

January 18, 2022

Federal Insurance Office
ATTN: Richard Ifft
Room 1410 MT
U.S. Department of the Treasury
1500 Pennsylvania Avenue, NW
Washington, DC 20220

RE: Terrorism Risk Insurance Program 2022 Data Call – Request for Comments

Dear Mr. Ifft:

The American Property Casualty Insurance Association (APCIA) appreciates this opportunity to offer comments on the proposed 2022 Terrorism Risk Insurance Program Data Call. APCIA is the primary national trade association for home, auto, and business insurers. APCIA members represent all sizes, structures, and regions – protecting families, communities, and businesses in the U.S. and across the globe.

Treasury has proposed no unusual changes in 2022 to the portion of the data call relevant to terrorism coverage (other than for captive insurers). APCIA has no comment on those aspects of the proposed 2022 data call. However, Treasury has proposed to collect new data on cyber insurance coverage, whether or not such coverage relates to terrorism. Our comments below all relate to these new requested data elements.

Advance Coordination

As an initial matter, we note that both the TRIA authorizing statute and FIO's general authorizing statute (the Dodd-Frank Act) require Treasury to coordinate in advance with state insurance regulators and other agencies or sources of information before collecting any data directly from insurers. The Secretary is authorized to collect data directly only if she determines that the needed data is not available from other sources. After an initial rough start, Treasury and state insurance regulators now do an admirable job of coordinating the terrorism data call. However, Treasury is now proposing to collect non-terrorism cyber insurance data for the first time.

Treasury's Request for Comments makes no reference to its statutory obligation to coordinate in advance with state regulators (though it does ask for public comment on whether there are other public sources of data). Treasury is presumably aware that the National Association of Insurance Commissioners (NAIC) is already collecting some data on cyber coverages using different reporting parameters than those proposed by Treasury. We therefore urge Treasury to consult with state regulators to determine whether data in the NAIC's possession could be available and useful to Treasury as a substitute for the data Treasury proposes to collect directly from insurers. At a minimum, Treasury should document publicly the steps taken to meet its statutory advance coordination obligation and, if existing available data is not sufficient for Treasury's purposes, Treasury should explain why.

Retrospective Data Collection

Treasury proposes to seek data on cyber coverages *retrospectively* for the calendar year 2021. However, most insurers are unlikely to have collected some of the data being requested. While it might be possible (though burdensome) to collect the desired data prospectively, it is particularly burdensome to require insurers to collect data retrospectively, and in some cases may not even be possible as it would require seeking data from past policyholders who would have no obligation to supply the data. It is difficult for insurers to comply with data requests for data on the current calendar year and even more difficult, if not impossible, to provide data retrospectively. A retrospective data call, in particular, would likely involve a very labor-intensive, manual review of data (and manual collection of additional data). Compliance by the anticipated May deadline will be difficult for most insurers, and impossible for many. It was in recognition of this that, when Treasury first initiated the terrorism data call, responses in the first year were made voluntary and not mandatory. It would be appropriate to do so again as well with respect to any new cyber data to be sought for 2021. Even for prospective data call, IT systems cannot be changed overnight. Insurers need adequate lead time. Because 2022 has already begun and insurers have had no advance notice of Treasury's ultimate data requirements for this year, Treasury should delay any mandatory data collection on cyber coverage until the calendar year 2023.

Treasury should be aware that some of our members have said that Treasury's estimate of the work hours needed to collect and report the new cyber data is significantly understated, especially given that some of the data is not currently in the possession of many insurers. One member indicated that "up to 30 hours will be needed to interpret the requirements and to pull, summarize, validate, and format the data per the report specifications."

Collection of Data by Policyholder Size

Treasury has proposed to collect data on cyber coverage by policyholder size. Treasury's proposed measure of policyholder size is the number of employees the policyholder employs. With the exception of workers compensation coverages, most insurers have no underwriting-related reason to collect this data and thus will not have the data readily available. Treasury's Request for Comments does not explain how policyholder size provides useful information to Treasury in its study of cyber exposures and coverages, and we therefore urge Treasury to consider eliminating the requirement that reported data be broken down by policyholder size.

We speculate that Treasury may be attempting to equate the degree of risk exposure to policyholder size. If so, APCIA is not certain there is an appropriate method by which to measure size. Employee headcount seems to us an unreliable indicator. For example, a policyholder with a relatively small number of employees might nevertheless maintain a large data base of electronic records posing a degree of exposure that is not commensurate with the size of the company's workforce. We have considered whether premium volume would be a better measure. In some ways it might, but then policyholders are rated based on a number of factors unrelated to size. Moreover, cyber coverages written for large policyholders may be syndicated risks with multiple insurers on the risk, so the amount of premium charged by one insurer would not necessarily be indicative of policyholder size. We have also considered whether annual revenues would be a good measure. Again, depending on Treasury's goals, it might, but revenues are not necessarily indicative of risk exposure. Moreover, some of our members have told us that they do not collect this information.

For these reasons, we reiterate our recommendation that Treasury abandon its proposal to collect data by policyholder size. Should Treasury nevertheless desire to pursue that data, APCIA would be happy to engage with Treasury staff to try to better understand Treasury's needs and determine how we can help Treasury meet them.

Extortion vs. Ransom Coverage

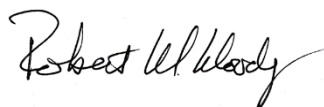
Treasury is also requesting data on liability limits and loss payments on both extortion and ransom coverage, with each to be reported separately. Some APCIA members have indicated that these are not always separate coverages. Thus, Treasury might consider whether and how insurers can indicate to Treasury that they do not provide these coverages separately. Some members have also said that they do not have separate loss codes for extortion and ransom coverage, meaning that it may be difficult or impossible for some insurers to break this data down in the manner Treasury has requested.

Some members are also unclear as to how Treasury would define extortion and ransom coverages and what the difference is between them. The usefulness and integrity of the data Treasury collects is dependent upon all insurers reporting data in the same way and with a uniform understanding of Treasury's requirements. We therefore urge Treasury to provide a clearer explanation of this in any final data call.

Finally, we note that some insurers may provide cyber as a named risk (*i.e.*, not "silent cyber") in a package policy, but without separate limits applicable to the cyber risk(s) or with a sub-limit(s) for cyber risk(s). While insurers could simply report the policy's overall limits (or the cyber sub-limit as applicable) in responding to Treasury's cyber questions, Treasury might consider whether it would be useful to know whether the limits are risk-specific and separate from other covered risks or not. Again, though, this may be difficult for some insurers to provide, especially retrospectively.

APCIA appreciates the opportunity to provide these comments and we are available to FIO staff on an ongoing basis to assist with this and any other matters in any way we can.

Sincerely,



Robert W. Woody
Vice President & Counsel