has been directed by Congress to look into several questions that have been raised about how the Terrorism Risk Insurance Act (TRIA) would apply in the case of a large-scale cyberattack against American businesses. The Cyber Risk Task Force of the American Academy of Actuaries[1] offers the following comments to help you and the GAO staff as you prepare your response to the congressional inquiry.

We live in an increasingly interconnected world. The various forms of technology that have enabled this interconnectivity and produced countless benefits for society can also be the cause of tremendous damage through cyber events, whether intended or unintended. Cyber risk insurance has provided a solution that improves the resilience of businesses against cyberattacks.

Fortunately, the cost of cyber risk to society to date has only amounted to a fraction of what it could be. In several reports discussing cyberattack scenarios, potential aggregated losses amount to levels that would be devasting to the U.S. economy.[2] These events stem from a variety of different cyber vulnerabilities. For example, various studies considered disruption of a cloud service provider, or a mass software vulnerability leading to widespread data breaches, or a global ransomware attack, or a cyberattack on the Northeastern U.S power grid. Economic losses associated with these events could range in the hundreds of billions, and in extreme scenarios over $1 trillion.

[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.
[2] U.S. Cyberspace Solarium Commission, March 2020; The Council of Economic Advisers, February 2018, "The Cost of Malicious Cyber Activity to the U.S. Economy."

The most extreme scenario is captured in a 2015 report published by Lloyd's[3] of London and developed by the University of Cambridge Center for Risk Studies. In this scenario, an industrial system's sabotage results in an electricity blackout affecting 15 states in the Northeastern U.S. The mechanism employed in the scenario is a malware infection that causes electricity generators to overload and burn out, leading to widespread blackouts. Although improbable, the scenario is believed to be technologically feasible. Depending on the severity of the event, there is a wide range of estimates, with economic losses falling between $243 billion and more than $1 trillion, and insured losses falling between $21 billion and $71 billion. This level of insured losses may be understated in today's market as cyber insurance penetration has increased since the report was published. Data from the National Association of Insurance Commissioners (NAIC) indicates the number of stand-alone policies for cyber coverage grew from 103,455 in 2017 to 161,120 in 2019, as reported by S&P Global Market Intelligence.

It is worth noting that in these published reports laying out various cyber risk scenarios, insured losses are estimated to be a small fraction of the total economic losses. Contributing to this small fraction is the fact that the market for cyber insurance policies is still relatively immature, although capacity has been increasing.[4]

The concern around aggregation of losses from extreme events due to systemic risk factors has been one impediment to the growth of the private cyber insurance market. However, guidance released by the U.S. Department of the Treasury in December 2016,[5] clarifying that stand-alone cyber insurance policies are included in the definition of property and casualty insurance under TRIA, has helped accelerate the availability of stand-alone cyber insurance coverage. Prior to the release of this guidance, many primary cyber insurance policies specifically excluded cyber terrorism in some manner. Many insurers have removed or narrowed the cyber terrorism exclusion, providing coverage for cyber terrorism.

The current treatment of cyber coverage under TRIA has enabled a more robust participation among reinsurers due to the mitigation of losses under extreme scenarios like the one laid out above. The development and effective functioning of the cyber insurance market depends on the contributions from the primary insurance, reinsurance, and captive insurance markets.[6]

There are several issues that the December 2016 Treasury guidance did not address, however. 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 issues now would contribute to greater confidence and stability in the cyber insurance market:

- The guidance fell short of addressing the fact that there are a variety of non-stand-alone cyber coverages that are included in other insurance policies, such as professional liability, which are intended to cover third-party cyber liability losses. However, because

[3] Lloyd's; Emerging Risk report—2015, Innovation Series, Society & Security; *Business Blackout—The insurance implications of cyberattack on US power grid*.
[4] Aon; *U.S. Cyber Market Update—2018 U.S. Cyber Insurance Profits and Performance*; June 2019.
[5] U.S. Treasury Department; "Guidance Concerning Stand-Alone Cyber Liability Insurance Policies Under the Terrorism Risk Insurance Program"; *Federal Register*; Dec. 27, 2016.
[6] Congressional Research Service; "Terrorism Risk Insurance: Overview and Issue Analysis for the 116th Congress"; Dec. 27, 2019.

professional liability policies are specifically excluded from TRIA, cyber liability losses related to such policies are not be eligible for TRIA protection. It would be useful to have a public discussion of whether TRIA would or should apply to cyber-related claims in other insurance lines.

- The impact of the Treasury guidance was also not totally clear. Some issuers in the cyber insurance market believed that cyber risk was covered under TRIA to the extent it is provided in a TRIA-covered line. Treasury addressed the lines of business question by referencing lines in the NAIC annual statement blank. When the NAIC made some cyber-related changes in the coding on its product coding matrix, those changes may have been misunderstood by some as changes to the statutory annual statement filings. The Treasury guidance references new cyber sublines in the annual statement, which are not actually in the annual statement. The NAIC annual statement blank does require a supplemental filing related to cyber insurance.

- 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 of 2017 is an example. While the target is believed to have been Ukraine, the computer virus affected many countries and companies globally. The resulting damage just to the Merck & Co., Inc. pharmaceutical company is was more than $1 billion.[7] It would provide further clarity if specific guidance were given on which types of attacks would be considered terrorism, and the relevance of the involvement of foreign governments in determining whether an act is considered terrorism or "war." 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 Department that an event was caused by non-governmental 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 GAO and the Congress should consider a different standard for cyberattacks—one that does not require the identification of the attackers.

The American Academy of Actuaries Cyber Risk Task Force appreciates that the GAO is turning its attention to the question of TRIA coverage for cyber risk. We look forward to working with you and the GAO staff to explore this topic and help resolve these various questions in advance of a real-life test of the law.

If you have any questions about this letter or seek additional information from the Academy, contact Marc Rosenberg, senior policy analyst for casualty, at 202-785-7865 or rosenberg@actuary.org.

[7] "Was It an Act of War? That's Merck Cyber Attack's $1.3 Billion Question"; *Insurance Journal*; Dec. 3, 2019.

Sincerely,

Edmund Douglas, MAAA, FCAS
Chairperson
Cyber Risk Task Force

Cc: Dan Garcia Diaz, Lijia Guo, Frank Todesco