The Advisory Committee on Risk-Sharing Mechanisms (ACRSM) convened at 2:00 PM on February 1, 2024, in the Cash Room at the U.S. Department of the Treasury, 1500 Pennsylvania Ave. NW, Washington, D.C., with John Seo, Chair, presiding.

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

Committee Members Present

JOHN SEO, Chair, Fermat Capital
D. KEITH BELL, The Travelers Companies, Inc.
DEREK BLUM, RMS
MICHAEL COHEN, RenaissanceRe*
MATT MCCABE, Guy Carpenter (Proxy for Erica Davis)
MIKE KESSLER, Chubb (Proxy for John Lupica)
THOMAS SRAIL, Willis Towers Watson

Also Present

JEANETTE QUICK, Deputy Assistant Secretary of Financial Institutions
STEPHANIE SCHMELZ, Deputy Director, Federal Insurance Office
ANNETTE BURRIS, Designated Federal Officer, ACRSM, Federal Insurance Office
RICHARD IFFT, Federal Insurance Office
JEREMY PAM, Federal Insurance Office

Speaker Participants

DAMINI MAGO, Panelist, RMS
DOUG ALBERT, Panelist, Guidewire-Cyence
PASCAL MILLARE, Panelist, CyberCube
STEFAN HOLZBERGER, Speaker, AM Best
MIKE LAGOMARSINO, Speaker, AM Best

* Denotes virtual participant

Welcome and Opening Remarks

Annette Burris (DFO) opened the first meeting of 2024 for the Advisory Committee on Risk-Sharing Mechanisms (ACRSM) and took roll. She welcomed Deputy Director of the Federal Insurance Office, Stephanie Schmelz for attending in place of Director Seitz, then turned the meeting over to the Chair, John Seo. Chair Seo opened the meeting with an overview of the agenda items which include programmatic updates, a moderated discussion with panelists from three modeling firms, insight from a modeling agency on emerging risks, and an update on FIO's evaluation of a potential

federal response for catastrophic cyber risk. He reminded the audience that although the agenda would have a cyber theme for the current meeting, future meetings would explore other terrorism risk-related issues. He then introduced Jeanette Quick, Deputy Assistant Secretary for Financial Institutions Policy at the Department of the Treasury.

Deputy Assistant Secretary Quick welcomed the attendees to the meeting, and provided the audience with her background when she served as Senior Counsel for the Senate Banking Committee and was involved with the reauthorization of the Terrorism Risk Insurance Program (TRIP) in 2015. She explained how the reauthorization changed certain aspects of TRIP, instituting the data collection and reporting requirements, as well as forming the ACRSM. She emphasized the importance of TRIP to the insurance industry and financial institutions, as well as the importance of the ACRSM membership to provide crucial insight to administer the Program.

Updates of the Terrorism Risk Insurance Program

Richard Ifft then updated the group on what FIO does to prepare for potential triggering of the Program in the event of a certified act of terrorism, analyzing the financial mechanics of the Program and if it is still pertinent in terms of the current insurance market, and continuing engagement with stakeholders. The Office continues to address operational readiness and administration issues with security upgrades to the TRIP Claims system, program forms, and calculation of the Insurance Marketplace Aggregate Retention Amount (IMARA). He noted the upcoming TRIP data call, and the modeling analysis the Office is continuing to do. He also spoke to FIO's involvement in the upcoming International Forum for Terrorism Risk (Re)Insurance Pools (IFTRIP) Conference.
Highlights of the presentation included:

1. The TRIP claims system security upgrade was a migration to the Treasury Cloud.
2. The TRIP claims system forms are updated every three years, and this year they were updated according to Paperwork Reduction Act parameters through the public comment process and approval from the Office of Management and Budget (OMB). No comments were received.
3. The TRIP claims system will be up and running within 10 days of a certified act of terrorism.
4. The IMARA for 2024, where the recoupment rate is 140 percent, will increase to $48.5 billion based on 2020-2022 figures. This was published in the Federal Register in December. FIO is looking at whether mandatory recoupment and the growing IMARA could lead to unintended results.
5. The eighth mandatory TRIP data call will be occurring in the coming months, and there were no major changes. There has been broadly consistent reporting every year, which helps the Office observe changes in the market. This year's report will address the Effectiveness of TRIP.
6. FIO acquired a modeling tool developed specifically for TRIP impacted events, at the recommendation of the ACRSM. The model was used for last year's

Small Insurer Report and continue to be used to model events that may impact the program.

7. The Office has also obtained a cyber risk model that will be able to show the impact of various cyber terrorism events.
8. Mr. Ifft noted that FIO is the Chair of IFTRIP for the next two years, and that it will be hosting the 2024 IFTRIP Annual Conference in Washington, D.C. There are 15 countries that are part of IFTRIP. The Conference will be the first in-person IFTRIP Annual Conference since 2019 and will be held in Washington in late April 2024.

No questions were asked by the membership.

Discussion on Modeling Cyber Catastrophic Events

Chairman Seo then turned to the next session, which was a panel discussion led by the Chair. The panelists for the discussion were Doug Albert from Guidewire-Cyence, Damini Mago from Moody's RMS, and Pascal Millaire from CyberCube. Questions were holistically aimed toward various approaches within catastrophic modeling, and different viewpoints that influence the available models. He also referred to the potential impacts of such catastrophic events upon TRIP.

1. The first question asked panelists to rate from 1 to 10 where cyber cat modeling was five years ago versus today, and where it may be in the next five years.
    a. Doug Albert stated that five years ago he would rate cyber modeling at a 3, he thought the modeling was at around a 6 or 7 today and thought it could be around a 9 in the next five years. He noted a lot of interest in cyber modeling at the federal level, therefore there is energy focused in this area, which is good.
        i. Five years ago, they had two main events: the Wanna Cry and NotPetya incidents triggered by nation-state actors. His organization was able to use these limited incidences and apply techniques from actuarial predictive modeling without a lot of historic data. Since these events, there has been little relevant data.
        ii. He highlighted his work with the Department of Defense, as well as other federal entities that are on heighted defense for new techniques and tactics. Public discourse and needs enable private vendors to get more information into their models to assist government and industry partners. Continued investment and sharing of data are key to get to a 7-9 target in five years, as well as collaboration across a variety of different groups.
    b. Damani Mago started off by speaking in a historical context.
        i. Cyber cat modeling started eight to nine years ago and is in tandem with the insurance marketplace. When it began there was a need to understand how the models mature, as well as understand what that means.
        ii. Modelers came up with Armageddon scenarios of worst case, which could be subjective and not very data driven.

