Remarks by Assistant Secretary Graham Steele at the Federal Insurance Office and NYU Stern Volatility and Risk Institute Conference on Catastrophic Cyber Risk and a Potential Federal Insurance Response

November 17, 2023

As Prepared for Delivery

Good afternoon. My name is Graham Steele, and I am the Assistant Secretary for Financial Institutions at the Treasury Department. It's my pleasure to help conclude this Treasury FIO-NYU conference on catastrophic risk and a potential federal insurance response.

A number of people are responsible for making today's event a success. Many thanks to our co-sponsor and generous host, NYU Stern's Volatility and Risk Institute, co-directed by my friend Dick Berner, and to VRI's Assistant Director Matt Hemphill. Thanks also to my executive branch colleagues from the Office of the National Cyber Director and the Cybersecurity and Infrastructure Security Agency for joining us today. Thanks to our experienced and knowledgeable panelists, representing so many insurance industry stakeholder organizations, for sharing their very useful insights. Thanks to my Treasury colleague FIO Director Steven Seitz and the Federal Insurance Office team for organizing this conference and spearheading Treasury's work on this issue. And considering the range of important roles that many of you in this room have in the cyber insurance ecosystem, thanks to all of you for coming this morning. I hope you've found the discussions useful. The Treasury team looks forward to continuing to work with you on these issues.

As the Assistant Secretary for Financial Institutions, I oversee a broad policy portfolio, encompassing banks, credit unions, and the insurance sector, as well as cybersecurity and critical infrastructure, community development, and consumer protection. The topic of today's conference sits at the intersection of insurance and cybersecurity and critical infrastructure. Let me begin by discussing the relevant work done by those two offices, before diving deeper into the topic of the conference, catastrophic cyber insurance specifically, and concluding with a few points about our plans going forward.

Cyber-related risk is a top priority for Treasury and the Biden administration. As you heard this morning from Director Seitz, for over a decade the Federal Insurance Office has followed the evolution of the insurance sector's important role in our increasingly digitally interconnected world. Treasury and FIO have been working closely with our partners across the administration and are focusing on the following cyber insurance-related topics:

First: cyber resilience. FIO has worked with colleagues within Treasury and the administration on improving insurers' own cyber resilience. We have also cooperated with other federal and state partners and with international colleagues through multilateral groups such as the G-7.

Second: we are focused on cyber insurance in lines of insurance eligible for coverage under the Terrorism Risk Insurance Program, or "TRIP." A cyber attack could be certified by Treasury as an "act of terrorism" as defined in the Terrorism Risk Insurance Act, provided it otherwise meets the requirements of TRIP. In recent years FIO has increased its collection of data on cyber insurance in order to improve Treasury's evaluation of cyber insurance within the scope of TRIP, as well as improving our understanding of the overall cyber market.

Third: FIO is prioritizing its work in The International Forum of Terrorism Risk (Re)Insurance Pools, or "IFTRIP." IFTRIP is the umbrella organization for over 15 international terrorism risk insurance pools and mechanisms that engage in the insurance or reinsurance of terrorism risk. FIO serves as the Vice Chair of IFTRIP and next April Treasury will be hosting the 2024 IFTRIP Annual Conference in Washington, DC as part of our work to assume more leadership of this group going forward. At the Annual Conference, we expect that industry representatives and public sector authorities will discuss issues presented by terrorism risk in particular, as well as catastrophic risk more generally. Our decision to take on more of a leadership role in the group demonstrates our commitment to working with our international partners on cyber issues. We're excited about the direction of IFTRIP's future work under greater U.S. leadership, and we look forward to increasing our collaboration with the sector in this area.

Fourth: Treasury and FIO continue to monitor and collect data on cyber insurance market developments. We have long recognized that cyber insurance is a dynamic and growing market. FIO's 2023 Annual Report, published in September, observed a 50 percent increase between 2021 and 2022 in direct premiums for cyber insurance, growing from approximately $4.8 billion in direct premiums for both package and stand-alone policies in 2021, to approximately $7.2 billion in direct premiums last year. However, this premium growth is not

proportional to the growth in coverage. Cyber insurers wrote nearly 4 million policies in 2022, which is only a 10 percent increase from 2021.

