PUBLIC COMMENT: FOUNDATION FOR DEFENSE OF DEMOCRACIES

Department of the Treasury

2026 TRIP Effectiveness Report

AUTHORS

Nicholas Leiserson
Advisor, FDD's Center on Cyber and Technology Innovation

Aarushi Garg
Research Intern, FDD's Center on Cyber and Technology Innovation

Washington, DC
May 8, 2026

FDD
FOUNDATION FOR DEFENSE OF DEMOCRACIES

www.fdd.org

Executive Summary

The cyber insurance market has grown substantially over the past two decades but has not matured to meet the scale of the threat.[1] Despite reaching over $14 billion in gross written premium, the market has persistent coverage gaps, volatile pricing, and underwriting practices that fall short of policymakers' expectations.[2] In 2016, the White House Council of Economic Advisers estimated that malicious cyber activity cost the U.S. economy between $57 billion and $109 billion annually.[3] Unfortunately, those costs have only risen over the past decade. U.S. insurance claims, however, totaled only about $3 billion in 2023.[4] That gap between what cyber incidents cost and what cyber insurance covers is symptomatic of a market failure — a failure that a government reinsurance program would resolve.

One structural cause of this failure is accumulation risk. Unlike most insurable perils, cyber losses are highly correlated across firms, sectors, and geographies. A single vulnerability or attack can generate simultaneous claims across an insurer's entire portfolio, making it structurally impossible for private markets to diversify away systemic cyber risk. The emergence of AI-enabled, vulnerability discovery tools has sharpened this problem, raising the prospect that a single AI-identified exploit could simultaneously affect thousands of organizations sharing common infrastructure. The market is unlikely to resolve this accumulation risk on its own or fast enough to account for the changing cyber threat environment.

Treasury is wisely attempting to address this challenge, soliciting comment on the terrorism risk insurance issues presented by cyber-related losses and the impact of the Terrorism Risk Insurance Program (TRIP) in connection with such exposures (Question 5); potential changes to that would encourage take-up of insurance for cyber-related losses (Question 6); and the availability of reinsurance or capital markets support for cyber-related losses arising from acts of terrorism as defined under the Terrorism Risk Insurance Act (TRIA) (Question 7). This comment addresses all three questions.

The Terrorism Risk Insurance Program (TRIP) offers a useful model for government intervention in insurance markets, but its architecture differs from what a cyber reinsurance program requires in important ways. TRIP was designed to reverse an exclusion — terrorism

---

[1] Information contained in this submission is drawn and adapted from: Nick Leiserson, "How a Government Reinsurance Program Can Accelerate Maturation of the Cyber Insurance Market," *The Foundation for Defense of Democracies*, June 17, 2025. (https://www.fdd.org/analysis/2025/06/17/how-a-government-reinsurance-program-can-accelerate-maturation-of-the-cyber-insurance-market)

[2] Andreas Schmitt and Greg Eskins, "Closing the Cyber Risk Protection Gap," *Marsh McLennan and Zurich Insurance Group*, September 26, 2024. (https://www.marshmclennan.com/web-assets/insights/publications/2024/september/mmc-zurich-cyber-whitepaper.pdf)

[3] U.S. Executive Office of the President, Council of Economic Advisers, "The Cost of Malicious Cyber Activity to the U.S. Economy," February 2018. (https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf)

[4] The $3 billion figure is for domestic insurers, which represent approximately 75 percent of the U.S. market. Total covered losses are slightly higher due to alien insurers but well below estimated losses. Craig Kerman, Raymond Clouse, Brienna Reese, and Xuan Lin, "U.S. Cyber Market Update: 2023 U.S. Cyber Insurance Profits and Performance," *Aon*, August 2024. (https://www.aon.com/getmedia/4afa8654-6534-48c3-91c1-b27d57170cdb/20240806-US-Cyber-Market-Update.pdf)

coverage that insurers had stopped offering — whereas the cyber insurance problem is one of accumulation risk within an active market.

Additionally, the cyber incidents most U.S. companies experience likely cannot be classified as acts of terrorism. Treasury is wisely seeking information about what cyber-related losses arise from acts of terrorism, but this is likely a fraction of the risk that companies are attempting to offset through the purchase of cyber insurance.

