DEPARTMENT OF THE TREASURY
FEDERAL INSURANCE OFFICE (FIO)
ADVISORY COMMITTEE ON RISK-SHARING MECHANISMS (ACRSM)
MINUTES –26 JULY 2023

The Advisory Committee on Risk-Sharing Mechanisms (ACRSM) convened at 3:30 pm on 26 July 2023, in the Cash Room at the U.S. Department of the Treasury, 1500 Pennsylvania Ave. NW, Washington, D.C., with Annette Burris, Designated Federal Officer, presiding.

In accordance with the Federal Advisory Committee Act, the meeting was open to the public.

Committee Members Present

KEITH BELL, The Travelers Companies, Inc.
DEREK BLUM, RMS *
MICHAEL COHEN, RenaissanceRe*
ERICA DAVIS, Guy Carpenter*
JOHN LUPICA, Chubb *
PETER MOLLER, Arch Re *
THOMAS SRAIL, Willis Towers Watson
DR. JOANNA SYROKA, Ph.D., Fermat Capital (proxy for Dr. John Seo)

Also Present

ANNETTE BURRIS, Senior Insurance Regulatory Policy Analyst, Federal Insurance Office, (Designated Federal Officer)
TOM CLEMENTI, CEO, Pool Re *
RICHARD IFFT, Lead Management and Senior Insurance Policy Analyst, Terrorism Risk Insurance Program, Federal Insurance Office
JEREMY PAM, Senior Insurance Regulatory Policy Analyst, Federal Insurance Office
STEVEN SEITZ, Director, Federal Insurance Office

* Denotes virtual participant

Welcome and Opening Remarks

Annette Burris (DFO) welcomed everyone to the first 2023 meeting of the Advisory Committee on Risk-Sharing Mechanisms (ACRSM) and took roll. She then turned the meeting over to Director Steven Seitz who noted Michael Cohen, Peder Muller, Erica Davis, and Tom Srail as new members of the Committee. He also reminded the audience that the Committee was formed under the Terrorism Risk Insurance Program Reauthorization Act of 2015 to provide advice, recommendations, and encouragement to Treasury regarding the creation and development of nongovernmental risk-sharing mechanisms for protection against losses arising from acts of terrorism. He also thanked the Committee for helping advise FIO on the Terrorism Risk Insurance Program (TRIP). Director Seitz also reminded the group of the 2019 reauthorization of the Program and its extension until 2027. He also updated the Committee that FIO will become the Chair of the International Forum for Terrorism Risk (Re)insurance Pools (IFTRIP) in 2024.

2020 Past Work of the ACRSM Committee

The meeting then moved to Richard Ifft, who provided a recap of past ACRSM initiatives and report recommendations. He moved through past Committee recommendations and provided updates on activities around these short and long-term issues:

1) Cyber: The Committee recommended that FIO consider cyber risk insurance in the context of the Program. Also noted was the FIO Cyber RFI and FIO's role, as a result of GAO report recommendations and the National Cybersecurity Strategy, to determine if there should be a federal insurance response for catastrophic cyber risk.
2) Nuclear Biological Chemical and Radiologic Exposures (NBCR): While NBCR risk can be excluded in most TRIP lines, Treasury's data calls reflect that many carriers do not fully exclude NBCR risk in all cases. The Committee in the past noted the concern that TRIP's current structure may leave uncovered insured losses that could exceed the program cap of $100 billion annually. FIO is currently performing modeling to assess likely program responses; the initial results of that modeling reflect that even after accounting for the scope of NBCR exclusions, there remains the possibility of covered losses for a single terrorism event involving NBCR agents in excess of the program cap.
3) Certification: The Committee provided recommendations concerning guidance, structure, and timing of the certification process to address market uncertainty issues. In furtherance of this work, FIO issued a federal register notice in November 2020, seeking comments on these and related issues concerning certification, and is continuing to consider those issues, and looks forward to working with the Committee on that matter.
4) Insurer Marketplace Aggregate Retention Amount (IMARA): The IMARA is the threshold for determining whether Treasury must recoup payments it makes under the Program. Under TRIA, if annual payments made by all participating insurers are below the IMARA, then Treasury must recoup all amounts expended at a premium of 140 percent, up to that IMARA threshold. If total annual payments by participating insurers are above the IMARA, then Treasury has the discretionary authority, but not the obligation, to recoup all of the expended amounts that are above the IMARA threshold. The IMARA figure for calendar year 2021 was $41.7 billion. For 2022, it was $42.6 billion, and for 2023 it is now $45 billion. The IMARA increases annually with the increasing insurer premium base, meaning that the amount between the IMARA and the program cap of $100 billion will continue to decrease over time, and the Committee recommended that FIO review the potential consequences of this for the Program.
5) Recoupment: Recoupment is required at a factor of 140 percent of all amounts expended by Treasury to the extent insurers have not paid amounts satisfying the IMARA. The Committee inquired whether there was some mechanism to keep the Federal Government from recovering more money than it expends in connection with an act of terrorism. FIO is continuing to analyze the issue.
6) Captive Insurers: Captive insurers, or alternative carrier mechanisms, participate in the Program as licensed insurers. Treasury does retain rule-making authority over their participation in the Program. FIO has in the past provided guidance on the issues presented by captives. The Committee recommended that Treasury examine that the participation of captive insurers in the Program, noting that because of the small deductibles that captive insurers can have, captives may obtain disproportionate recoveries under the Program as compared with what a conventional insurer might be able to recover. Treasury's November 20, 2020, Federal Register request for comments also sought information on these issues. Treasury expanded its annual data call to require captive insurers to provide even more detailed information than is currently required for other categories