iii. Modelers in the last five years are thinking of the risk more holistically, where it does not happen the same way every time. The modeler must think about 'the breadth of the relevant cyber ecosystem, the threat actors, the vulnerabilities. How do they simulate? How do they think? There are many combinations, and it is complex.
iv. It must also be thought of as a human peril from a threat perspective as well as a defensive perspective. Modelers must consider what are the factors that drive a threat actor, and which ones contribute to systemic risk from a modeling standpoint.
v. She did not feel comfortable assigning a number score for where modeling is at today. She stated there is a good handle on the frequency side, but that severity is still being worked on. There is interest from not just the insurance industry but also capital markets and government agencies. Noted the insurance industry can't handle the systemic risk and many parties need to come to the table to solve for this.
vi. John Seo noted she stated the systemic side has come a long way, which is what the committee is most concerned about.
    1. She noted attritional activity and that there is good history as to it. So systemically she would say they are at a 7-8. In terms of perils the number would be 8-9, because they know it is malware and cloud outages are the most common, but how they do it is more in the 6-7 range. Cyber risk supported four catastrophe bonds last year, which is rare and shows the continued interest in the area.

c. Pascal Millaire thanked the group for the opportunity to participate in the panel. He agreed with the other two panelist that there has been great development over the last five years. He struggles to place a number on it and states it has progressed from interesting to useful.
    i. He noted that in Quarter 4 of 2023 billions of dollars in reinsurance transactions were undertaken based on the cat models being discussed. Furthermore, 7.5 percent of ILS issuance was based on cyber risk. This demonstrates that the models are good enough for the insurance companies and attracting other investment as well.
    ii. CyberCube raises around $150 million focused on cat cyber modeling and continues to invest in it every year.
    iii. The models' performance is easier to see on the attritional loss side today than five years ago, when they weren't tested. In 2021 CyberCube had an attritional loss model ratio of 61 percent, which was 4 percent off from NAIC's actual number of 65. In 2022, they projected a number at 44 percent, and the NAIC data showed that it was 43 percent.
    iv. It's harder to test the maturity of the cat models to project scenarios that have never happened before, with technologies being deployed for the first time. However, there are existing models that are

market-accepted both within and outside of insurance.

v. John Seo noted that in earlier days the models were dismissed, but now there are arm's length transactions where a serious amount of risk is being transferred based on the outputs of the models. Is there a lot of room for improvement?
    1. Pascal Millaire stated there is always room for improvement and the models will never be a 10. It's true of all models. as the technology landscape evolves, technology modeling tools will allow ecosystem stakeholders to understand single points failure in systematic ways.
    2. John Seo noted that the technology to conduct cyber attacks is growing, but so are the ways to counteract these attacks.

2. John Seo asked if the modelers can ever stay ahead of the curve to assess the ever-evolving risk?
    a. Doug Albert interjected that his prior work was on the offensive side working for the US intelligence community; the risk could be modeled as an infinite resource an infinite number of times. There is a good amount of information and tools not just cyber physics, but also network dependencies. These can be quantified and give solid recommendations to organizations going through digital transformations and can put up a good defense. The notion there will be forever an epidemic of say ransomware attackers is false. There are tools that can limit these attacks, although it will never be gone entirely.
    b. Damini Mago states that the defenders are evolving, like blocking a network with a lot of traffic so they can't work on the internet. If the attackers advance, so do the defenders where we have a lot of data to parameterize their size and motivations.
        i. For example, a student in the basement of his mother is not capable enough to launch that big systemic attack. Very simply put, it's either financial motivation or geopolitical. When we think about financial motivation, there are only so many ways you can earn money. You can steal the data and sell it, blackmail, or fool someone. There is that risk/reward from a threat actor perspective, and that's just one part of the equation.
        ii. There are software vulnerabilities, such as the Log4j last year. There is a cross-platform vulnerability because it may never happen the same way again. There needs to be a way to go about assessing different permutation combinations of things that could essentially go wrong: a supply chain attack or a worm simulation. There is a way to narrow down the possibilities to get to the problem and then we need to understand the impact.
    c. Pascal Millaire added that the history of the cyber insurance market over the course of the last ten year has had relatively a lack of volatility in loss ratios in the insurance market except for a ransomware spike between 2020 and 2021.
        i. CyberCube advises clients on profitable growth in the cyber

insurance space and compares volatility of losses to other lines of business. Cyber insurance really is not an outlier; rather, it is in the middle of the pack, and history has shown that it can be modeled effectively, and industry has done a pretty good job at consistent loss ratio performance.

ii. Ransomware was a discontinuity that changed cyber risk and the economics of cyber insurance and losses.

iii. The industry responded quicky in terms of adjusting pricing and underwriting. Insurers pointed out things like open RDP ports and multi-factor authentication that was the source of many of these claims. It is a dynamic risk, but it's a modellable risk. It's a risk that's been modeled well for over a decade in an industry that's shown its responsiveness to really be able to move the dial when those discontinuities happen.

3. John Seo asked - what information that you're not already getting would assist in helping you better understand the risk going forward?
   a. Pascal Millaire differentiated between exposure data and incident data.
      i. For exposure data the modelers are relatively well served, particularly with the technology tools that exist today for the insurance industry. 75 percent of all cyber insurance premium globally was run through the CyberCube model in 2023. They map hundreds of thousands and millions of companies to tens of thousands of technologies to which those companies are exposed. The great developments over the course of the last five years are the ability of tools to understand the single points of failure to which companies are exposed.
      ii. For incidents there is no entity in the cyber realm (like the National Oceanic and Atmospheric Administration (NOAA) that categorizes hurricanes) categorizing cyber events. Losses experienced in catastrophic aggregation scenarios, both the insurance industry and the public sector only see a small fraction because not all risks are insured and not all insurers pull their data, but progress is being made. There is of course a lag from the commencement of an incident to what is available to modelers, to insurers, and to the private sector.
      iii. For a potential federal response to catastrophic cyber events, it would be important to look at analogs such as the certification of acts of terrorism in TRIP and query whether there is a comparable analog needed for cyber cat events as this is further explored. He cautioned that in any such program, it would be very important to differentiate between day-to-day attritional losses that only impact one organization, for which there is legitimate concern about sharing that data, pooling it, or sharing it with a third party.
   b. Damini Mago agreed there are many ways to understand each company's technology. The missing piece of that equation is not knowing what they're

using it for.