The questions posed by Treasury's request for public comment, taken together, point to the same conclusion: the existing TRIP framework was not designed for cyber risk's specific characteristics, private reinsurance markets cannot resolve the structural constraints that limit cyber insurance, and a standalone federal cyber reinsurance program is the appropriate remedy. Treasury is uniquely positioned to advance this work.

To do so, the department should use the 2026 Effectiveness Report to formally recommend to Congress the creation of an authority for a standalone cyber reinsurance program: one focused on currently covered risks, with an aggregate loss trigger, defined retention and coinsurance parameters, a cap on total liability, and a recoupment mechanism to protect taxpayers.

Cyber Insurance Is Not Improving Cybersecurity Behavior

For decades, policymakers have looked to cyber insurance as a key tool for reducing the impact of cyberattacks.[5] Insurance serves two functions in this context. It helps ensure continuity: companies can remain productive if insurance helps them become whole again following a cyber incident.[6] And it can incentivize socially desirable behavior: by linking premium discounts to responsible cybersecurity choices, insurers can pressure policyholders to act in less risky ways.[7]

The market, however, is not living up to policymakers' expectations. Only a small fraction of the losses due to cyber incidents are covered by cyber insurance. That in part reflects the low uptake of cyber insurance. Cyber insurance is not federally mandated, and few private entities require minimum cyber coverage from their counterparties as a condition of doing business.[8] Education about the benefits of insurance or regulatory requirements to purchase insurance would drive up purchases.[9] On the other hand, supply-side constraints (discussed below) are keeping premium prices high. Mandating coverage without first resolving supply-side constraints would simply drive up the price of a limited pool of coverage.

---

[5] U.S. Executive Office of the President, "The National Strategy to Secure Cyberspace," February 2003. (https://www.cisa.gov/sites/default/files/publications/cyberspace_strategy.pdf)
[6] Kai-Uwe Schanz, "The Role of Insurance in Promoting Social Sustainability," *The Geneva Association*, November 2022. (https://www.genevaassociation.org/sites/default/files/2022-11/social_sustainability_report.pdf)
[7] Yu-Hung Chen and Baojun Jiang, "Effects of Monitoring Technology on the Insurance Market," *Production and Operations Management*, August 1, 2019. (https://doi.org/10.1111/poms.13023)
[8] Jack Kudale, "Sector Down: Ensuring Critical Infrastructure Resilience," *Testimony before the House Homeland Security Committee, Subcommittee on Cybersecurity and Infrastructure Protection*, June 27, 2024. (https://docs.house.gov/meetings/HM/HM08/20240627/117445/HHRG-118-HM08-Wstate-KudaleJ-20240627.pdf)
[9] U.S. Environmental Protection Agency, "Cyber Insurance for Drinking Water and Wastewater Systems," October 2024. (https://www.epa.gov/system/files/documents/2024-10/cyber-insurance-final-508-101624.pdf)

A limitation on the uptake of cyber insurance is that customers are increasingly finding the product unattractive.[10] While the market experienced rapid early growth — gross written premium roughly doubled from approximately $6.5 billion to $13.9 billion between 2021 and 2022 — growth slowed to under 4 percent globally in 2023.[11] The next year, the U.S. cyber insurance market contracted slightly, with direct written premiums falling 7 percent and the number of policies in force slipping 0.03 percent.[12] Facing rising costs and narrowing coverage, some policyholders have chosen to self-insure or forgo coverage entirely.[13]

Cyber insurance is also failing to improve cybersecurity behavior. While chief information security officers report that underwriting conversations give them significant leverage to implement stronger cybersecurity measures with their boards and senior executives, underwriting has not driven significant changes in cybersecurity posture as policymakers expected.[14] It is more sophisticated today than it was a decade ago, when it often consisted of questionnaires or phone-call interviews, but self-attestation still remains its foundation.[15]

Self-attestation has its limits. A company's policies and technologies are constantly changing, modern information systems are enormously complex, and firms may overstate their security posture without reliable means of independent verification.[16] Claims adjustment provides an opportunity to hold policyholders accountable for commitments made during underwriting, but whether for fear of losing market share or fear of losing in court, carriers have not used this