to address some of those matters.

7) Risk Transfer: The Committee made several recommendations suggesting that FIO take further steps to increase its modeling and risk assessment capabilities. Treasury has acted on this recommendation to obtain access to modeling capabilities that allow it to evaluate the impact of acts of terrorism, both on the marketplace, as well as their potential impact upon the TRIP reimbursement structure. Treasury included its initial results of its modeling analysis in this year's Small Insurer Report and will continue to work with these tools. FIO also encourages recommendations from this Committee for further work in this area.
8) Nonprofits: In the 2019 Reauthorization Act, Congress required that Treasury evaluate whether places of worship were able to obtain affordable terrorism risk insurance coverage. Treasury's analysis since 2019 indicates that such places of worship can and do obtain such insurance. The Committee suggested in its 2020 report that Treasury expand this analysis to include nonprofit entities more generally. Based upon Treasury's engagement to date, most of the issues that have been raised by the nonprofit sector relate to property and casualty insurance generally as distinguished from terrorism risk insurance specifically.

Mr. Ifft concluded this portion of his presentation, and the meeting was opened for questions from the members. No questions were asked on past issues and updates.

2023 Terrorism Risk Insurance Program Small Insurers' Report

Richard Ifft then moved to the features of the 2015 Terrorism Risk Insurance Program Reauthorization Act explaining that in addition to collecting data, Treasury does report to Congress on an annual basis about the Program. In even-numbered years, FIO produces a general report on the effectiveness of the Program. In odd-numbered years, FIO's report addresses the competitiveness of small insurers in the terrorism risk insurance marketplace. Treasury completed that report this year using the most recent data obtained for calendar year 2022 and produced the report to Congress on time. By statute, the report is required to summarize various specified issues. Small insurers are defined as entities that cannot trigger the Program simply based upon satisfaction of their own individual deductible, so they have annual TRIP-eligible lines premium of less than $1 billion a year. Over the last three years, 2020, 2021, and 2022, there has been a steady increase in the small insurer percentage of the terrorism risk insurance market, with annual premiums increasing from $22 billion in calendar year 2020, to $31.2 billion in calendar year 2022.

In addition, Treasury looks at the extent insurers are extending terrorism risk insurance at a zero-cost premium. In prior reports, FIO observed that small insurers typically had a greater percentage of their policyholders than larger insurers where there was no specific charge allocated to terrorism risk. That figure is now the same for both small insurers and larger insurers, such that about 33 percent of all domestic U.S. insurers are extending terrorism coverage for a zero-dollar premium.

Mr. Ifft stated FIO also looked at take-up rates in general and by line of business for small insurers. The take-up rate for policy holders of small insurers does tend to be somewhat lower than for larger insurers. 61 percent of the policyholders of non-small or large insurers obtained terrorism risk insurance, and that figure was 55 percent for small insurers and varies somewhat by line of business. FIO also looked at geographic writings of carriers and noticed the smaller the insurer is, the more likely its writings are going to be concentrated in a smaller number of states. As the insurer gets larger and larger, that universe of states tends to expand.

