November 14, 2022

Federal Insurance Office
Attention: Mr. Richardt Lift
Room 1410 MT
Department of the Treasury
1500 Pennsylvania Avenue NW
Washington, DC 20220

RE: Comment Letter on Potential Federal Insurance Response to Catastrophic Cyber Incidents

Dear Mr. Lift:

The Risk and Insurance Management Society ("RIMS") submits this letter in response to the request for public comments by the Federal Insurance Office ("FIO") on the "Potential Federal Insurance Response to Catastrophic Cyber Incidents," as published in the Federal Register on September 29, 2022 at 87 FR 59161 *et seq*.

Founded in 1950, RIMS supports more than 200,000 risk practitioners and business leaders from over 75 countries through networking, professional development, certification, advocacy, and research. RIMS publishes the award-winning Risk Management Magazine and produces RISKWORLD®, the largest annual gathering of global risk professionals. RIMS's members are in businesses in all critical infrastructure systems, plus ordinary retail and services. A crucial part of risk management is the continuity of business operations through risk management techniques to avoid, reduce, and plan for causes of loss that impair business operations, and then to restore the business to normal operations as quickly as possible, including risks to facilities, supplies, human resources, supply and distribution chains, and the functional systems within those such as information systems and financial management. RIMS and its members have a strong interest in addressing catastrophic cyber incidents affecting critical infrastructure because of the direct and indirect effects on member businesses. RIMS' comments convey the views of RIMS' members, who are risk managers responsible for managing their organizations' risks and procuring insurance, where appropriate, to offset those risks.

Executive Summary

RIMS' members responding to a recent member survey overwhelmingly support a federal cyber insurance backstop. Although numerous types of cyber incidents could catastrophically impact critical infrastructure, the FIO should consider the scope of the new federal backstop: should it be limited to critical infrastructure, or should the new program be available to all organizations in light of the cascading impact of failure of critical infrastructure

of the economy? We think this distinction needs to be addressed as a core question before the extent and method of coverage can be addressed.

RIMS supports consideration of a broader federal backstop because RIMS members report that the private insurance market is not making available insurance for catastrophic cyber incidents at the desired level. Member organizations purchase significant cyber insurance limits but would purchase more limits if available for a reasonable premium. Even when available, war exclusions in cyber insurance policies could limit or eliminate coverage for catastrophic losses. Thus, a federal insurance response is warranted for catastrophic cyber incidents, whether as part of an amended Terrorism Risk Insurance Program (TRIP) or in a new independent type of insurance backstop program. In whatever federal form or organization a catastrophic cyber backstop program takes, such program should not create moral hazards by encouraging organizations to take undue risks or fail to implement cybersecurity controls because member organizations' existing cybersecurity controls already exceed their insurance requirements. If the federal backstop does impose cybersecurity controls as a condition for federal cyber coverage, the backstop should adopt existing external standards such as by NIST or ISO (as we discuss later) rather than implement a new federal cybersecurity standard. For these reasons, and in support of a federal insurance response for catastrophic cyber incidents, RIMS provides comments on questions 1, 4, 6, and 7.

RIMS Comments

I. Topic 1, Catastrophic Cyber Incidents (Questions 1-3)

A. Question 1: Nature of Event: Numerous types of cyber incidents could have a catastrophic effect on U.S. critical infrastructure.[1]

Although the request for comments focuses on critical infrastructure, disruption to critical infrastructure could adversely impact both critical infrastructure[2] and dependent economic

---

[1] We have included hyperlinks to some sources rather than write the full web address.

[2] The request does not define "critical infrastructure." The GAO Report *Cyber Insurance, Action Needed to Assess Potential Federal Response to Catastrophic Attacks* (June 2022), defines (or categorizes) critical infrastructure as NIST does, as "the systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating effect on security, national economic security, economic stability, national public health or safety, or any combination of those matters." (The GAO's definition slightly differs from the European Union's Council Directive, 2008/114/EC, which defines critical infrastructure as "an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.") Those "systems and assets" seem to be the categories the CISA calls "sectors" comprised of chemical facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear, transportation systems, and water and wastewater systems. Some critical infrastructure may be owned and managed by municipalities or federal corporations or agencies, such as electrical power systems, emergency, health care, transportation systems, and

sectors. Failure of a primary system will cascade to multiple other system failures. For example, failure of communications, electricity, water and wastewater systems (not individual units that are direct to one business operation) will cause most of the other systems to cease operations. A failure in chemical services, on the other hand, may not result in a failure of communications or electrical systems. A failure in transportation, while significant, depends on which transportation system fails and the alternative systems that remain in place. This primary versus secondary failure, or first- and second-order effects, are not exclusive.