[10] Gareth Mott, Sarah Turner, Jason R.C. Nurse, Jamie MacColl, James Sullivan, Anna Cartwright, and Edward Cartwright, "Between a rock and a hard(ening) place: Cyber insurance in the ransomware era," *Computers & Security*, May 2023. (https://doi.org/10.1016/j.cose.2023.103162)
[11] "Reality check on the future of the cyber insurance market," *Swiss Re*, November 18, 2024. (https://www.swissre.com/risk-knowledge/advancing-societal-benefits-digitalisation/about-cyber-insurance-market.html); "U.S. Cyber Insurance Maintains Strong Profits; Premium Growth Slows," *Fitch Ratings*, April 16, 2024. (https://www.fitchratings.com/research/insurance/us-cyber-insurance-maintains-strong-profits-premium-growth-slows-16-04-2024)
[12] "Report on the Cybersecurity Insurance Market," *National Association of Insurance Commissioners*, November 10, 2025, page 3. (https://content.naic.org/sites/default/files/inline-files/2025_Cybersecurity_Insurance%20Report.pdf)
[13] "Report on the Cybersecurity Insurance Market," *National Association of Insurance Commissioners*, November 3, 2023. (https://content.naic.org/sites/default/files/inline-files/Final%202023%20Cyber%20Report.pdf); Nathan Eddy, "Organizations Consider Self-Insurance to Manage Risk," *Dark Reading,* March 30, 2023. (https://www.darkreading.com/cyber-risk/organizations-reassess-cyber-insurance-as-self-insurance-strategies-emerge)
[14] Stephen Lawton, "Why CISOs Should Get Involved With Cyber Insurance Negotiation," *Dark Reading*, July 27, 2023. (https://www.darkreading.com/cyber-risk/why-cisos-should-get-involved-with-cyber-insurance-negotiation)
[15] "Report on the Cyber Insurance Market," *National Association of Insurance Commissioners*, October 18, 2022. (https://content.naic.org/sites/default/files/cmte-c-cyber-supplement-report-2022-for-data-year-2021.pdf); Ben Beeson, "Examining the Evolving Cyber Insurance Marketplace," *Testimony before the Senate Committee on Commerce, Science, and Transportation*, March 19, 2015. (https://www.commerce.senate.gov/services/files/68D2A98E-BA98-4ACA-A034-503D67AB6604)
[16] Brett Helm, "Reliance on Self-Attestation Is Not Working for the Cyber Insurance Industry," *CPO Magazine*, October 27, 2023. (https://www.cpomagazine.com/cyber-security/reliance-on-self-attestation-is-not-working-for-the-cyber-insurance-industry)

process to enforce the risk-mitigation procedures their policyholders claim to have implemented.[17]

More broadly, policymakers had hoped cyber insurance would also serve as the foundation for evidence-based cybersecurity. Yet empirically backed cybersecurity controls remain few and far between. Even the limited models that tie claims data to underwriting have not produced significant benefits for the broader cybersecurity community.[18]

These are not problems the market will resolve on its own, at the pace the threat environment demands.

Supply-Side Constraints or Why the Market Cannot Fix Itself

The single most important structural limitation of the cyber insurance market is the inability to diversify risk. In traditional insurance lines, geography and other factors allow insurers to spread exposure across largely independent events. Cyber risk does not work this way. Just three operating systems dominate the desktop and laptop computer market and three hyperscale cloud infrastructure-as-a-service providers have commanding market share.[19] Since the technology and services that most companies rely on are broadly identical, a single vulnerability can affect an insurer's entire book of business — millions of systems can be brought down in an instant with one replicating virus or one piece of faulty code.[20] This is accumulation risk, and it is intrinsic to how digital infrastructure is built. Private reinsurance cannot solve it either, because reinsurers face the same diversification problems, no matter the group of carriers for which they write policies.[21]

To mitigate the impact of the insurance company's risk that many policyholders will make claims at the same time, the insurer must keep more capital on hand per dollar underwritten. This constricts the number of policies they can provide with a set amount of capital, and it keeps premiums higher than they would be otherwise.