i. You can have a bank, for example, which goes down on account of a cloud outage. It was down for a couple of hours, but most of their revenue is coming from mortgages. The attack doesn't affect the bank's mortgages or revenue generation. So even if you know how an entity gets impacted, you don't know what they're using that cloud service provider for. You might see that they use either Amazon or Azure.
ii. The more you go into the bigger revenue companies, they are using multi-cloud services in multiple regions. There are resiliencies built in.
iii. The first step in understanding what those technologies are. The next step is having a standardization to see which part of the technology your revenue depends upon. There are so many ways and so many technology providers who collect this information, but there is no standard way of saying what does it mean.
iv. Do they have backups and what does that mean? Do you backup your critical systems? How often do you backup? Is your backup in cloud or on Remote Infrastructure Management (RIM)? Is it away from the firewall? Have you tried restoring from a backup? Is it a good backup? There are so many layers to those questions that there is no standardization.
v. When compared to a fire following an earthquake, there's a sprinkler system. We know it's ISO certified. Everybody in this entire country – indeed, globally – knows what that means. We need that same standardization from a hygiene perspective on the cyber side of the fence as well.
vi. The second issue is on the incident data. We haven't necessarily seen cat events. There have been near misses, but not necessarily on systemic risk because there are great mitigation practices in place. There hasn't been one yet, which is not to say there's never going to be one.
vii. Event collection is necessary. The SEC recently came out with a rule requiring public companies to report when they have an incident. Private companies, especially the small-sized companies don't report incidents, especially if it never makes it to the news. That's the data that's lacking. A reporting requirement even for the small-sized companies is quite crucial for us to understand. If you see the size of the economy, at RMS we have a US economic database of about 38 million companies that have revenue of less than $1 million. Micro companies can get impacted if you have a systemic risk. That is a critical piece missing as well, from the data standpoint.

c. Doug Albert stated from inventory perspective he agrees but there are some nuances to add.

i. For the small businesses, the information exists. The mechanisms by which that information can be conveyed to the that demographic, or

to the knowledge of the vendors, is probably something that could be assisted with.

ii. In relation to the NOAA comment, they have been doing a large amount of work thinking about defense and mitigation requirements. CISA has been great in recent years. Combining that with this mission and figuring out how to put a little bit more of an economic basis, and there could be a significant amount of government assistance.

iii. For systemic risks, the argument is that the biggest sort of risk within cyber isn't necessarily solely a cyber or digital event. It's the fact that cyber pervades pretty much every and all industries. Even in our own national security reports, they note the increasing dependency of cyber and digital within our critical infrastructure and are finding ways to say we're not just interested in looking at purely technological factors.

iv. They are seeking to develop the collection of that technographical information. Cross-cyber and physical domain is an area that is the subject of Guidewire investment and focus. Finding ways for government to allow that information to be more available and to be collected will help. The case example is Colonial Pipeline. Thankfully there was a proper separation of the operational technologies associated with the actual deployment of product versus the IT system. The system going down still resulted in an actual interruption event. The interruption economic loss factor that probably could be analyzed a little bit more.

v. Facilitating information being shared such that, instead of just outside-in, an aggregate view can help apply methodologies to validated and accurate data to give you much more useful and accurate insights into that loss.

4. A question from member Derek Blum: Pascal Millaire spoke about exposure data and its importance. When looking at terrorism risk or Nat Cat, it's important to think about the accuracy or uncertainty and the utility of that data. If there was, say, a nuclear attack, it wouldn't really matter that much. A lot of the attributes we capture on, for example property information for terrorism, we do try to capture information for those kinds of models about the structure itself. When we talk about this kind of technographic information, it's changing a lot more rapidly. How accurate is it to begin with? Is it providing a false sense of security by knowing that if it's not even necessarily that relevant for some of the catastrophic cyber attacks?
    a. Pascal Millaire responded with reference to when catastrophic cyber attacks happen. They happen against a single point of failure, a technology, a technology company. The starting point would be to ask: what are those technologies that are sources of catastrophic cyber aggregation?
        i. Over the course of the last eight years of building CyberCube models, they have amassed a catalog of 45,000 different companies, technologies, technology vendors, and versions against which an attack malware outage could lead to an aggregation accumulation

event.

ii. Exposure data isn't enough. Time is needed to understand if it is accurate and reflected in the actual underlying technology dependencies. They cross reference our brokerage applications from the majority of the world's top 20 brokers, with the market share of the various providers to make sure what they are seeing in the data is reflective.

iii. There are two things then: decide when that bottom-up analysis is sufficient to be included in a model that's going to price catastrophic cyber risk, and where more market share-based approaches are needed because that data isn't reliable.

iv. It is fast moving, but the technology dependencies can be observed with internet-scale data collection infrastructure that observes the different relationships happening between servers. It will be a never-ending task as the technology landscape evolves.

v. For the insurance industry and public sector modeling, there is a focus on that incident data and the accumulation of incident data because all models are trained against that data. He did not believe there is a sufficiently comprehensive data set out there today for accumulation events to train models against.

b. Damini Mago stated RMS takes a 50,000-foot view at how they approach the issue, rather than look at individual companies. They look at companies in the thousands, and don't get specific because details get lost. Modeling vendors need to reduce the uncertainty.

i. They look at industry revenue that is country specific, and how revenue is generated. Threat actors are a large part of that equation because they focus on a certain type of company like healthcare or IT services.

ii. RMS collects data as to what are the typical sectors that will potentially be attacked and what technologies are being used. A big company is probably spending resources training employees because they are a point of entry. They invest in cyber security measure.

iii. For exposures RMS looks from a size sector jurisdiction because the more precise it is accuracy is lost and uncertainty increases.

iv. On the risk side they take the software family approach, how many there are then create a scenario for each one. There are billions of different scenarios that could be developed. They are precise but not useful in understanding what is an accurate systemic risk. New software has new vulnerabilities emerging every day.

v. The day-to-day approach to handle the problem is gathering information, managing it, and mitigating it. From a systemic risk potential, you must be able to abstract it so you can think about the possible combinations that could happen to assess what the risk might look like.

c. John Seo noted Pascal and Damini have different approaches, which is question 3.