Importantly, there is substantial room for further growth. 2022 cyber premiums remained under one percent of the total P&C market, despite the consistent movement toward the digital transformation of everything we do in the physical world – a trend intensified at the peak of the pandemic, and which has not since reversed. Additionally, the broker Marsh, whose CEO you heard from today, recently estimated that 36 percent of its insurance clients buy cyber insurance, and that the largest companies – those with greater than $1 billion in annual revenues – are far more likely to buy cyber coverage than small and medium-sized enterprises.

I'd like to take a brief step back to discuss the broader cyber threat landscape. Treasury's Office of Cybersecurity and Critical Infrastructure Protection's, or "OCCIP," mission is to improve the security and resilience of the financial services sector through Treasury's unique role in the Financial and Banking Information Infrastructure Committee, or "FBIIC," and the G7, both as a cabinet-level Department, and as Sector Risk Management Agency, or "SRMA," for the financial services sector. OCCIP serves as the central node for information related to all-hazard threats and seeks to build and maintain resilience through exercises sharing relevant threat information. Additionally, OCCIP serves as a central hub and coordinating body for financial institutions and regulatory agencies that respond to cyber incidents when they do occur. Finally, OCCIP advances U.S. Government policies and conducts whole-of-nation coordination for cybersecurity and infrastructure protection based on findings from the activities I've just described.

In its SRMA capacity, OCCIP has been on the forefront of some of the most important issues of the day, including Treasury's landmark Financial Services Sector's Adoption of Cloud Services report and the upcoming work that we are undertaking on the implications of artificial intelligence, or "AI," on financial services sector cybersecurity. The increasing adoption of cloud services and AI will only raise the stakes for public and private sector efforts to ensure operational and cyber resilience. Combating the growth of ransomware, and thereby decreasing policyholder ransom payments, remains a policy priority for Treasury and the Administration. Industry sources report that after a possible decrease in successful attacks in 2022, there has been a substantial resurgence in ransomware attacks in 2023. In a notable recent example, just last week, the US broker-dealer affiliate of the bank ICBC suffered a ransomware attack that has impacted its client clearing business. This is not the first time

this year that ransomware has disrupted financial sector operations. In February and March, a ransomware attack on the trading firm Ion similarly disrupted its cleared derivatives business for several days.

Criminal actors with financial motives are not the only threat requiring the maintenance of up-to-date cyber controls, as we have seen in the multiple global crises playing out in the news. Both the Russian invasion of Ukraine and the Israel/Hamas conflict have included state and non-state threat actors employing cyber tactics with increased proficiency.

In the weeks following Russia's invasion of Ukraine, Russian state-sponsored cyber actors conducted a wave of cyberattacks against Ukrainian infrastructure, including several attacks targeting financial services sector entities. By April 2023, there was a significant drop in these incidents and a lull in state-sponsored activity has continued. Additionally, Russia has been observed to coordinate destructive and disruptive cyberattacks aimed at Ukraine, network penetration and espionage in targeted countries that are perceived as Ukraine's allies, and cyber-influence operations designed to influence people globally. The Computer Emergency Response Team of Ukraine (CERT-UA) recorded nearly 4,000 cyber incidents between January 2022 and September 2023. This represents a three-fold increase in cyber activity to the pre-war period.

Cyber activity in the context of the Russia/Ukraine conflict is not limited to government actors. We have observed that non-state cyber actors on both sides of the conflict have targeted a wide range of organizations – including in the financial services sector – with relatively unsophisticated incidents known as distributed denial of service attacks (DDOS). In June 2023, pro-Russia hacktivist group NoName057(16) threatened to target Ukraine's financial sector. In the following four days, numerous Ukrainian banks were targeted with DDoS attacks. Targets included four of the nation's largest commercial banks, including First Ukrainian International Bank (PUMB), State Savings Bank of Ukraine (Oshchadbank), Credit Agricole Bank, and Universal Bank.

Shifting to Israel, since the onset of the conflict, there has been a significant increase in hacktivist groups targeting both Israeli and Palestinian entities. The tactics, techniques, and procedures include low-level DDoS attacks, website defacements, data breaches, exploitation of known common vulnerabilities and exposures (CVE), and a newly identified destructive wiper malware called Bibi-Linux (being used to destroy data in attacks targeting Linux systems belonging to Israeli companies), which has had minimal disruptive impact.

According to Cloudflare, hacktivist groups have primarily targeted newspaper and media outlets with DDoS attacks, which have accounted for 56% of all attacks against Israeli websites. The second most targeted industry was the computer software industry, accounting for 34% of all DDoS attacks. The third most targeted was the Banking, Financial Services, and Insurance sector; followed by Government Administration websites. Additionally, Indian cyber intelligence company FalconFeeds has identified 90 pro-Palestinian hacktivist groups. The most prominent pro-Palestinian hacker groups are KillNet, Anonymous Sudan, and Mysterious Team Bangladesh.