The structural nature of accumulation risk is coming into sharper relief with the emergence of AI-enabled vulnerability discovery. Frontier AI models capable of identifying and exploiting software vulnerabilities at scale can significantly compress the timeline between vulnerability discovery and financial loss. The impact can scale rapidly across organizations sharing common

---

[17] Daniel W. Woods, "Where Are the Insurance Disputes over Cyber Hygiene?" *DanielWoods.info*, March 6, 2024. (https://www.danielwoods.info/blog/2024/cyber-hygiene-exclusions)

[18] Jay Heiser, "Stop Performing Cybersecurity Theater: It Is No Longer Scaling," *Gartner Research*, January 5, 2023. (https://emt.gartnerweb.com/ngw/globalassets/en/doc/documents/779000-stop-performing-cybersecurity-theater.pdf); Guy Carpenter and Oliver Wyman, "Using data to prioritize cybersecurity investments," *Marsh McLennan*, April 11, 2023. (https://www.guycarp.com/content/dam/guycarp-rebrand/pdf/Insights/2023/Using_data_to_prioritize_cybersecurity_investments_report.pdf)

[19] Felix Richter, "Big Three Hold Dominant Lead in Accelerating Cloud Market," Statista, February 9, 2026. (https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers)

[20] *United States v. Park*, No. MJ 18-1479 (C.D. Cal. June 8, 2018) (WannaCry); "External Technical Root Cause Analysis — Channel File 291," *CrowdStrike*, August 6, 2024. (https://www.crowdstrike.com/wp-content/uploads/2024/08/Channel-File-291-Incident-Root-Cause-Analysis-08.06.2024.pdf)

[21] Henry R.K. Skeoch and Christos Ioannidis, "The barriers to sustainable risk transfer in the cyber-insurance market," *Journal of Cybersecurity*, February 20, 2024. (https://doi.org/10.1093/cybsec/tyae003)

cloud providers or infrastructure.[22] Industry analysts have noted that a single, widely exploited AI-identified vulnerability could affect thousands of organizations simultaneously, constituting what insurers describe as a "cyber catastrophe" event. These developments reinforce the case that accumulation risk cannot be priced away by private markets alone, and that it is worsening.

Accumulation risk is compounded by two additional structural challenges. Attritional risk — the chance that underwriting models mis-price cyber risk — means that insurers may charge insufficient premiums and pay more claims than expected.[23] Un-modellable risks such as state-backed attacks cannot be priced at all. War exclusions in cyber policies address this in part, but they have introduced their own complications: there is no settled case law on what constitutes an act of "cyber war" for insurance purposes, and such exclusions generate litigation risk.[24]

The Case for a Federal Reinsurance Backstop and What It Should Look Like

Federal intervention is necessary because, in the absence of sufficient actuarial data about cyber risks, the market cannot quickly develop risk models that resolve these constraints. In fact, such data may never fully materialize given the human element inherent to cyber incidents.[25] The federal government has substantially greater fiscal capacity to absorb losses than any private insurer, and it possesses a unique capacity to recoup those losses through assessments of the industry — an option unavailable to private firms.[26]

A well-designed federal reinsurance program would directly address the accumulation risk weighing on market growth, while minimally disrupting existing claims, contracts, or processes. In essence, the government would be removing a portion of the tail risk — low-probability, high-impact events — for carriers, just as traditional reinsurance does in other lines.[27] Because an insurer's aggregate claims would be effectively capped below the total coverage it underwrites, any individual policy would be cheaper to provide and require less capital to backstop. A

---

[22] Gia Snape, "How Anthropic's Mythos is fueling cyber risk aggregation fears," *Insurance Business*, April 23, 2026. (https://www.insurancebusinessmag.com/us/news/cyber/how-anthropics-mythos-is-fueling-cyber-risk-aggregation-fears-572751.aspx)

[23] Michael Georgiou, Stephan Brunner, Ed Pocock, Tim Marshall, Aidan Flynn, Henry Skeoch, Alex Jackson, Sioned Bentley, and Tim Davy, "Cyber Realistic Disaster Scenario Development and Modelling: Triple Threat," *Beazley, Gallagher Re, and Munich Re*, 2024. (https://www.munichre.com/content/dam/munichre/contentlounge/website-pieces/documents/Whitepaper-Systemic-Cyber-Insurance-Industry-Losses.pdf)