Mr. Ifft then addressed the harder look FIO is taking on cyber insurance and cyber policies. Small insurers do participate in the cyber insurance market. That participation is somewhat less than it is for their participation in the TRIP eligible lines market overall. Small insurers have about a five percent share of the cyber insurance market, which is distinguished from their 12 percent share of the market as a whole. However, a closer observation of the data, focusing on policies issued to small policyholders, is that the market share of small insurers for this population goes up significantly. Measured by number of policies, the figure is 17 percent. Measured by premium, the small insurer share goes up to 26 percent. Small insurers, while they may have a smaller percentage of the market overall, have a materially larger market share when the focus is upon the universe of small business policyholders.

The presentation then moved to Nuclear, Biologic, Chemical and Radiological (NBCR) risk. FIO obtains reporting on whether NBCR risk is not entirely excluded from policies. For the last three years figures for small insurers, by premium, were 29 percent, 22 percent, and 20 percent, respectively. That is for the policies where the risk is not entirely excluded, and there are significant property events involving NBCR where even those percentages indicate there could be some significant aggregate exposures presented. Looking at liability limits as opposed to property limits, approximate 20 percent (by premium) does not fully exclude the risk.

In addition, small insurers tend to have a smaller share of the market in the property and casualty lines of insurance not subject to the Program (for example, auto), as compared to the TRIP-eligible lines of insurance. The small insurer share of P&C lines not subject to the Program is approximately eight percent, as compared with the 12 percent share of the market they have in the TRIP-eligible lines of insurance.

FIO also considers the scope of terrorism risk insurance under the Program provided for places of worship. Significantly, small insurers are the largest provider of terrorism risk insurance for places of worship than any other segment of the market. Measured by premium, small insurers represent just over 50 percent of the market, with larger insurers providing less than 50 percent, and much smaller shares contributed by alien surplus lines insurers and captive insurers. This is an area where small insurers are the largest market participant.

Mr. Ifft finished his presentation by addressing FIO's new work in terrorism catastrophe risk modeling. FIO now has modeling capability that allows it to look at the financial risk presented by terrorism attacks at specific locations (GPS coordinates, addresses, zip codes) and involving a variety of attack modes. Those figures can then be analyzed against the actual TRIP structure, allowing FIO to estimate what the impact both to industry and the government will be on account of the total indicated losses.

Mr. Ifft concluded, and the group was asked if they had any questions.

Tom Srail asked about the analysis of small policyholders and what constitutes a small policyholder and whether it is by revenue size or policy limit size. Richard Ifft answered that a small policyholder, as defined in cyber portion of the data call, was an entity with under 100 employees, or $10 million or less in revenue.

Mr. Blum asked a question of Mr. Ifft: Captive insurers are an outlier in that their premium increased in the 2022 data call, and then went back down in 2023. Is there an explanation for that? Did something change in the way you were capturing data or requesting data that would explain this? Or is this simply that there was an increase in the amount of insurance and then a decrease?

Mr. Ifft stated it shouldn't have anything to do with the way we collect the data because the new categories introduced in 2022 simply required more granular reporting, opposed to changes in the data categories. For captive insurers the premiums for that sector may go up or down depending upon market conditions and the industry generally, and FIO's work to date has not analyzed for that.

Mr. Blum had a follow-up question about data collection in general: When Treasury puts out the data call, do you get 100 percent response? And what happens and what happens if you don't? Was there a difference in the rate of response between small versus non-small insurers?

Mr. Ifft responded that FIO gets what it considers to be very close to 100 percent reporting. The uncertainty on the reconciliation is based upon the fact that it is based upon the carrier's reporting to state regulators through the NAIC. There is not 100 percent coincidence between the NAIC lines of insurance and the TRIP-eligible lines of insurance. FIO tries to get them as close as possible, but in some ways, they cannot be reconciled entirely. FIO does estimates, which is easier with the larger insurers, because there are fewer of them involving a lot more money, making it easier to look at those. It also appears that there is virtually 100 percent reporting for smaller insurers. When comparing our results with the NAIC reporting lines or reporting figures, it appears to be lower, that it goes down to maybe 80 percent. NAIC data may include a lot of non-TRIP eligible premium in certain lines otherwise subject to TRIP, therefore comparison points are not perfect. The companies appreciate their obligation to report, and it is FIO's belief the companies understand their obligation to do this and are doing it. We do check periodically with individual companies and sometimes call companies to inquire why they haven't reported when the NAIC data would suggest that they should. Invariably, the answer is the premium that we're seeing in the state reporting isn't TRIP eligible lines premium. It then brings them down under the reporting threshold and hence there's no requirement to report. FIO does have a $10 million reporting threshold on an annual basis which represents about a half of one percent of the entire market, which ultimately excuses about 400 entities from having to report. From a burdensomeness standpoint, we've always felt that was the right decision to make.