For a business that itself is critical infrastructure and is attacked,[3] such as a utility provider or major food provider, the second-order losses caused by the attack would be widespread and deep. But other sectors could also be severely impacted. Businesses such as food purveyors and grocery stores, banks, health care providers and pharmacies, may have backup capacity limited to a few days. Beyond that, food would spoil, certain drugs would be rendered unstable and unusable, and banks could not process transactions to allow the remaining businesses to remain functional. Without access to a federal backstop, these organizations could sustain debilitating losses because of a cyber attack on critical infrastructure. For that reason, RIMS recommends that the federal backstop extend to all economic sectors rather than only critical infrastructure.

II. Topic 2, Potential Federal Insurance Response for Catastrophic Cyber Incidents (Questions 4-8)

A. Question 4, Insurance Coverage Availability:

1. The private insurance market is not making available insurance for catastrophic cyber incidents desired by policyholders.

Although 91% of organizations responding to RIMS recent survey reported that they purchased cyber insurance, and 53% of those organizations purchased limits above $10 million, many respondents could not procure desired limits in the private insurance market, demonstrating that the private market is not providing desired cyber insurance coverage. 73% of respondents purchasing limits below $10 million would have purchased limits *above* $10 million if available for a reasonable premium.[4] Premium concerns impacted the insurance procurement of the majority of responding organizations: 61% of respondents reported that high premiums

---

water systems, while other critical infrastructure may be in the private sector, often with significant federal statutory requirement and federal agency oversight, and sometimes state regulatory oversight as well.

[3] A hierarchy of attacks is: Network Denial, Enterprise Denial, Enterprise Manipulation, Mission Denial, and Mission Manipulation; in David Musielewicz, 2020. "The Spectrum of Cyber Attack," *Air & Space Power Journal*, vol. 34(4): 91-100. The specifics of an attack are not important to this comment.

[4] 10% of respondents purchased limits between $5 and $10 million, and 23% purchased limits between $2 and $5 million. Only a small percentage purchased low or no cyber insurance limits: 7% purchased limits between $1 and $2 million, 1% purchased limits below $1 million, and just 7% did not purchase cyber insurance at all.

impacted their cyber insurance purchasing decision. These survey results demonstrate that the private market is not providing the cyber insurance sought by insureds.

2. While the private insurance market provides some cyber insurance coverage, war exclusions would limit or eliminate coverage for catastrophic losses.

Cyber insurance policies, like other liability policies, typically exclude coverage for losses arising out of acts of war. Because catastrophic cyber incidents, as that term is outlined in the FIO request, could be caused by nation-state actors, insurers may assert war exclusions as defenses to coverage for these cyber events. The difficulty for insurers, and thus for businesses, is that state-actors committing cyberattacks have not followed previous war conventions by declaring war, not even the current "special military operation" by Russia against Ukraine. Where war can be conducted without a declaration of war, and without a nation's armed forces firing explosives and bullets, (what the military refers to as "kinetic warfare", but which is not the insurance definition of war), then insurers' invocation of war exclusions will lead to insurance uncertainty and the potential loss of coverage for catastrophic cyber incidents.[5]

Under these conditions, cyber policies war exclusions are ambiguous at best. By way of example, the "War" exclusion in Form CY 00 02 11 21© issued by the Insurance Services Office, Inc., excludes coverage for cyber liabilities "[b]ased upon, arising out of or attributable to: 1. War, including undeclared or civil war or civil unrest; 2. Warlike action by military force, including action hindering or defending against an actual or expected attack, by any government, sovereign or other authority using military personnel or other agents; or 3. Insurrection, rebellion, revolution, usurped power or action taken by government authority in hindering or defending against any of these." The policy form does not define the term "War," but the first prong of the definition broadly defines "War" to include "undeclared or civil war or civil unrest." The second prong requires an action "by any government, sovereign or other authority," and the third prong refers to a "government authority." Thus, an undeclared war may still constitute war under insurance policy exclusions for war. A leading cyber insurance provider, Lloyd's of London through its member companies, developed and require a cyber war exclusion to be added to its policies. Likely the insurance market will soon adopt similar exclusions for other