[24] Josephine Wolff, "How the NotPetya attack is reshaping cyber insurance," *Brookings Institution*, December 1, 2021. (https://www.brookings.edu/articles/how-the-notpetya-attack-is-reshaping-cyber-insurance); Tony Chaudhry, "State Backed Cyber-Attack Exclusions," *Lloyd's Market Bulletin*, August 16, 2022. (https://assets.lloyds.com/media/35926dc8-c885-497b-aed8-6d2f87c1415d/Y5381%20Market%20Bulletin%20-%20Cyber-attack%20exclusions.pdf)

[25] Ariel Levite, Scott Kanry, and Wyatt Hoffman, "Addressing the Private Sector Cybersecurity Predicament: The Indispensable Role of Insurance," *Carnegie Endowment for International Peace*, November 7, 2018. (https://carnegieendowment.org/research/2018/11/addressing-the-private-sector-cybersecurity-predicament-the-indispensable-role-of-insurance)

[26] U.S. Department of the Treasury, Bureau of the Fiscal Service, "Highlights of the FY 2020 Financial Report of the U.S. Government," last modified April 6, 2023. (https://fiscal.treasury.gov/accounting/us-financial-report/2021/results-in-brief)

[27] Baird Webel, "Terrorism Risk Insurance: Overview and Issue Analysis for the 116th Congress," *Congressional Research Service*, December 27, 2019. (https://crsreports.congress.gov/product/pdf/R/R45707)

government reinsurance program allows society to continue reaping the benefits of private risk pricing without penalizing insurers for the unique characteristics of technology risk and the absence of historical data on which to rely.

Policymakers should make the reinsurance mechanism as simple as possible. In other government insurance backstops, insurers have some retention: after a triggering event, insurers pay a portion of claims with no government reimbursement. For claims above the retention, there is coinsurance, where the carrier pays a small proportion of claims and the government pays the balance. This simple mechanism ensures that insurers have skin in the game while limiting their tail losses to the retention amount plus a fraction of the total coverage they have underwritten.[28]

A cyber reinsurance program should use this mechanism. As the program matures, Treasury should allow the program to evolve as the market does and therefore use its regulatory authority (rather than statutory requirements) to set retention amounts and coinsurance percentages.[29]

At least in the first years of the program's existence, recoupment — assessed as a surcharge on policies after a payout — would provide a better funding mechanism than prepaid premiums, which are difficult to set accurately without actuarial data.[30]

To be eligible for participation in the program, Treasury should require data sharing. Given policymakers' aspiration that insurance will drive positive cybersecurity behaviors and provide a key data source for evidence-based cybersecurity, data-sharing requirements should be built into the program from the start.[31] Validated cyber incident data is difficult to come by, and it is harder still to find such data paired with information about the cybersecurity control environment on victims' systems.[32] Victim organizations are quite reticent to share such data broadly — but one of the few places they do share, at least to some extent, is with their insurers.[33] As a condition of participation, the government should require insurers to share anonymized data at regular intervals with either the government or a designated third-party entity such as a nonprofit. That aggregate data, shared back with the broader cybersecurity community, could significantly enhance the discipline of evidence-based cybersecurity, and should not prove too onerous a burden on insurers.[34]

The program should cover currently insured risks, not new ones. Broadening coverage to include war-excluded or otherwise un-modellable risks would change the nature of the intervention

---

[28] Ibid.
[29] "Cyber Insurance: State of the Risk," *Insurance Information Institute*, February 2024. (https://www.iii.org/sites/default/files/docs/pdf/triple-i_state_of_the_risk_cyber_02062024.pdf)
[30] Baird Webel, "Terrorism Risk Insurance: Overview and Issue Analysis for the 116th Congress," *Congressional Research Service*, December 27, 2019. (https://crsreports.congress.gov/product/pdf/R/R45707)
[31] Sasha Romanosky, Lloyd Dixon, R.J. Briggs, and Henry H. Willis, "Insuring Catastrophic Cyber Risk," *RAND Corporation*, June 9, 2025. (https://www.rand.org/pubs/research_reports/RRA3817-1.html)
[32] Mariam Baksh, "Federal Contractors Argue Cyber Insurance Isn't a Safe Bet for Better Security," *Nextgov/FCW*, October 14, 2020. (https://www.nextgov.com/cybersecurity/2020/10/federal-contractors-argue-cyber-insurance-isnt-safe-bet-better-security/169231)
[33] Daniel W. Woods, Rainer Bohme, Josephine Wolff, and Daniel Schwarcz, "Lessons Lost: Incident Response in the Age of Cyber Insurance and Breach Attorneys," *USENIX*, August 2023. (https://www.usenix.org/system/files/usenixsecurity23-woods.pdf)
[34] Ibid.