No future questions were asked by the members.

FIO's Catastrophic Cyber RFI

Jeremy Pam with FIO then began his presentation on cyber. FIO increased its collection of cyber related data as part of its annual TRIP data calls beginning in 2022, and first reported on it in the 2022 TRIP effectiveness report. This is continued in FIO's data call this year, and in the Small Insurer Report. FIO's annual reports have also included discussions of cyber insurance and cybersecurity. FIO coordinates cyber insurance and cybersecurity issues with our other Treasury offices, and other parts of the Executive Branch, such as the White House's Office of the National Cyber Director, or ONCD.

Mr. Pam explained the current activity around cyber. Last June, the Government Accounting Office (GAO) issued a report on cyber insurance that concluded with a recommendation (which Treasury and the Department of Homeland Security (DHS) accepted) that FIO and DHS' Cybersecurity and Infrastructure Security Agency (CISA) conduct a joint assessment to determine the extent to which risks on critical infrastructure from catastrophic cyber incidents and potential financial exposures warrant a federal insurance response. FIO, in coordination with CISA, published in the Federal Register on September 29th, 2022, a request for information, or RFI, seeking comment on a number of questions related to a potential federal insurance response to catastrophic cyber incidents. These questions focused on whether a federal insurance response is warranted, if so, what form such a response might take. The questions formed around:

1. The nature or definition of catastrophic event, such as how does it relate to critical infrastructure.
2. How to measure financial and insured losses, including data and methodologies. It also asked about which cybersecurity measures are most effective, and related, if at all, to a federal insurance response.
3. Insurance coverage availability such as what coverage is available and what limitations in coverage exist.
4. What data and research is useful, and what would respondents be willing to share with the government.
5. Whether respondents thought a federal insurance response is or is not warranted.
6. Detailed questions around potential structures for federal insurance response, including, potential models for an insurance response, whether participation should be required, what the scope of coverage might be, and how it should relate to reinsurance.
7. A concluding catchall question was asked for any other issues.

There here were 60 comments, 56 unique, from a wide range of commenters. These commenters included insurers and reinsurers (including specialist cyber insurers), insurance and reinsurance brokers, an insurance rating agency, multiple trade associations (insurance, reinsurance, and insurance related), insurance risk modeling analytics organizations, insurance think tanks and academic experts, cybersecurity consultants and cybersecurity product companies, and 15 organizations representing multiple critical infrastructure sectors, including the financial services sector, the healthcare and public health sector, the energy sector, the communications sector, and the food and agriculture sector.

Mr. Pam went on to describe high-level summary of a few commenter themes that were identified from these RFI responses. There were six key initial themes:

1. Broad support for developing some type of future federal insurance response. Commenters that expressed this view include primary insurers, reinsurers, insurance and reinsurance brokers, reinsurance and insurance-related trade associations, insurance risk modeling analytics organizations, insurance think tanks, academic experts, cybersecurity consultants, and cybersecurity project companies, and the trade associations speaking for the critical infrastructure sectors. Some commenters expressed the view that adopting a federal insurance response now would be premature, citing the still developing cyber insurance market. However, these groups also stated their support for further investigation and analysis.
2. There was general agreement that any federal insurance response should address cyber hygiene. Responses listed specific cybersecurity controls that should be part of insurer enforced minimum cybersecurity standards, such as multifactor authentication, end point detection and response, software patching and update discipline, network segmentation, offline backups, and regular cybersecurity training. Some of the commentators noted that required cybersecurity controls would help mitigate the potential moral hazard effect of providing government support for insuring cyber incidents. A few stated that access to a new federal insurance response should be explicitly conditioned on the adoption of cybersecurity controls meeting minimum standards. Other commentators noted potential limitations in what can be accomplished by even the best cybersecurity controls. A few commenters called for the Federal Government to promote and encourage cyber hygiene best practices to help inform private insurer underwriting.
3. Commenters proposed a range of ideas for the structure of a potential federal insurance response. FIO is continuing to evaluate these different proposals. Proposals included (a) creation of a new structure not modeled on any existing government program; (b) a new structure loosely modeled on but separate from the Terrorism Risk Insurance Act, and TRIP, dedicated to addressing catastrophic cyber risk; (c) amending TRIA to expand TRIP to cover catastrophic cyber incidents more generally; (d) create a new governmental public private partnership modeled on the UK's Pool Re; (e) create a new structure modeled on FEMA's National Flood Insurance Program; and (f) create a new structure based upon a government sponsored enterprise analogous to Fanny Mae or Freddy Mac under which the Federal Government would assume catastrophic cyber risk.
4. Some commenters stated that TRIP is not the best model for a federal insurance response relating to catastrophic cyber risk. Some of these commenters noted reservations about a certification process, particularly one with an attribution requirement.
5. Commenters suggested numerous structural elements not featured in TRIA. Several commenters expressed preference for a pure financial trigger, stating that this is preferable given the other complexities already inherent in cyber risk.
6. There was support for cross-border scenarios while assessing catastrophic cyber insurance. Some commenters stated that the likely international need of a catastrophic cyber incident requires careful consideration of how a U.S. federal insurance response would address cross-border issues. Specific scenarios raised included losses from a catastrophic cyber incident in the U.S. by a non-U.S. entity.

Mr. Pam then went to speak about the collective work on catastrophic cyber insurance. FIO, in coordination with CISA and ONCD, is conducting post-RFI engagements with commenters and other public and private sector stakeholders, including international counterparts. Mr. Pam closed with stating the high-level summary of the main issues raised by commenters does not

suggest FIO's endorsement of or agreement with any of the themes suggested. FIO, CISA and ONCD will coordinate to undertake the substantial analysis and engagement on whether there needs to be a federal insurance response for catastrophic cyber risk, and if so, what form it will be.

With closing, the members were asked if there were any questions. Dr. Joanna Syroka noted that she believed consideration should be given to cybersecurity controls required by the insurance industry, the relevant policy terms and conditions, the capital regime governing the existing cyber insurance market, and its claims-paying capacity for catastrophic cyber events. Mr. Pam responded by acknowledging a need to understand the full capabilities of the private market as an important component of the analysis, including how the capital regime currently works from either a ratings perspective or a regulatory point of view. He indicated that it would be important to understand what kind of events the industry could withstand and where the government may need to step in.

Dr. Syroka then had a follow-up, stating the easiest thing would be to get an understanding of what the capital regime is from a rating agency standpoint (noting that rating agency requirements may be more onerous than existing regulatory requirements), and that a global perspective of these issues be taken. She suggested as a starting point speaking to one of the rating agencies about how they view cyber insurance, how they treat capital requirements in the line of business, and how that compares to other lines of business. She indicated that it would be important to understand their thoughts and where they plan to go with the cyber line of business from a catastrophe point of view.

Mr. Pam acknowledged that insight.

Erica Davis stated that she had information on that point she could share if helpful, and stated her organization has quarterly meetings with the rating agencies with a focus on North America. Mr. Pam welcomed any help and would share his contact information afterward.

There were no further questions around the Catastrophic Cyber presentation.

The meeting then turned over to Mr. Steven Seitz to introduce the next speaker, Tom Clementi from Pool Re, and acknowledged the late evening hours as he joined virtually in from the U.K. A background was given on Mr. Clementi, as newly appointed CEO of Pool Re. Mr. Clementi was with Lloyd's of London prior to joining Pool Re and has also served as a counselor for the City of London.

Pool RE

Mr. Clementi thanked Mr. Seitz for the introduction and begins by discussing Pool Re and what is being planned in the coming 12 months, as well as advances they are making in modeling capabilities, and Pool Re's work with IFTRIP, and some comments around U.K. cyberspace.