5. Keith Bell interjected that it seems the weakness now is incident data, and there is more exposure than incident data. Is there an estimate of the number of unreported incidents that could cause a lack of robust modeling going forward?
    a. Damini Mago stated RMS captures their own incident data, across all the different cyber perils like data breach, ransomware, and malware. They have 150,000 data breach incidents across the board, which is a global exposure database. She noted this is the same with ransomware, and with cloud outages: when it happened and what happened.
        i. They calculate using historical data which is relevant for attrition and under-reporting. There has been a lot of work with industry to figure out how much may be underreported. This is extremely important for small-sized firms because the focus of the available data is on large companies. Large companies report because they must show it in their fillings, which skews the numbers for the smaller companies. They use a variable in their model to capture that information based on the work the industry is doing.
    b. Keith Bell followed up on the observation that smaller and medium-sized companies don't report, noting that if attacks and means of attacks are evolving over time, they are not being picked up and they could be missed by the models.
        i. Damini Mago answered that issue is quickly changing because even smaller companies that have had a small cyber incident are making headlines. Multiple companies may go down at the same time, which will bring attention.
            1. If there is a mandate to go get incident response from those insurance companies, we will start seeing companies come forward because there will be a regulatory action.
        ii. Pascal Millaire interjected that there could be a positive to this, that insurance companies already have a tremendous amount of attritional loss data.
            1. Insurance analytics and modeling are tying those specific claims down to security indicators and the industry is clamping down: for example, open RDP (Remote Desktop Protocol) ports leads to losses, and there is a 7x increase in losses arising from that vector.
            2. CyberCube models things like end-of-life products that leads to an 11x increases in losses. Certain ransomware tool kits had a 20x increase in losses.
            3. There is a need for more incident data and better cyber security practices which the insurance industry is doing, and it is an important part of the Cybersecurity Insurance and Data Analysis Working Group (CIDAWG) initiative because it is driving better cyber security protocols.
            4. Underreporting is important when asking big societal questions around cyber risk and where losses are not being insured. If there is going to be a federal response to

catastrophic cyber events, both insured and non-insured risk need be considered in some sort of reporting mechanism.

5. The insurance industry deserves credit for evaluating existing claims experience which drives advancements in understanding what good cyber security is and isn't as far as frequency and severity for attritional modeling.

iii. Damini Mago noted that the CyberAcuView initiative is comprised of the biggest primary insurers who are making an effort in terms of collecting claims data; to an extent they are trying to regulate the kind of information needed.

1. Cyber is not standardized whether you look at insurance policies or even as modeling vendors. There is an effort by the industry to create a standard as to how you collect claims information. Sometimes there is death by data, so there is a need to explore the right kind of data. These initiatives help move the needle.

iv. Doug Albert stated he agreed with the rest of the panelists and wanted to provide a larger perspective. Within the system of insurance and that target space the modelers have on insurance, there is visibility with that data. An interesting aspect is the analysis of critical infrastructure and generally the evolution of the economy and every business that has some degree of a cyber component.

1. Small businesses, such as a hot dog stand or donut shop, perhaps don't know they need cyber insurance, are not familiar with it, and maybe are not getting their needs served. They are the most likely to get completely wiped out in some sort of systemic event. There is an interesting partnership opportunity to insure these entities and make sure we are not losing anything within this sphere. Most startup businesses likely are not thinking of the need for cyber insurance when they are beginning or are familiar with it.
2. From a federal perspective or a local government perspective, some type of public-private partnership is in the best interest. From an economic perspective, it is bad. But from a human cost of individuals starting businesses who are getting wiped out by an apex predator and they have no reasonable chance of defending themselves, it would feel like a tragedy.
3. Getting information on small business is something we can arguably facilitate and try to understand. Can there be forums that can provide education and information that allows us to build better models and understand the totality of the loss?

c. Derek Blum stated we have shifted to the insurance side of the issue from the data aspect and there is also the policy information, where the insurance industry practices are shifting. There are not a lot of standards, and if we think about quantifying the risk it is critical that models account for insurance policy terms and conditions. I am curious how the different

models handle that. How can you keep up with the pace of changing standards and practices of these terms and conditions?

i. Pascal Millaire agreed that is a critical point. As a modeling firm we are tasked with modeling the industry's losses but also particularly the losses of a particular carrier and their policy language.
    1. CyberCube from the very beginning runs their model on the terms and conditions by policyholder. In 2023, they made a fundamental change with Version 5 release of their portfolio manager model to reflect the cat risk is being dealt with differently by different market participants.
    2. The introduction of war exclusions, widespread event exclusions, cyber policies were covering very different things and there were big differences between what was covered – for example, in the Lloyd's marketplace versus what was being covered by many insurers here in the United States.
    3. CyberCube responded by creating a new widespread event modeling feature which looked at different languages and showed what the impact was on the 1-in-200-year losses. A paper was published in 2023 showing, depending on language, the 1-in-200 loss was in some cases down by as little as 9 percent, but in other cases it was down as much as 60 percent.
    4. When we think about the future of modeling, we think about how we are going to provide an accurate view of the tail loss events associated. This looks different by carrier and by policy language, and the policy's response to extreme events. CyberCube made fundamental changes to their model to capture the differences, which have an impact on cat average annual losses, but also when looking at 1-in-200-year tails – whether the widespread events are covered or not.

ii. Damini Mago stated the flow of data is not uniform across the board.
    1. When the modelers start to see the primaries are getting detailed data, even some of them don't get all the revenue information which is critical because that defines how much Business Interruption coverage one will have, and that is a key driver in the tail.
    2. It starts to get unsteady with the lack of data on the primary side, but as it goes higher up in the value chain to reinsurers and to capital investors, you get less and less of that information.
    3. The RMS model allows the ability to import the detail exposure but also the aggregate exposure. They have the U.S. industry database that helps disaggregate the information and give you a good proxy of what your detailed exposure might look like. There are a lot of practices happening in the industry to increase the quality of the data. They can also

enrich the data because when one thinks of who is getting attacked, it is a company and their particular attributes. They enrich the information based on those attributes. They are doing work on data whether it is detailed data or aggregated.

4. Coverages are a bit tricky with cyber but getting better. There is no standardization in terms of the coverages that are offered within the market; there is not even a standard template. Five years ago, there was a lot of disparate coverages, but now they have a relative sense on what is being covered.
5. There are incident response costs, breach of privacy, financial fraud if it is a crime policy, as examples.
6. RMS models 16 different coverages because they know there is some flexibility that the clients need to get the information and model it accurately. They also parameterized at that level of granularity on the exposure side.
7. War exclusions are becoming more and more prevalent and common in the marketplace. Lloyd's has a mandate to have war exclusion in place and many carriers have a different variation. War exclusions have never been tested in court, so there remains subjectivity in terms of the actual scope of coverage.
8. RMS says events have a label: 'State-sponsored threat actors' are part in this kind of an event. One can exclude the events that are state-sponsored triggered, and instead say it is an economic loss of say $30 billion, $40 billion, or $100 billion. If it is that big of a loss triggered by state-sponsored event, the company can start to see the sensitivity to where to apply war exclusion, as well as model what it may look like. The RMS model provides sensitivity tools for clients to test different terms and conditions across the board, given the subjectivity that may attend judicial review of these provisions...

iii. Doug Albert provided that Guidewire-Cyence approaches it similarly with a bottom-up simulation for these types of events.