entirely: instead of the government taking what insurers believe to be a modellable risk and reducing the error bars around it, the government would be requiring insurers to cover what they regard as completely un-modellable. If a government wants to provide protection against acts of cyber war, a more effective approach is to act as a carrier directly — setting premiums and paying claims — or to offer post-incident support from the General Fund, as would happen in the case of property damage due to war.[35]

Insurance companies have paid claims for attacks attributed to nation-states, but there has been some concerning backsliding in this area which policymakers should monitor and take action to ensure does not become a trend. Malicious actors in the employ of foreign governments have caused some of the more costly incidents on record, but war exclusions should be narrowly scoped and applicable only where there is a clear geographic boundary and major combat operations between states or state-like entities.[36] Infrastructure exclusions should be triggered only where there is substantial geographic disruption to an essential service. With the exception of acts of war, cyber incidents, even those with some state involvement, should continue to be covered.

TRIP as a Model and Its Key Distinctions

The United States has faced challenges with human-caused threats destabilizing insurance markets before and has addressed those challenges through government intervention. The parallels between the cyber insurance market and the terrorism insurance market that TRIP was designed to address are real. Both involve scalable attacks by malicious actors on domestic infrastructure. Both are inherently difficult to model due to their human-caused nature. Both lack deep pools of actuarial data. Like the proposed cyber reinsurance program, TRIP is a coinsurance model with a total cap on government liability. It relies on recoupment to ensure taxpayers are eventually made whole, and it aims to leverage the existing market rather than substitute bureaucratic judgment on the price of risk.[37]

There are, however, key distinctions. TRIP is predicated on reversing an exclusion: following the September 11 attacks, insurers had largely stopped offering terrorism coverage, and the Terrorism Risk Insurance Act required them to offer it again. The cyber insurance challenge is different. Cyber insurance is an active, growing market; the problem is not an exclusion of coverage but rather accumulation risk — the inability to adequately diversify a portfolio of cyber

[35] U.S. Department of the Treasury, Federal Insurance Office, "Summary of Comments on Request for Comment: Federal Insurance Response to Catastrophic Cyber Incidents," March 29, 2023. (https://home.treasury.gov/system/files/311/2023-03-27%20Presentation%20Summary%20of%20Cat%20Cyber%20RFI%20Responses.pdf)
[36] Jon Bateman, "War, Terrorism, and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions," *Carnegie Endowment for International Peace*, October 2020. (https://carnegie-production-assets.s3.amazonaws.com/static/files/Bateman_-_Cyber_Insurance_-_Final.pdf); Sean Steinberg, Adam Stepan, and Kyle Neary, "NotPetya: A Columbia University Case Study," *Columbia University School of International and Public Affairs*, November 2022. (https://www.sipa.columbia.edu/sites/default/files/2022-11/NotPetya%20Final.pdf)
[37] Baird Webel, "Terrorism Risk Insurance: Overview and Issue Analysis for the 116th Congress," *Congressional Research Service*, December 27, 2019. (https://crsreports.congress.gov/product/pdf/R/R45707)

policies — that limits capacity and raises cost. That distinction drives differences in program design.