Mr. Clementi gave an overview of Pool Re and how it began in the face of the Irish Republican terrorism in the 1990's, and the mainland bombing campaigns that led to the withdrawal of terrorism coverage by the private insurance market. Pool Re was established as an insurance

industry mutual backed by the U.K. Treasury. It provides unlimited terrorism coverage to the U.K. insurance market in return for premiums. In the last 30 years, there has been very few claims and therefore Pool Re has built a substantial reserve fund. If the fund is exhausted by an event, the U.K. Government would then provide an unlimited guarantee.

He then mentioned four key elements of the Pool Re system:

1. The offering of risk-based pricing for businesses that can demonstrate they have taken appropriate and preventative measures to reduce the threat of terrorism or mitigate the impact.
2. Investment in wider resilience initiatives, by using a small portion of funding to support U.K. homeland security projects that can reduce or mitigate terrorism threat. Initiatives such as counterterrorism technology or detection of toxic gasses in public spaces.
3. Monetizing the financial support that the U.K. government provides by paying the government 2 billion pounds over the last few years for the guarantee that is given, which hasn't been used in 30 years.
4. A prefunded pool that enables fast and secure payments to be made to businesses after an event. This enables it to inject funding quickly into the U.K. economy after a large terrorism event, and with minimal likelihood of fraud. He interjected as an example that after COVID-19, there was an attempt to get money into the hands of businesses on an ad hoc basis where funding sometimes did not make it to the correct people. Conversely, he noted, Pool Re's scheme gets money into the businesses that need it with little chance for fraud.

Over the last 30 years, the terrorism threat has evolved and so has the coverage for its members. It started with basic foreign explosion, but now includes CBRN, non-damage business interruption, as well as physical damage caused by cyber. Mr. Clementi stated that this has allowed the private market to flourish and enabled a buffer of private sector capital to sit between the U.K. taxpayer and a terrorism event. Showing figures on a slide, he noted it is estimated that the government's attachment point is around the 13-to-15-billion-pound mark. In the case of an event, the members retain the first 250 million pounds, then there is retrocession of 2.5 billion pounds, including a cap on what is bought from the private market. It then moves into the balance of the fund and then into the government guarantee. If there were to be a very big event it is likely premiums would go up significantly, take up would increase and the attachment point then becomes nearer to 13-15 billion pounds. He noted that it would be a quite remote event before the government gets involved, highlighting model estimates reflecting around a 1 in 2000 return.

Mr. Clementi then went on to state that Pool Re operates a facultative reinsurance scheme, which means that risks are passed back to our member insurers on a risk-by-risk basis, but there is a proposal to change this to a catastrophe treating model. There is also a proposal to bifurcate conventional terrorism from non-conventional terrorism, such as cyber and CBRN. This enables the retention structure to be split between CBRN and conventional bomb blasts. Member insurers have been clear they have a limited appetite to underwrite more CBRN risk but are prepared to accept more conventional terrorism risk onto their balance sheets. Splitting terrorism in two enables retentions for conventional terrorism to increase with more risk returned to the private market, which further insulates the British taxpayer from risk of loss.

There are three reasons for making the changes:

1. A delivery of a scheme with less operational friction that is fit for contemporary digital insurance marketplaces.
2. It returns risk to the market to distance the government and the taxpayer from picking up the tab.
3. It enhances resilience of the U.K. economy by increasing penetration of terrorism insurance coverage amongst small and medium-sized enterprises (SMEs).

Moving to a treaty structure gives member insurers flexibility around pricing and facilitates the reintegration of terrorism coverage back into standard property policies. Many entities across the U.K. will find themselves covered for terrorism, especially outside the peak zone (Central London) without asking to be covered.

Pool Re is also enhancing modeling capabilities and has been building a model in recent times. Historically the model has been a simplistic one, a tariff-based rating schedule where there is a different rate based on different zones in the country. They are moving from that tariff system to a system that is risk reflective in pricing and should make it cheaper to buy coverage, especially if the bulk of risk falls within member retentions.

The model is an exposure-based catastrophe model based around frequency and severity, with a set frequency and severity assumptions for each threat that is covered. There is a distribution for frequency and severity. It covers all threats Pool Re addresses, from knife attacks to conventional explosions, gas, airplane impacts, or physical damage from a cyber trigger (i.e., remote digital interference). These are passed through a simulation engine, and it comes up with an overall loss distribution. The Tyche platform is used, which is owned by Aon. Modeling is done at a policy and risk level to be able to capture loss for any member. Annual data collection is done, and it takes approximately four months to scrub data, which helps them understand how exposure changes year to year. There are visualization capabilities which allows them to draw an area around an event and download the exposures in that area that may have occurred. Data is at a postal code level, similar to U.S. zip codes. Data is now in the 95th percentile, up from 65 percent in 2017.