1. For aggregate events, they are still looking at the characteristics of individual companies. It is important for them in terms of ability to generate pure economic loss; they then apply the insurance policy structure on top of that.
2. They flag similar things around state-sponsored attacks. There are in line with the market behavior at that time, but usually in partnership within our teams.
3. If a company has a specific circumstance, they give a very detailed raw output that the company can adjust to accordingly. They provide a product that is in line with market expectations and trends. With granular output, it provides the ability to make arbitrary adjustments as well as potentially counter-factuals and simulations to see what types

of things could occur.

4. It is fundamentally like RMS, by providing a lot of important data, but ultimately part of a larger business process where there are many participants and a company can adjust to their needs accordingly.

Chairman Seo thanked the panelists for providing their distinct voices for their companies.

AM Best Presentation

Chairman Seo commenced the AM Best presentation by introducing Stefan Holzberger, its Chief Rating Officer, and Michael Lagomarsino, the Senior Director of Property and Casualty Commercial Lines at AM Best.

1. Stefan Holzberger began with familiarizing the audience with AM Best, a specialist credit rating agency. AM Best rates the financial strength, claims paying ability, and credit quality of insurance organization in 100 countries. He thanked FIO and ACRSM for providing the opportunity to share their thoughts.
    a. A brief introduction to AM Best's rating methodology process was first in the presentation, which then moved to cyber risk and its different components.
        i. The foundation of the rating process is an ongoing dialog with the rated company's management team.
        ii. He noted it was important to understand that the rating analysis is both qualitative and quantitative, and involves regular, intimate interaction with the company. The ratings are meant to be forward-looking.
        iii. Considering all the uncertainties insurance companies are faced with, and not knowing liabilities until months or years later, they are trying to identify potential future events that could damage the organizations' earning or balance sheet strength.
        iv. The AM Best rating methodology is done in a building block approach. There are four blocks:
            1. Balance sheet strength, from a credit standpoint, comes down to available capital and the aspects of required capital. The risk that the insurance organization has decided to undertake. This forms the baseline of the rating methodology.
                a. Once the balance sheet strength assessment is concluded, they may arrive at a BBB, or BBB+, or A- as a starting point for their rating. They then will either increase, decrease or leave the baseline assessment alone.
            2. The operating performance are for earning and profitability of the insurance organization. This speaks to the competitive market advantages and disadvantages of the organization.

    a. What is the organization's product profile, the regulatory environment in the markets it operates.
3. The Business Profile is the regulatory environment in the market in which the business operates. The Business Profile along with Operating Performance are leading indicators of future balance sheet strength and provide a long-term perspective of the organization's credit quality.
4. Enterprise risk management is critical.
    a. The insurance industry underwrites contracts; they are also institutional investors and take on investment risk. There are also reinsurance counterparties that have credit risk, and operational risk. There is a lot of uncertainty around those aspects of business.
    b. AM Bests expects insurance organizations through risk management capabilities to actively and formally seek to identify emerging risks. There is also an expectation they underwrite the business they retain on a net basis within their risk appetite and tolerance in the markets they are competing in. They also expect the risk management capability to successfully manage those risks which they choose to underwrite.
    c. Enterprise risk management stress testing is very important. Critically important tools, like we heard about from the modeling organizations, helps test those capabilities.
    d. If an aspect of a company is not fully captured, there is rating enhancement or drag rating, which means that an insurance entity could be part of a stronger or weaker overall group that could benefit from the strength of the parent company, and its financial flexibility.
        i. An example would be an insurance company within the Berkshire Hathaway organization that could get a rating enhancement because of the parent organization, which is a piece of the issuer credit rating and overall credit worthiness of the organization.
5. Cyber risk ties into many aspects of AM Best's building block analysis. It is critical to shock loss and cat cyber can impair the balance sheet. As stewards of the company, we want to know what management is doing to quantify that risk exposure to their balance sheet.
    a. Attritional loss versus cat loss if there is a historical experience for an organization underwriting cyber, then it is not necessarily indicative of the potential kind of severity one may see down the road.

Therefore, stress testing is very important.

i. They are seeing extensive use of quota share reinsurance. Companies move cautiously in terms of how much risk they retain on a net basis through extensive use of reinsurance. This is common regarding cyber exposure.
ii. As far as operating performance, they look at the profitability of a cyber book of business, its accretive to earnings, or potential to be a loss leader, and will that change over time.
iii. They look at whether the business profile or product concentration risk is dedicated to cyber and is it a well-diversified book of business or monoline. Diversification is considered to be a feature of successful underwriting, and AM Best recognizes that being monoline in a high-risk product like cyber is challenging from a concentration standpoint.
iv. The policy limits being offered have an impact. How high are the limits in relation to the capital and surplus of the organization, as well as the financial flexibility of that organization. They consider if the cyber portfolio is concentrated in a particular industry or spread across various industries and geographies.
v. For enterprise risk management they look at risk aggregation, which is important to stress testing. They consider the downside scenario and what a bad year my look like from an operating performance and balance sheet strength perspective.

2. Mike Lagomarsino then took over the presentation to speak about why incorporating cat risk and stress testing is necessary. Managing exposure to cat events is essential to protecting and preserving balance sheet strength. A number of risks can cause companies to go insolvent, whether natural or manmade.
    a. For example, the Florida property market in the last couple of years has had significant insolvencies as a result of natural catastrophes.
    b. Stress testing allows AM Best to capture the uncertainties inherent in an insurer's operations and business plans.
    c. AM Best follows a diverse group of companies and perils that may be exposed, whether natural, terrorism, casualty clash or cyber.
    d. Their proprietary capital model is Best's Capital Adequacy Ratio (BCAR), which is a comprehensive tool that evaluates many risks to an insurers balance sheet simultaneously. It generates and overall estimate of the

required capital needed to support those risks and it compares a company's required capital against the available to come up with a BCAR score across different confidence intervals and return periods.

e. The model incorporates a catastrophe risk charge for capital calculation, incorporates it into the capital model, and assess the catastrophe risk management capabilities. The data is provided by the companies, for each of its largest perils.
f. He noted cat models are useful for analytics but cannot be sued solely for the management of maximum exposure. They also must monitor aggregate exposures, including what-if deterministic scenarios using hypothetical severe events in areas of concentrated exposures or overlaying historical events on current portfolios.
g. When the data is collected, they calculate a catastrophe charge for each of the perils that a company may be exposed to and build in a charge using the larger of natural or manmade catastrophes.
h. They also conduct a cat-related stress test to quantify the impact a stress scenario can have on company's finances. The stress test applies a second event very often, with an overlay. This usually creates a straight reduction to equity or available capital and increases to recoverable and loss reserves. The AM Best analyst is most interested in seeing how far the BCAR score drops as a result of a severe event.
i. For companies that do not have the financial wherewithal to fill that gap, it could cause a negative rating action on their balance sheet.