TRIP requires every insurer to offer terrorism coverage, and the risk underlying those policies is overwhelmingly catastrophic rather than attritional: there has been no certified terrorist attack under TRIP since the program's inception, much less one reaching the loss thresholds for reinsurance to activate.[38] A cyber reinsurance program should be designed around the opposite reality: most cyber losses are attritional, occurring across the market every day, and the government backstop should activate only for the correlated, market-wide events — the grey swan catastrophes — that private capital cannot efficiently absorb. That calls for an industry-wide aggregate loss trigger rather than a certification mechanism, and a greater emphasis on data collection than TRIP requires.[39]

The biggest difference is the state of the market at inception. TRIA came at a time of crisis, when terrorism coverage had effectively vanished. Cyber insurance is not in those dire straits. Nonetheless, the time to act is now.[40]

In past congressional reauthorizations of TRIA, the issue of cybersecurity has come up, but the focus has been on whether terrorist attacks causing property damage using cyber tools would qualify for reinsurance under the existing law. Cyber terrorism is not where the bulk of the risk lies for critical infrastructure in the United States.[41]

Recommendations: What Treasury Should Do Now

Much of the analytical and design work necessary for a cyber reinsurance program falls within Treasury's existing authorities. Treasury administers TRIP, houses the Federal Insurance Office, and — in response to a Government Accountability Office recommendation[42] — has convened stakeholders to discuss program design.[43] The 2026 Effectiveness Report, due to Congress by June 30, 2026, is the right vehicle to translate that engagement into a concrete legislative recommendation.

---

[38] Ibid.
[39] "Terrorism Reinsurance," *Pool Reinsurance*, accessed May 2026. (https://www.poolre.co.uk/reinsurance)
[40] Gregory J. May, "The TRIA Cyber Risk Coverage Debate: Should Be Resolved as Part of Its Renewal," *Nelson Mullins LLP*, accessed May 2025. (https://www.nelsonmullins.com/storage/8a6a44e4523b7c75ab341dacf271523c.pdf)
[41] Nicholas Leiserson and Mark Montgomery, "Don't let Congress punt on cyber insurance reform," *CyberScoop*, November 3, 2025. (https://cyberscoop.com/congress-cyber-insurance-reform-op-ed)
[42] U.S. Government Accountability Office, "Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks," June 21, 2022. (https://www.gao.gov/products/gao-22-104256)
[43] "Catastrophic Cyber Risk and a Potential Federal Insurance Response," *Conference held at New York University Stern School of Business with Volatility and Risk Institute, New York University Stern, and U.S. Department of the Treasury, Federal Insurance Office*, November 17, 2023. (https://www.stern.nyu.edu/experience-stern/about/departments-centers-initiatives/centers-of-research/volatility-and-risk-institute/events/past-conferences/catastrophic-cyber-risk-and-potential-federal-insurance-response); U.S. Department of the Treasury, Federal Insurance Office, Itinerary, "Exploring Potential Forms of a Federal Insurance Response to Catastrophic Cyber Incidents," May 16, 2024. (https://home.treasury.gov/system/files/311/Agenda%20for%20May%2016%20cat%20cyber%20insurance%20conference%20%28final%20public%29.pdf)

Specifically, **Treasury should use the 2026 Effectiveness Report to formally recommend that Congress enact a standalone cyber reinsurance program**. The report should outline the core design parameters described above: an industry-wide aggregate loss trigger, government coinsurance above a defined insurer retention threshold, a cap on total federal liability, Treasury authority to set parameters in regulation rather than statute, and a recoupment mechanism. This recommendation would give Congress the analytical foundation it needs to act to meet the urgent cyber risks that face the nation.

Conclusion

The cyber insurance market cannot mature fast enough on its own to address the pace and scale of today's cyber threats. Accumulation risk fundamentally limits the ability of private insurers to scale coverage, and neither incremental underwriting improvements nor voluntary market development will resolve this structural constraint in the time available. The emergence of AI-enabled, vulnerability discovery tools has made this more urgent, not less.

A federal cyber reinsurance backstop offers a targeted solution: it addresses the specific market failure while preserving private insurers' role in underwriting and pricing day-to-day risk. The program design need not be complex. A coinsurance mechanism with defined retention thresholds, a liability cap, a recoupment mechanism, and mandatory data-sharing provides the essential architecture. The program should focus on currently covered risks, employ an aggregate loss trigger calibrated to small but correlated catastrophes, and maintain narrow, clearly scoped exclusions for un-modellable war risk. A backstop is a critical tool to accelerate market maturity while also helping the entire cybersecurity discipline become more data driven.

Treasury is uniquely positioned to advance this work. The 2026 Effectiveness Report is the right platform to recommend an authority for a standalone cyber reinsurance program. Congress and the administration should not let this opportunity go to waste.