[5] "'War' has been defined almost always as the employment of force between governments or entities essentially like governments, at least de facto." *Pan Am. World Airways, Inc. v. Aetna Cas. & Sur. Co*., 368 F. Supp. 1098, 1130 (S.D.N.Y. 1973), *aff'd*, 505 F.2d 989 (2d Cir. 1974); the word 'war' when used in a private contract or document should not be construed on a public or political basis, in a legalistic or technical sense, but should be given its ordinary, usual and realistic meaning, viz., actual hostilities between the armed forces of two or more nations or states de facto or de jure." *Stanbery v. Aetna Life Ins. Co*., 26 N.J. Super. 498, 505, 98 A.2d 134, 138 (Law. Div. 1953).

companies.[6] Insurers may rely on this language to invoke this or similar war exclusions to eliminate coverage for catastrophic cyber incidents.

To date, insurers have not invoked war exclusions in response to cyberattacks, although the NotPetya attack was attributed to Russia. The most recent case to address the war exclusion was *Merck v. Ace American Insurance Co.*, a New Jersey trial court decision in 2021, arising from Russia's cyberattacks against Ukraine in support of Russia's ground force operations, and the consequential transmission of malware outwards from targets in Ukraine, but the *Merck* case involved a property insurance policy, not a cyber insurance policy. The case nevertheless raised the problem of applying a war exclusion to an undeclared war against a nation other than the United States. The general understanding in the industry is that cyber insurers paid for the consequential impacts on insureds whose computers and IT systems were damaged by NotPetya.

A cyberattack against an asset or system in critical infrastructure (utilities, for example) requires attribution to the attacker to determine whether the attack might be excluded as terrorism or war, or "merely" criminal. Yet these distinctions may be thoroughly blurred when nations engage in attacks absent a declaration of war and through the use of non-military operations, yet with the obvious acquiescence or cover of a criminal enterprise operating in a totalitarian state.[7] Such operations are really what we might call "undeclared warfare saboteurs." On this spectrum, the U.S. and other Western governments may be able to trace back the origin of the malware to a hostile country and even a particular location therein (as with Russia and NotPetya). Meanwhile, every business that was hit directly and indirectly by such sabotage finds itself a victim of an undeclared and even perhaps an unknown war. This is a problem for cyber insurance and its buyers, the insured businesses.

B. Question 6. Federal Insurance Response: A federal insurance response is warranted for catastrophic cyber incidents.

As discussed above, RIMS members cannot procure the desired cyber insurance limits for reasonable premiums. And even if they do so, insurers will likely assert war exclusions to eliminate coverage for catastrophic cyber incidents. Not surprisingly, RIMS member organizations overwhelmingly support a federal cyber insurance backstop: *80%* of respondents support a federal cyber insurance program that provides a federal backstop. 11% were not sure, and only 10% of respondents opposed a federal backstop. The demographics of survey

---

[6] Given the dramatic consequences of state-attributed cyber hacks such as WannaCry, Petya, and NotPetya and the likelihood of similar attacks being launched in the future, insurers may increasingly try to limit potential payouts by invoking arguments similar to Zurich's.' Justine Ferland, 2019. "Cyber Insurance – what Coverage in Case of an Alleged Act of War? Questions Raised by the *Mondelez v. Zurich* case." *Computer Law Security Review*, vol. 35: 369-376, at p. 376. The Mondelez case involved a property policy, not a cyber insurance policy.

[7] See for example the Department of Justice's February 2021 indictment of cyber criminals acting on behalf of the North Korean Government.

respondents illustrate the strong desire for federal participation by even large member organizations. 39% of respondent organizations employ more than 10,000 people, an additional 10% employ between 5,000 and 10,000 people, and 29% employ between 1,000 and 5,000 people. Fewer than 20% employed less than 1,000 people (10% employed between 500 and 1,000 and 13% employ less than 500 people.)