3. Mike Lagomarsino then moved to terrorism.
    a. US companies with exposure to terrorism, have the federal TRIP backstop which was extended in 2019 to 2027. It reduces AM Best's concerns about the US government's long-term commitment to a federal role. Therefore, the catastrophe charge in the BCAR reflects credit for both their-party reinsurance and TRIP protection when a terrorism Probable Maximum Loss (PML) is large.
    b. They have what is called a terror stress test, designed to quantify the impact that a large insured terrorism loss could have on a primary insurer's capital if TRIP was not available. It is not permanent since there is an expiration date involved. It is a temporary reduction in the cat charge. For concentrated companies in high-risk cities, AM best has less tolerance between the TRIP applicable and non-applicable stress tests.
    c. They are concerned as the expiration of TRIP approaches, to such a degree they have asked companies for corrective actions they may take to remove those concentrations of exposure in their book of business. These discussions generally begin 18 to 24 months prior to the expiration since most policies are written for a one-year term. If underwriting actions need taken, the company will need more than one year to communicate to AM Best how they will reduce exposure.
    d. John Seo asked a question: TRIP has not been triggered, but you go through these renewal actions. Your model has a material impact for certain companies, is that correct? Is that what is being said?

i. Mr. Logomarsino stated that is true and, in those instances, as they approach TRIP reauthorization, AM Best asks for an underwriting plan or plan of action to include facultative reinsurance, for example. They feel comfortable with the plans the companies have provide that have material exposure with terrorism.
ii. John Seo followed up with a hypothetical, if the program were not renewed, one would expect there would be a significant impact on the industry itself. There would be a significant reaction.
iii. Mr. Logomarsino affirmed.

4. Mr. Lagomarsino continued to provide a brief overview of the AM Best questionnaire. He noted it was a new rating tool meant to collect detailed information on a company's affirmative underwriting operations.
    a. It is important due to the growth in the line and lack of transparency around affirmative cyber within financial statements, including US statutory statements. There is currently not a stand-alone line for cyber, it is comingled with a lot of other statutory statements.
    b. The data in the questionnaire is structured around the AM Best building blocks. They gather data to assess the nature of a company's affirmative portfolio.
    c. They assess the risk appetite and underwriting strategy, look at the reinsurance utilized (traditional and non-traditional). They also look at third parity MGAs, MGUs for underwriting, or TPAs from the claims perspective.
    d. They ask questions on types of coverage offered: First party, third party, package or stand-alone. They also ask for limit and retention levels.
        1. They ask for types of insureds and geographies, and approach this from size of insureds across the spectrum.
        2. As far as performance they ask for loss ratio information, number of claims paid versus reported.
        3. From a balance sheet perspective, they request information on PMLs, third-party vendor models, internal models, and deterministic scenarios they are running.
    e. This information is used to come up with a cyber catastrophe charge that is built into the capital model. They will also apply that to stress testing.
    f. They are rolling the questionnaire out to 60 affirmative writers globally throughout 2024 at the time of their annual management meeting. He then turned it back to Stefan Holzberger.
    g. Stefan Holzberger made a comment on the questionnaire that they are also in the learning process when it comes to cyber exposures and understanding the peril. They anticipate questionnaire to give rich data where they can start to understand a standardization trend around this line of business, as well as insights for benchmarking and peer comparisons.
        i. They are optimistic cyber will be part of this to a degree and understand how insurance organizations are managing it.
        ii. It will also help them understand who the outliers are and ask why they are taking on more risk or looking at risk differently than their peers.

h. John Seo interjected FIO is likely envious if they can put out a questionnaire like this but imagines this is a voluntary response by the insurance companies. Does AM Best get a high response rate?
    i. Stefan Holzberger stated they do. He believes the groups understand that they are not just making the request because we don't have enough to do, and we don't think they have enough to do. It is material for the analysis, and it is growing. They are hoping for 100 percent compliance.
        1. When the information is not received, they take a view of the risk that is probably more onerous than it would be if the companies provided the details.
        2. The companies they follow look very closely at how AM Best evaluates their risk-adjusted capital, and if the companies put in a little bit of work, they know it may improve their score. So, they are generally happy to do so.
            a. Mike Lagomarsino stated that this information should already be captured by the companies if they are writing affirmative cyber. It should be something they are capturing to analyze for their own portfolios.

i. Derek Blum asked if the questionnaire is stand-alone, and if AM Best envisions that it will be rolled into the SRQ and cyber section. He also had a follow-up question around collaboration with modeling firms around 9/11 to help craft sets of questions. He asked if they engaged with modelers that were on the panel about if the right kinds of questions were in the form. Has there been direct engagement and, if not, do they plan for there to be?
    i. Mike Lagomarsino stated there had been engagement with leading modelers as well as brokers, distributors, and advisors. They did not take all suggestions, but there was a significant buy-in as far as their input.
    ii. Stefan Holzberger said whether it becomes a standard component to the supplemental rating questionnaire has not been decided yet.

j. Matt McCabe asked how the companies get feedback from the evaluations. Do they get peer evaluation, or do they get a benchmarking against their peers? Do they get feedback or is it just an overall rating? How is it communicated?
    i. Mike Lagomarsino noted he would not call it an overall rating since they are not just looking at their affirmative cyber. It is usually a portion of a much bigger part of what they write.
        1. AM Best does not necessarily have benchmarking at this point for affirmative cyber. It is how the companies are managing cyber, and how they are entering the market and writing it. It is not scoring their affirmative cyber performance. It is part of a much bigger piece of overall underwriting.
    ii. Stefan Holzberger stated a lot of consultancies have put out surveys, and one of the incentives is that respondents have access to the data.