Closer to home, Google, Amazon, and Cloudflare reported in October that they had withstood the internet's largest-known DDoS attack, exploiting a new vulnerability known as "Rapid Reset", with Google Cloud (from which you heard on the last panel today) reporting that its cloud service had dealt with an attack more than seven times larger than the previous largest attack. In response, our colleagues at CISA swiftly issued an advisory notice warning about the vulnerability and recommending that organizations that deliver essential internet services quickly apply patches to their networks and implement other mitigation measures.

The insurance sector has an important role to play in strengthening policyholder cyber controls in order to improve resiliency against attritional cyber incidents, including ransomware attacks. By requiring robust cybersecurity practices to qualify for coverage, cyber insurers can, and have, incentivized best practices that defend against ransomware attacks and avoid the need for policyholder ransom payments.

With all of that context, let me return to the main subject of my remarks, and today's conference: insurance for catastrophic cyber incidents, and whether some kind of federal insurance response – such as a potential government partnership with the commercial cyber insurance market – is warranted. Treasury's research, analysis, and engagements with stakeholders in this area over the past year and a half have suggested a few preliminary observations, which I think we've heard echoed in the discussions today.

One such observation is that catastrophic cyber risk appears to be different from attritional cyber risk in at least some significant respects, at least for now. As you've heard today, while cyber insurance is a growing and evolving market, insuring for catastrophic cyber risks presents distinct challenges that need to be addressed. Unlike for natural catastrophes, there is only limited historical data on systemic cyber incidents causing catastrophic losses with which to model actuarial projections, despite the rapidly increasing interconnectedness of our digital and networked world. Risk evaluation for cyber is further complicated in that

cyber risks can cascade across geographic and commercial boundaries. This limits the ability of insurers and reinsurers to use traditional risk transfer strategies focusing on the region, industry, or size of the entity insured, and thereby requires the reevaluation of underwriting and risk management strategies to account for such differing accumulation risks. Although the quality of cyber models is improving, they still have a long way to go, and they remain particularly assumption-dependent and may produce divergent results, particularly with respect to tail scenarios. This uncertainty has increasingly led the sector to manage its exposure through tighter wording and broader exclusions and has also contributed to the reluctance of capital providers to provide greater capacity to the market.

Even so, one might ask, why is it necessary to decide whether some kind of federal insurance response is warranted *now*? In his remarks at the beginning of this event, Director Seitz described some of the origins of this inquiry, including language included in the 2019 reauthorization of the Terrorism Risk Insurance Act, and a June 2022 Government Accountability Office report that concluded with a recommendation that FIO and CISA conduct a joint assessment of whether a federal insurance response to catastrophic cyber incidents is warranted, which recommendation Treasury and DHS accepted, leading to FIO's Request For Information about a *Potential Federal Insurance Response to Catastrophic Cyber Incidents* last fall.

As you heard earlier from Deputy National Cyber Director Dudley, Treasury's work in this area was highlighted in the Biden Administration's National Cybersecurity Strategy released in March of this year. Specifically, strategic objective 3.6 of the Strategy states: [quote] "The Administration will assess the need for and possible structures of a Federal insurance response to catastrophic cyber events that would support the existing cyber insurance market." [end quote]. This objective appears in pillar three of the strategy, which is to "Shape market forces to drive security and resilience."

The framing of the objective to assess the need for a federal insurance response to catastrophic cyber incidents as part of the National Cybersecurity Strategy's overall emphasis on strengthening national resilience underlines a second observation that Treasury's work on catastrophic cyber risk has suggested, and an answer to the question raised earlier, why now: the broad benefits for resilience and market certainty of advance planning for the economic impact of a catastrophic cyber incident. This is a point that many of you in this room appreciate and have identified yourselves. It is also an issue that our team has dealt with

while assessing the impact of the COVID-19 pandemic on insurance markets and the potential policy responses in 2020.

