EVERSHEDS SUTHERLAND

A look ahead

US Treasury Department announces initiatives for further study of a federal insurance backstop for catastrophic cyber events

On November 17, 2023, the United States Treasury Department's Federal Insurance Office (**FIO**) and the Volatility and Risk Institute at the NYU Stern School of Business jointly hosted a conference on *Catastrophic Cyber Risk and a Potential Federal Insurance Response* at which Treasury and FIO announced initiatives for further study for the development of a Federal insurance backstop for catastrophic cyber events.

I. Background

The prospect of a federal cyber insurance response gained significant momentum in recent years in response to growing awareness of the threats to national security and the US economy posed by cyber risk. In June 2022 the Government Accountability Office (**GAO**) published a report, titled Action Needed to Assess Potential Federal Response to Catastrophic Attacks, that recommended FIO and the Cybersecurity and Infrastructure Security Agency (**CISA**) produce a joint assessment for Congress on the extent to which the risks to the nation's critical infrastructure from catastrophic cyberattacks and the potential financial exposures resulting from these risks warrant a federal insurance response.

In response to the GAO Report, in September 2022, FIO published a request for comment on questions related to cyber insurance and catastrophic cyber incidents to inform a joint assessment by FIO and CISA on the extent to which risks to critical infrastructure from catastrophic cyber incidents and potential financial exposures warrant a federal insurance response. FIO received 60 comments from interested stakeholders.

In July 2023, the Biden Administration published a National Cybersecurity Strategy Implementation Plan that includes as a strategic objective the exploration of a "federal cyber insurance backstop" and identified FIO as the responsible agency for assessing the need for and possible structures of a federal insurance response to catastrophic cyber events. The plan sets the first quarter of 2024 as the deadline for the assessment.

II. Federal Backstop

During the Conference, Treasury's Assistant Secretary for Financial Institutions, Graham Steele, answered the question of whether there is a need for a federal insurance response to catastrophic cyber incidents with, "the final answer looks less like a straightforward 'yes' or 'no' than a more nuanced 'it depends'" and indicated further exploration of the proper federal insurance response should be undertaken. He reported the conclusions that Treasury has made so far are (1) the private market for insurance against attritional cyber risk from losses other than those related to major catastrophes is dynamic and growing and, as a result, Treasury's assessment of potential federal response will be focused on catastrophic risk; and (2) Treasury will remain focused on policy options for a public-private collaboration or other federal response that "cabins" catastrophic risk alongside the commercial market. To many in the audience, this signals exploration of a program along the lines of the federal Terrorism Risk Insurance Program, which is also administered by FIO.

Steele also reported that FIO will take a leadership role in the International Forum of Terrorism Risk (Re)Insurance Pools (**IFTRIP**), an umbrella organization for over 15 international terrorism risk insurance pools and mechanisms that engage in the insurance or reinsurance of terrorism risk, and will host the 2024 IFTRIP Annual Conference in Washington, DC. Treasury also will host a conference in April to explore in more detail some specific ideas about the form of a federal response and may organize one or more informal groups of subject matter experts and key stakeholders on specific topics.

III. Cybersecurity Insurance Data Analysis Working Group

FIO Director Steven Seitz announced the reconstitution of the Cybersecurity Insurance Data Analysis Working Group (**CIDAWG**) to establish a cyber repository whereby relevant federal agencies would be permitted to provide participating insurers with certain anonymized and/or aggregated information regarding cyber threats in order to more accurately price policies and to assist insureds with risk mitigation.

CIDAWG was first established in 2014 as a joint effort by FIO and the US Department of Homeland Security to consider the following four issues:

- The value of a cyber incident data repository
- The cyber incident data points that should be shared into a repository to support to support needed analysis
- Methods to incentivize such sharing on a voluntary basis
- A potential repository's structure and functions

Among other things CIDAWG proposed creating a Cyber Incident Data and Analysis Repository that would provide insurers and other stakeholders with information to develop coverage and risk management solutions. The group also published the following three working papers before it was disbanded:

- The Value Proposition for a Cyber Incident Data Repository
- Establishing Community-Relevant Data Categories in Support of a Cyber Incident Data Repository
- Overcoming Perceived Obstacles to Sharing into a Cyber Incident Data Repository

While the insurance industry was generally supportive of the initial CIDAWG Repository, there were concerns about how to keep data anonymous and secure.

Contacts

If you have any questions about this Legal Alert, please feel free to contact any of the attorneys listed or the Eversheds Sutherland attorney with whom you regularly work.

John S. Pruitt
Partner
T: +1 212 389 5053
johnpruitt@eversheds-sutherland.com

Michael Bahar
Partner, Co-Lead of Global Cybersecurity and Data Privacy
T: +1 202 383 0882
michaelbahar@eversheds-sutherland.com

Alexander F.L. Sand
Counsel
T: +1 512 721 2721
alexandersand@eversheds-sutherland.com

Daniel McCarty
Associate
T: +1 212 287 6952
danielmccarty@eversheds-sutherland.com

eversheds-sutherland.com