DEPARTMENT OF THE TREASURY

Guidance Concerning Stand-alone Cyber Liability Insurance Policies under the Terrorism Risk Insurance Program

AGENCY: Department of the Treasury, Departmental Offices

ACTION: Notice of guidance.

SUMMARY: This notice provides guidance (Guidance) concerning the Terrorism Risk Insurance Program (Program) under the Terrorism Risk Insurance Act of 2002, as amended ("TRIA" or "the Act"). In this notice, the Department of the Treasury (Treasury) provides guidance regarding how insurance recently classified as "Cyber Liability" for purposes of reporting premiums and losses to state insurance regulators will be treated under TRIA and Treasury's regulations for the Program (Program regulations).

DATES: [INSERT DATE OF PUBLICATION IN THE FEDERAL REGISTER].

FOR FURTHER INFORMATION CONTACT: Richard Ifft, Senior Insurance Regulatory Policy Analyst, Federal Insurance Office, 202-622-2922 (not a toll free number), Kevin Meehan, Senior Insurance Regulatory Policy Analyst, Federal Insurance Office, 202-622-7009 (not a toll free number), or Lindsey Baldwin, Senior Policy Analyst, Federal Insurance Office, 202-622-3220 (not a toll free number).

SUPPLEMENTARY INFORMATION:

This Guidance addresses the application of certain provisions of TRIA[1] and the Program regulations[2] with respect to certain insurance policies covering cyber-related risks. This

[1] Public Law 107-297, 116 Stat. 2322, codified at 15 U.S.C. 6701, note. As the provisions of TRIA (as amended) appear in a note, instead of particular sections, of the United States Code, the provisions of TRIA are identified below by the sections of the law.
[2] 31 CFR part 50.

Guidance may be relied upon by the members of the public unless superseded by subsequent amendments to the Program regulations, or by subsequent guidance.

I. Background

TRIA was enacted following the attacks on September 11, 2001, to address disruptions in the market for terrorism risk insurance, to help ensure the continued availability and affordability of commercial property and casualty insurance for terrorism risk, and to allow for the private markets to stabilize and build insurance capacity to absorb any future losses for terrorism events. TRIA requires insurers to "make available" terrorism risk insurance for commercial property and casualty losses resulting from certified acts of terrorism (insured losses), and provides for shared public and private compensation for such insured losses. The Secretary of the Treasury (Secretary) administers the Program; pursuant to the Dodd-Frank Wall Street Reform and Consumer Protection Act, the Federal Insurance Office assists the Secretary in administering the Program.[3] The Program has been reauthorized three times, most recently on January 12, 2015, when President Obama signed into law the Terrorism Risk Insurance Program Reauthorization Act of 2015, extending the Program until December 31, 2020.[4]

TRIA requires participating insurers to "make available" terrorism risk insurance in connection with "property and casualty insurance" as defined in the Act.[5] By regulation, Treasury has further defined "property and casualty insurance" by reference to the classification of certain lines of commercial insurance set forth in the National Association of Insurance Commissioner's Exhibit of Premiums and Losses (commonly known as Statutory Page 14).[6]

[3] 31 U.S.C. 313(c)(1)(D).
[4] Public Law 114-1, 129 Stat. 3.
[5] TRIA sec. 103(c) ("make available" requirement); *id.*, sec. 102(11) (definition of "property and casualty insurance").
[6] 31 CFR 50.4(w).

Pursuant to the Program regulations, insurance reported on Statutory Page 14 under "Line 17 – Other Liability" is generally subject to TRIP. However, insurance reported on that page as "Professional Errors and Omissions Liability Insurance," a sub-line within "Other Liability" for state regulatory purposes, is expressly excluded from TRIP by the Act.[7] Under the Program regulations, "professional liability insurance" is defined consistently with "Professional Errors and Omissions Liability Insurance" as that term is defined for state law purposes.[8]

Cyber risk insurance is a broad term that includes insurance products covering risks arising "from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks," as well as "physical damage that can be caused by cyber attacks, fraud committed by misuse of data, any liability arising from data storage, and the availability, integrity, and confidentiality of electronic information."[9] The cyber risk insurance market has evolved significantly since it first emerged approximately two decades ago and is expected to continue experiencing rapid growth.[10] A 2016 report on cyber insurance noted that 19 different categories of coverage are available to a greater or lesser extent in the cyber insurance market, including first and third party coverage related to data breaches, cyber extortion, business interruption, data and software loss, physical damage, and death and bodily injury.[11]

---

[7] TRIA sec. 102(11)(xi) (excluding "professional liability insurance"); *see also* 31 CFR 50.4(w)(2)(xi).
[8] 31 CFR 50.4(t); *compare* National Association of Insurance Commissioners, Uniform Property & Casualty Product Coding Matrix (Effective January 1, 2016) (NAIC 2016 P/C Product Coding Matrix), p. 9, *available at* http://www.naic.org/documents/industry_pcm_p_c_2016.pdf.
[9] CRO Forum, "Cyber Resilience: The Cyber Risk Challenge and the Role of Insurance" (December 2014), p. 5, *available at* http://www.thecroforum.org/cyber-resilience-cyber-risk-challenge-role-insurance/.
[10] PricewaterhouseCoopers, "Insurance 2020 & Beyond: Reaping the dividends of cyber resilience" (2015), p. 10 (estimating that the global premium market will reach $5 billion by 2018 and at least $7.5 billion by 2020) (PwC Cyber Insurance Report), *available at* http://www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends-cyber-resilience.pdf.
[11] Cambridge Centre for Risk Studies and Risk Management Solutions, "Managing Cyber Insurance Accumulation Risk" (February 2016), pp. 10-11, *available at* http://static.rms.com/email/documents/managing-cyber-insurance-accumulation-risk-rms-crs-jan2016.pdf.