Mr. Clementi then spoke to work with academic institutions around CBRN scenarios, as well as cyber. In collaboration with Guy Carpenter and Cranfield University there have been created computational fluid dynamic structures around bomb blasts, showing how blasts move around, over, and in-between buildings. These modeling initiatives are a priority for Pool Re and underpin the move to a treaty model that will go live in April 2025.

Mr. Clementi also spoke about IFTRIP's role in the international forum. He noted Steven Seitz's role in IFTRIP as the Vice Chair with a step up as the Chair at the end of 2023. He noted the importance of the forum in years ahead and entering an age of insecurity. He stated there have been bookend events of catastrophic loss in the last 23 years such as 9/11, the global financial crisis, and the worldwide pandemic. Given climate change and AI, he stated the concern from a cyber risk point of view. There are many other countries facing these same challenges with the potential to be systemic in nature. Public/private partnerships and pools within IFTRIP can really help address some of the challenges and will ensure that the insurance industry maintains

relevance in the years ahead. IFTRIP is a forum for collaboration on these issues with the focus on terrorism, but also other risk that share similar characteristics that are hard to insure and have the capacity to aggregate a pace across sectors and geographies. IFTRIP conferences attract many important players to discuss these issues.

IFTRIP is looking at systemic cyber events and climate changes, as well as CBRN. Climate change is a national security issue and its impact on terrorism is important as a long- term driver along with population growth. Population growth in central and sub-Saharan Africa, particularly amongst 15 to 25-year-old males, is a driver of terrorism. This is where you see climate change the most which is going to move people over the next few decades, and they are coming north to Europe. This will create a gloomy outlook for the foreseeable future. IFTRIP will help us discuss these issues and commission research to understand how to prepare.

Pool Re also did work with Oliver Wyman on the state of cyber insurance in the marketplace and what the insurance market could do in conjunction with the government to enhance cyber resilience in the U.K. The study was done because of the fast-growing cyber market worldwide, where the bulk of the global premium probably relates to U.S. businesses. He noted the cyber market has developed as a standalone dedicated line of business, incorporating appropriate exclusions and supplements, and has repriced in the light of recent ransomware attacks. The cyber market deserves credit but there are significant gaps, and the Oliver Wyman study looked at those. The study focused especially on the demand side, but on the supply side as well, which relate to larger corporations and critical national infrastructure. Root causes of protection gaps were looked at, and how to shore these gaps and create resilience. Supply and demand challenges was also looked at.

Pool Re is looking to work with the rest of the U.K. insurance industry, trade associations, large companies, and brokers as well as the National Science Security Center to find consensus on initiatives moving forward. There is an expectation the industry speaks with a united voice to and ideas before asking for government support. Potential initiatives focus on the demand side. The insurance press in the U.K. focuses on supply side issues in relation to capacity shortages, often related to cyber war exclusionary language. This obscures the almost bigger issue of demand which causes waves in the economy. Raising educational awareness of threats is one idea brought forward, helping businesses understand cyber impacts and how it may manifest, as well as educating around the cyber insurance and what it covers and does not cover. Like the U.S., possibly linking cyber certification to the underwriting process. Showing good cyber hygiene is in place at a policyholder could lead to a premium discount. Another idea is making cyber insurance a prerequisite to winning a government contract. At present, this happens in the U.S. more so than the U.K. as a requirement.

Mr. Clementi mentioned some of the issues that will need to be addressed on the supply side, including data sharing. He noted that sharing data is important to supporting the sheer volume of capital which underlies the Nat Cat market and will be similarly important to address the amount of capital that needs to be brought in to support the growth of the cyber insurance market in the next decade. He stated improving the quality of the data and modeling will help attract capital. This review can be done by industry without government support. He interjected other initiatives could be controversial such as attribution, since cyber events can be held up for years determining if it was an act of warfare, criminality, or terrorism, and where the actor is located

jurisdictionally. Therefore, he indicated event classification should be based on impact and hopefully that will help with speedy payment. The last is a cyber classification system that could be used as a trigger for any kind of public-private partnership. He opined that a Cyber Re in the U.K. would only follow large events and be something that could be stood up preemptively. Penetration for cyber insurance in the U.K. is limited, particularly among SMEs, and to a lesser degree among large corporations and critical national infrastructure. If there was a critical cyber event the volume of losses would not reach a level the government would be expected to stop in. Like with Pool Re, a Cyber Re attachment point may likely be around 15 billion pounds. Economic losses may reach that point, but insured losses may not.