They can see the output, albeit on a consolidated, no-name basis. AM Best does not plan on giving clients that specific kind of feedback, but they will be transparent to the market. They will report anonymized data.

1. Specific insurance groups will get information back on how their cyber exposure fits into their ERM, and how it stacks up to other risks which influences their ultimate rating assignment. A well-run organization that is writing cyber profitably, managing exposures and severity could be credit positive. That is the feedback they would provide.

5. Stefan Holzberger continued with the presentation by talking about day-to-day blocking and tackling as far as how companies manage cyber risk. Companies are managing the exposure predominantly through underwriting actions as well as risk transfer. He noted policy wording is critical, and it is not unusual for organizations to move cautiously with a new line of business.
    a. They will exclude aspects of the risk exposure if they feel they cannot price and underwrite it effectively. An example would be war exclusions.
    b. Organizations are looking carefully at the coverage terms and conditions. A lot of the contract wording really hasn't been proven in court and there is not strong precedent upholding such policy language. The companies are scrubbing the wording very carefully to try to avoid unintended consequences and look for areas where cyber may be unintentionally covered for no premium.
    c. Vendor tools are utilized to assess the aggregation of risk, whether through probabilistic, deterministic, realistic disaster scenarios, or simply total insured value for that segment of their underwriting portfolio.
    d. As more loss experience comes through, more comfort and confidence on that line of business grows. There would be an expectation for risk transfer through quota shares.
    e. AM Best has relationships with monoline cyber writers and they are unique, heavy into technology.
        i. These companies use real-time exposure monitoring, they patch into policyholder systems and look for vulnerabilities. They are reaching out to their policyholders where they see the potential for a security breach.
        ii. If a policyholder doesn't want the policy canceled, they have a limited time to address the security risk and put a patch in.
        iii. AM Best sees it as a beneficial relationship. Not just indemnifying but working to mitigate the loss.
    f. Cyber models continue to mature and advance. Modeling capability used for underwriting and pricing, adding a cat load on a policy-by-policy basis is where the market needs to get to, as well as the ongoing increased confidence in data quality and output of models.
6. Mike Lagomarsino highlighted the perspectives of potential benefits and challenges from a government backstop, primarily from a benefit perspective.
        i. It would be a backstop that would avoid a lengthy economic

downturn and financial market volatility.
   ii. It would promote improved cyber hygiene and enhanced risk management capabilities.
   iii. It would enhance the resilience of the companies in terms of trying to avoid a moral hazard risk perspective.
   iv. It would lead to greater take-up rates for cyber coverage while attracting reinsurance capacity, especially if it was permanent.
   v. It is important not to crowd out the private market and allow for it to grow and insure the risk.

7. Derek Blum asked if AM Best could comment (noting the slide presentation) on why a federal backstop both has the risk of reducing cyber hygiene but also could improve it.
   a. Mike Lagomarsino stated they are trying to convey that the backstop, if structured properly, would promote improved cyber hygiene. He cautioned that if it was not structured properly, it could induce moral hazard risk where the companies become laissez faire knowing the government will step in, and therefore do not invest in their systems. There are potential benefits and pitfalls, and all parties need to have responsibility.
8. Richard Ifft asked if either could see cyber as they do terrorism coverage, where a company is taking on too much risk or there's things they could do to avoid a lower rating from AM Best, even though there is no cyber backstop at this point.
   a. Stefan Holzberger stated he could see that within the enterprise risk management framework, they are trying to understand what the risk tolerance of the organization is and what is their capacity to manage it. There are finite assets and resources, they choose to underwrite and retain.
      i. Once AM Best can benchmark some of the relationships around exposures and capital, they will start to identify the outliers. They then can have a pointed discussion with the companies to discuss if there is something inherently wrong with their portfolio and having an informed conversation.
   b. Mike Lagomarsino thought building cyber towards terrorism and natural catastrophes, there is a comfort around data capture and how we use that in the rating process.

Chairman Seo thanked the presenters for their informed presentations and expressed his excitement about the questionnaire. He then introduced Jeremy Pam, of the Federal Insurance Office, to update the group on FIO's evaluation of a potential federal insurance response to catastrophic cyber loss for critical infrastructure, and the potential implications for TRIP.

Federal Insurance Office Presentation

1. Jeremy Pam started by providing the group with an update since the July 2023 ACRSM meeting where FIO provided a briefing on the joint assessment of a federal

insurance response to catastrophic cyber incidents that FIO and the Cybersecurity and Infrastructure Security Agency (CISA), launched in June 2022.

a. He provided background on how FIO has monitored the development of the cyber insurance market since FIO's 2014 Annual Report. TRIP has monitored these developments since 2016 because cyber insurance may be written within TRIP-eligible lines and TRIP could apply to a cyber attack if it is certified as an act of terrorism, as defined in TRIA.
b. Following cyber attacks beginning in 2017 such as WannaCry and NotPetya and increase awareness of society's dependance on cyber connectivity during the pandemic and increasing concern about the cyber vulnerabilities of critical infrastructure, such as the Colonial Pipeline incident.
    i. FIO began to focus on the adequacy of insurance for catastrophic cyber risks specifically as distinct from attritional cyber incidents that constitute most of what is seen in cyber incidents such as ransomware, even large attritional cyber incidents.
c. The 2019 TRIP Reauthorization Act instructed the Government Accountability Office (GAO) to produce a report on cyber terrorism that would address overall vulnerabilities and potential costs of cyber attacks to critical infrastructure and the adequacy of TRIP to cover systemic cyber incidents.
d. In June 2022, GAO released the report *Cyber Insurance Action Needed to Assess Potential Federal Response to Catastrophic Attacks*. The report found that TRIP is limited in its ability to cover catastrophic cyber incidents that are not cyber terrorist attacks.
    i. The report recommended that FIO and CISA conduct a joint assessment of whether a federal insurance response to catastrophic cyber incidents more generally is warranted. FIO and CISA accepted the recommendation and began the assessment.
e. FIO briefed the ACRSM on the RFI that we published in the Federal Register in September 2022 and President Biden's March 2023 National Cyber Security Strategy, which committed the administration to assessing the need for and possible structures of a federal insurance response to catastrophic cyber events that would support the existing cyber insurance market.
    i. The July 2023 implementation plan for the National Cybersecurity Strategy, charged FIO with responsibility in coordination with CISA and ONCD for the initial phase of the assessment, assessing the need for a federal insurance response to catastrophic cyber events to be completed by the end of calendar year 2023.
    ii. FIO conducted extensive engagement on the subject with primary insurers, reinsurers, brokers, representatives of critical infrastructure, policyholders, and other stakeholders.
f. In November 2023, FIO co-sponsored a half-day conference in New York with NYU's Volatility and Risk Institute on Catastrophic Cyber Risk and a potential federal insurance response that featured panels with senior insurance industry executives, senior cyber insurance experts, and cyber

insurance policyholder representatives, and keynote remarks from senior officials of Treasury, CISA, and the Office of the National Cyber Director (ONCD).