Cyber risk insurance remains an evolving insurance market, both in terms of product development and regulatory oversight. Certain insurance policies that may contain a "cyber risk" component or which do not exclude losses arising from a cyber event continue to be written in existing TRIP-eligible lines of insurance and are thus subject to the provisions of the Program.[12] Prior to 2016, some insurers that wrote stand-alone cyber risk insurance may have offered and reported it for state regulatory purposes as Professional Errors and Omissions Liability Insurance, which, as noted above, is expressly excluded under TRIA from the definition of "property and casualty insurance."

As of January 1, 2016, however, state regulators introduced a new sub-line of insurance, identified as "Cyber Liability," under the broader "Other Liability" line. "Cyber Liability" is defined for state regulatory purposes as follows:

> Stand-alone comprehensive coverage for liability arising out of claims related to unauthorized access to or use of personally identifiable or sensitive information due to events including but not limited to viruses, malicious attacks or system errors or omissions. This coverage could also include expense coverage for business interruption, breach management and/or mitigation services. When cyber liability is provided as an endorsement or as part of a multi-peril policy, as opposed to a stand-alone policy, use the appropriate Sub-TOI of the product to which the coverage will be attached.[13]

This Guidance confirms that stand-alone cyber insurance policies reported under the "Cyber Liability" line are included in the definition of "property and casualty insurance" under TRIA and are thus subject to the disclosure requirements and other requirements in TRIA and the Program regulations as specified in the following Section.

II. Guidance

[12] *See, e.g.*, PwC Cyber Insurance Report, p. 9 (noting likely existence of cyber risk coverage "within your wider property, business interruption, [and] general liability . . . coverage").
[13] NAIC 2016 P/C Product Coding Matrix, p. 10. "Sub-TOI" refers to "Sub-Type of Insurance."

Treasury provides this Guidance to clarify that the requirements of TRIP apply to stand-alone cyber insurance policies reported under a TRIP-eligible line of insurance.[14] This Guidance is designed to address the application of TRIA and the Program regulations to such cyber risk insurance policies due to the aforementioned developments in this area, which may have caused some marketplace uncertainty.

Guidance One (Cyber Liability Included in Property and Casualty Insurance)

Effective January 1, 2016, policies reported for state regulatory purposes under the Cyber Liability sub-line on Line 17—Other Liability of the NAIC's Exhibit of Premiums and Losses (commonly known as Statutory Page 14) are considered "property and casualty insurance" under TRIA.

Guidance Two (Application to In-Force Policies)

(a) An in-force policy reported under the Cyber Liability sub-line on Line 17—Other Liability of the NAIC's Exhibit of Premiums and Losses (commonly known as Statutory Page 14), and which provides coverage for insured losses under TRIA, is not eligible for reimbursement of the Federal share of compensation unless:

(i) The insurer offered coverage for insured losses subject to the required disclosures under 31 CFR 50 Subpart B; or

(ii) The insurer demonstrates that the appropriate disclosures were provided to the policyholder before the date of any certification of an act of terrorism.[15]

[14] As is the case with all other coverages subject to TRIA, policy losses that do not arise from an "act of terrorism" certified by the Secretary of the Treasury would not trigger the Program backstop. For example, an act cannot be certified as an "act of terrorism" unless it is, among other things, "a violent act or an act that is dangerous to human life, property, or infrastructure . . . ." 31 CFR 50.4(b)(1)(ii). To the extent a cyber event did not satisfy this requirement, the backstop provisions of TRIP would not be implicated. Any specific determination in that regard could not be made in advance and would depend upon the circumstances and considerations presented in any particular case.

[15] *See* 31 CFR Part 50, Subpart G.

(b) An insurer that did not make an offer for coverage for insured losses under an in-force policy reported under the Cyber Liability sub-line on Line 17—Other Liability of the NAIC's Exhibit of Premiums and Losses (commonly known as Statutory Page 14) is not required to do so at this time.

Guidance Three (Application to New Offers and Renewals of Coverage)

Effective April 1, 2017, and consistent with TRIA and the Program regulations, an insurer must provide disclosures and offers that comply with TRIA and the Program regulations on any new or renewal policies reported under the Cyber Liability sub-line on Line 17—Other Liability of the NAIC's Exhibit of Premiums and Losses (commonly known as Statutory Page 14).

Dated: December 20, 2016

Michael T. McRaith,
Director, Federal Insurance Office.

BILLING CODE 4810-25-P

[FR Doc. 2016-31244 Filed: 12/23/2016 8:45 am; Publication Date: 12/27/2016]