Mr. Clementi concluded his presentation and Ms. Burris thanked him and opened the floor up for questions.

Mr. Keith Bell began by asking about the involvement of the U.K. government since Pool Re appears to be a mutual insurance company, and what are the members of the mutual. Mr. Clementi stated it is a reinsurance company, a mutual owned by members, and that Pool Re retains its own operational freedoms, governance, and ability to nominate directors and appoint board. The government only steps in when claims arise and burn through the fund. Large changes to need to be run past the Government but its involvement is limited.

Mr. Bell then followed up on a question on capital requirements under Solvency II and where there are any provisions for distribution of earning back to the customer. Mr. Clementi answered that Pool Re is Solvency II exempt because of the unlimited guarantee of the government. As far as distribution, Pool Re makes a significant payment to the government for the guarantee, which is 50 percent of premium income into the U.K. Treasury. Pool Re is required to pay 25% of any surplus on both underwriting and investments, which has been around 2 billion pounds since 2015, and has never called on the guarantee. This is also done for three years in arrears, and they accrue interest on some of those payments. The members also get a distribution, approximately 25 percent of the surplus. By distributing the surplus during high inflation years, the buffer between the U.K. taxpayer and a terrorism event has shrunk, and they are currently looking at how to address that.

Derek Blum asked whether Pool Re is only covering property losses, and if there is life insurance coverage. Tom responded they are only a property reinsurance company and pay for physical damage with some non-damage business interruption loss coverage as well. A new piece of legislation has been introduced that will require publicly accessible locations of 100 or more to have terrorism mitigation measures. This will spur businesses to pick up public and employee liability. He noted it will be interesting to see how the market responds, and if there will be a gap. He added that Pool Re is a brick-and-mortar insurer and he is cognizant that terrorists are more inclined to go after human targets where casualty reinsurance would be more applicable. Mr. Blum responded that he expects any measure put into place to reduce human casualty would benefit the property side as well.

There were no more questions and Annette Burris thanked Mr. Clementi, and he replied he was honored.

Ms. Burris then began with new business and administrative announcements. The first was a reiteration that FIO will become the chair of IFTRIP in 2024, and as chair will host the 2024 IFTRIP pools meeting in Washington, D.C. She then announced that Richard Ifft will have a new title as Lead Management and Senior Insurance Policy Analyst of the Terrorism Risk Insurance Program. The meeting was also updated with the announcement of the Committee's administrative session approvals. The first was that Dr. John Seo of Fermat Capital was chosen as Chair of the ACRSM, noting he could not be at the meeting. In addition, two new subcommittees were established around cyber risk and another around modeling and leads for those subcommittees were also chosen.

Ms. Burris then opened the floor for the Committee to discuss possible work within the newly formed subcommittees, and their focus. Dr. Joanna Syroka suggested the need for research into what the private sector was doing about cyber hygiene and cybersecurity protocols to understand what is driving movement in these areas. She also felt it was important to note the capital regime underlying cyber coverage and the ability of cyber insurers to pay claims in the event of a cyber catastrophe. Derek Blum noted that there are a lot of areas to cover for cyber besides attracting capital, another aspect is modeling for cyber and common definitions of events. Mr. Blum noted it is important on a global level to define what constitutes a cat cyber event. Tom Srail interjected that the IFTRIP work that Pool Re was looking into is also something our Committee could look at as well, noting the Cyber Insurance marketplace is heavily influenced by the U.K. He also stated the Committee should look very strongly at the RFI responses made last year and noted that the marketplace has changed a lot over the past three years.

Ms. Burris thanked the members for their input, then asked for any new business items the group would like to discuss. Hearing none, the meeting was adjourned at 4:59 PM.

I hereby certify these minutes of the July 26, 2023 Advisory Committee on Risk-Sharing Mechanisms public meeting are true and correct to the best of my knowledge.

Dr. John Seo, Ph.D.
Chair, ACRSM