C. Question 7. Potential Structures for Federal Insurance Response:

1. Potential Models:

Although TRIP can serve as one model by which to evaluate and create federal financial support against a catastrophic cyberattack, TRIP was intended for terrorism, and assumes that a terrorism event would be limited in location and targets, even if the attack affects some significant geographical area such as lower Manhattan following the World Trade Center attack. A catastrophic cyberattack may not be so limited, as for example the Colonial Pipeline attack that affected fuel supplies from Texas across the entire eastern seaboard states,[8] or the attack on Nordstream 1 that has significantly impacted multiple European countries. Many industries consist of only a few large firms with dominant market shares. This is concentration risk within sectors, for which the usual risk management techniques of duplication and segregation of assets and capabilities by any individual business may be inadequate to maintain that businesses' services.

The current cyber difficulties are mostly by nation states operating in various forms, and do not seem to fit within TRIP. Either TRIP should be enlarged to deal with these nation-state actions, or a new program should be created. Ambiguity about terrorism and undeclare warfare needs to be resolved at the federal level before businesses and insurers can address the losses that might be abated by insurance.

2. Cybersecurity Measures and Moral Hazard:

a. A federal backstop should not cause organizations to take undue risks or fail to implement cybersecurity controls.

RIMS members purchasing cyber insurance already maintain cybersecurity controls that exceed their insurers' requirements, thus indicating that neither the private insurance market nor a federal insurance backstop will cause organizations to take undue risks or fail to implement cybersecurity controls. 59% of respondents reported that their cyber insurance policies *do not* require cybersecurity controls that exceed their organization's existing cybersecurity controls,

---

[8] See Colonial Pipeline's webpage for the system, https://www.colpipe.com/about-us/our-company/system-map; and see Charlie Osborn, 2021. "Colonial pipeline Ransomware Attack: Everything You Need to Know," *ZDNet.com*, https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/

thus demonstrating that insurance does not drive the cybersecurity measures implemented by these organizations. 32% of respondents would purchase cyber insurance requiring cybersecurity controls that exceed their existing cybersecurity controls. 22% would not, and 46% were uncertain. We lack information as to how many RIMS members are ISO or NIST compliant for information security. We lack information as to how non-members of RIMS conduct their IT security, though general information suggests that many small companies without a real risk manager (as opposed to some person being given risk management responsibilities) or an information security officer or vendor have much weaker cyber controls.

Respondents purchase cyber insurance even if their organizations have not recently experienced a cyber incident. 65% of respondents reported that they had incurred *no* cyber losses within the last year. An additional 31% had incurred cyber losses below $1 million in the last year. Only 2% had incurred losses exceeding $10 million, with another 2% incurring losses between $1 and $5 million.

b. A federal backstop should not promulgate any new cybersecurity standard, but should only require organizations to adopt any of the available existing regulatory, statutory, or independent standards.

Because state governments and regulatory bodies as well as nongovernmental organizations have promulgated cybersecurity standards, the federal backstop should require no more than adherence to one or more existing cybersecurity standards. The evolving nature of cyberattacks makes it difficult to adopt one final, implementable standard. Possible standards include those now established or to be established by NIST or ISO (International Standards Office) for information technology security, by the New York State Department of Financial Services cyber security standards, or by those stated in the FTC's Stipulated Order and Permanent Injunction order against Equifax in 2019 that specifies a "Mandated Information Security Program." Many cyber insurers already require demonstrable levels of security and protections, sometimes as industry best practices, sometimes as insurers' conditions of coverage, or both, so many insureds already comply with externally imposed standards.

Conclusion

Thank you for the opportunity to present RIMS views on establishing a federal insurance response to catastrophic cyber incidents in response to the FIO's request for public comments on the "Potential Federal Insurance Response to Catastrophic Cyber Incidents," as published in the Federal Register on September 29, 2022 at 87 FR 59161 *et seq*.

Respectfully Submitted,

RMPrysock

Mark Prysock
General Counsel & Vice President of Advocacy
Risk and Insurance Management Society