In short, waiting until after a catastrophic cyber incident occurs is sub-optimal for everyone, including private sector firms, the government that bears the responsibility for stabilizing the economy, and ultimately the taxpayers. While none of the recent events that I noted earlier have resulted in catastrophic cyber incidents, they are increasing in their frequency and impact. Indeed, it may be a matter of when—not if—we experience a catastrophic cyber event. As the National Cybersecurity Strategy puts it, "Structuring [a response to a catastrophic cyber incident] before a catastrophic event occurs—rather than rushing to develop an aid package after the fact—could provide certainty to markets and make the nation more resilient."

It is worth noting here that in its discussion of cyber insurance, the National Cybersecurity Strategy uses the term "resilience" with respect to the U.S. economy as a whole – as distinct from the narrower context of the resilience of the insurance industry alone. I believe this is a distinction that has also been made during today's discussion.

As you have heard from my government colleagues earlier today, following its release of the National Cybersecurity Strategy, in July of this year the Administration published the Implementation Plan for the Strategy providing additional guidance to Treasury on next steps. The Implementation Plan reaffirms that Treasury—specifically FIO—is the agency responsible for answering the threshold question of whether some form of federal insurance response to catastrophic cyber incidents is warranted and sets forth the end of this year as the target date for when the Administration will answer this question through our assessment.

It has been a busy year and a half since we initiated our assessment of catastrophic cyber risk and insurance. Thus far, our initial focus has been on the threshold question of whether the risks from catastrophic cyber incidents warrant some kind of a federal insurance response. As summarized earlier by Director Seitz, we received a great deal of substantive and useful feedback to our RFI from a broad cross-section of stakeholders. In addition, we have benefited from both extensive industry meetings and internal research on the subject. Today's conference is an important part of our engagement effort. The panel discussions have helped us to gain further insights from the perspectives of industry parties on the important policy issues presented by catastrophic cyber risk and a potential federal response.

The National Cybersecurity Strategy and its Implementation Plan have charged us with answering a straightforward question about this complex issue: Is some kind of federal insurance response to catastrophic cyber incidents warranted? This is the main issue that we are seeking to answer right now. We're fortunate to have learned a lot from these conversations today. We need more of these types of conversations with the industry and other stakeholders going forward.

Based upon the work that we have done and the discussions we've had to date, the final answer looks less like a straightforward "yes" or "no" than a more nuanced "it depends." As today's event has highlighted, 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.

As for the immediate threshold question, however, we believe that further exploration of the proper federal insurance response to catastrophic cyber risk is warranted and should be undertaken.

And while much more work – and much more consultation – will need to take place about what form such a federal insurance response and/or such a public-private partnership should take, our work thus far has positioned us to reach at least one tentative conclusion regarding the scope of our focus, and to announce one concrete plan for our work in this area in 2024.

The conclusion regarding scope is that because we see that the private market for insurance against attritional cyber risk from losses other than those related to major catastrophes is dynamic and growing, we anticipate that our assessment of a potential federal insurance response will remain sharply focused on catastrophic cyber risk. And when assessing the insurance market for catastrophic cyber risk, we will remain focused on the policy options for some kind of public-private sector collaboration or other federal response that cabins catastrophic cyber risk alongside the existing and expanding commercial cyber insurance market.

I am also pleased to announce here that, in conjunction with Treasury hosting next year's International Forum of Terrorism Risk (Re)Insurance Pools, or IFTRIP, Annual Conference in Washington, DC in April 2024 that I mentioned earlier, Treasury will host an additional conference during the week of April 22 exploring in more detail some specific ideas about what form such a federal insurance response to catastrophic cyber risk, and/or a public-private partnership or other collaborative mechanism, might take. This conference, which FIO will

organize, will naturally draw on the expertise of industry and other cyber insurance stakeholders, and will, in effect, serve as the follow-on to today's event.

Furthermore, preparations for this April conference will help structure FIO's upcoming engagements with industry on this subject leading up to the conference, which could involve the organizing of one or more informal groups of subject matter experts and key stakeholders on specific topics relating to catastrophic cyber insurance.

FIO plans to take further actions along these lines after the new year. In the meantime, I look forward to seeing many of you at the subsequent event on catastrophic cyber insurance in April.

In closing, let me say that it is clear that there is a great deal of interest in, and a significant number of complex questions about, this important issue. I expect that many of you in this room will play an important role in helping to work through those questions in discussions with our FIO team.

I want to again extend my and Treasury's thanks to our co-sponsor, Dick Berner and NYU's Volatility and Risk Institute; to all of our excellent speakers today; and to all of you in the audience for coming. We at Treasury look forward to continuing to work further with you all on the important issue of insurance for catastrophic cyber risk in the future.

###