i. Many ACRSM members attended and there was a keynote from the Deputy Director of CISA.
ii. The first panel of C suite panelists included the CEO of March McLennan, the former CEO of AXIS Capital, President and CEO of Chubb, the President and CEO of Marsh, and the Group COO of Everest.
iii. The second panel featured cyber insurance experts including Pascal Millaire, CEO, CyberCube, who you've heard from earlier, the head of cyber from AIG, cyber counsel from HSB/Munich Re, the director of cyber from the Geneva Association, and the head of cyber underwriting from Beasley.
iv. There were remarks from the Deputy National Cyber Director from ONCD.
v. The third panel had cyber insurance policy representatives including the global cyber leader from Aon, the chair of the Digital Committee from the Federation of European Risk Management Associations (FERMA), the treasurer of RIMS, the President and CEO of the Associated Electric Gas Insurance Services, and the head of business of risk and insurance of Google Cloud.
vi. The Conference concluded with a keynote from Treasury Assistant Secretary Graham Steele, who noted, among other things, that "a well-designed federal insurance response could address the risks of tail events while incentivizing healthy private sector practices. Conversely, a poorly designed program could shift too much risk to the government and reduce firms' incentives to guard against certain forms of low probability, but nonetheless foreseeable risks."

g. FIO has now completed the initial phase of its work on the assessment of a potential federal insurance response to catastrophic cyber incidents, finding that further exploration of the appropriate form of a federal insurance response is warranted.
    i. FIO has notified GAO of the completion of the initial phase of its assessment.
    ii. GAO has responded that they are pleased about Treasury's continued commitment to assessing this very important issue and engagement with government and industry stakeholders.
h. FIO's completion of Phase 1 of its assessment has also been accepted as completing the relevant initiative of the National Cybersecurity Strategy and Implementation Plan, noted earlier.
i. FIO will now undertake the exploration of the appropriate form of a federal insurance response in Phase 2 of the assessment, in coordination with CISA and ONCD. FIO has already taken steps on this next phase of the assessment.
j. At the November conference, Assistant Secretary Steele announced that

Treasury will host a second conference on catastrophic cyber insurance shortly after the IFTRIP Conference, discussed earlier, coming up this April.

i. The upcoming conference, which we expect to take place in early May, will extend FIO's engagement on the topics discussed in November to begin consideration of the potential forms that a federal insurance response to catastrophic cyber risk might take.

k. FIO will continue to work with CISA, ONCD, and other stakeholders in the next phase of the joint assessment of a federal insurance response to catastrophic cyber incidents.

2. Derek Blum asked if FIO is looking seriously at this for us to get to the point of having a backstop for cyber. It's got to go through congressional approval and all that. Is there current engagement or is there anything pulling from the congressional side? Or is it mostly being pushed through FIO at this point?
    a. Jeremy Pam responded that the initiative started with a GAO report that was mandated in 2019 in the TRIP reauthorization, there has been dialogue with Congress, FIO and CISA throughout the process. He also noted they have been keeping GAO, and through GAO, Congress abreast of the process as we go along. If it matures further, that engagement will deepen.
3. Tom Srail stated there was near universal support for some sort of federal response. Are there any plans to engage the participants in that at all? Any further intent to gather more input, like the open comment period a year-and-a-half ago?
    a. Jeremy Pam responded that it is something that has begun and will continue going forward. He noted that Assistant Secretary Steele said Treasury would use the next conference to help structure our engagement. FIO has begun to start scheduling calls with participants.

Chairman Seo thanked Jeremy for his update.

Closing

Chairmen Seo then went on to speak to some organizational housekeeping issues and asked the group if end of July worked for the Committee's next meeting.

1. He asked for any objections.
2. No objections were heard.
3. He then asked for any developing issues the group would like to address, to introduce for the next ACRSM event.
    a. Chairman Seo noted he would like to mention a subject that was spurred by the AM Best presentation, which was TRIP reauthorization. He noted it there is generally a 24-month lag to react to a non-renewal in the industry.
        i. He thought it would be interesting to at least talk about renewal, because that is the job of the Committee.
            1. If the Program will not be renewed, there should be a mechanism that gives an adequate notice instead of a last-minute dramatic renewal.
            2. There is no intent to take away from the ability of Congress,

rather a heads-up if they are not going to do a renewal, so there is something in place in time.

3. The timing issue may seem minor, but it is important for insurers.

b. Richard Ifft responded that he thought it was interesting since they are three years out of expirations, almost 4 years.
    i. He noted a lot of disruption in late 2014 and early 2015 when the program literally lapsed for nine days. That was not good.
    ii. In 2019 the Program was reauthorized, without changes, almost a year in advance of its expiration, which was smooth. There were no market disruptions.
    iii. Treasury does not drive issues respecting Program reauthorization; however, we could put the issue of reauthorization on the ACRSM agenda in July for further discussion.
c. Chairman Seo stated if it is renewed in 2027 a reform could be a mechanism that explicitly requires Congress to decide to renew or non-renew in advance of the actual sun-setting.
d. Richard Ifft noted the last time TRIA was renewed it was not modified, and it was his understanding that was the consensus because it could be renewed much more quickly.
    i. Modifications require much more discussion and evaluation, and more significant engagement in Congress and with stakeholders.
    ii. The issue of Program reauthorization and where that stands in terms of the current lifecycle of the Program makes sense to us as an issue for the Committee's consideration in July.
e. Matt McCabe suggested that the Modeling Panel discussion reflected the number one thing lacking is incident response data. However, there was also the allusion to death by data, such that the data you receive is perhaps not as valuable as targeted data.
    i. He suggested one of the things that should come out of this Committee would be how to prioritize that data.
    ii. Naming the top incident response data that could be anonymized form incidents that would be more valuable. A good goal for the Committee to pursue.

Chairman Seo asked for any more input. Hearing none he adjourned the meeting.

Adjourn

I hereby certify these minutes of the February 1, 2024 Advisory Committee on Risk-Sharing Mechanisms public meeting are true and correct to the best of my knowledge.

John Seo
Chair, ACRSM