United States Government Accountability Office

Report to Congressional Committees

June 2022

CYBER INSURANCE

Action Needed to Assess Potential Federal Response to Catastrophic Attacks

Accessible Version

GAO-22-104256

GAO Highlights

Highlights of GAO-22-104256, a report to congressional committees

June 2022

CYBER INSURANCE

Action Needed to Assess Potential Federal Response to Catastrophic Attacks

Why GAO Did This Study

Cyber threats to critical infrastructure represent a significant economic challenge. Although cyber incident costs are paid in part by the private cyber insurance market, growing cyber threats have created uncertainty in this evolving market.

The Further Consolidated Appropriations Act, 2020, includes a provision for GAO to study cyber risks to U.S. critical infrastructure and available insurance for these risks. This report examines the extent to which (1) cyber risks for critical infrastructure exist; (2) private insurance covers catastrophic cyber losses and TRIP provides a backstop for such losses; and (3) cognizant federal agencies have assessed a potential federal response for cyberattacks.

GAO reviewed cyber insurance coverage literature and reports on cyber risk and the insurance market. GAO interviewed CISA and FIO officials and industry stakeholders (e.g., critical infrastructure owners, insurers, and brokers) that were selected based on factors such as expertise and market share.

What GAO Recommends

CISA and FIO should jointly assess the extent to which risks to critical infrastructure from catastrophic cyber incidents and potential financial exposures warrant a federal insurance response, and inform Congress of the results of their assessment. Both agencies agreed with the recommendations.

View GAO-22-104256. For more information, contact Daniel Garcia-Diaz at (202) 512-8678 or garciadiazd@gao.gov, or Kevin Walsh at (202) 512-6151 or walshk@gao.gov.

What GAO Found

U.S. critical infrastructure (such as utilities, financial services, and pipelines) faces increasing cybersecurity risks. Understanding these risks and associated vulnerabilities, threats, and impacts is essential to protecting critical infrastructure.

Cybersecurity Vulnerabilities, Threats, and Impacts
Vulnerabilities. Critical infrastructure has become more vulnerable to cyberattacks for reasons that include greater use of interconnected electronic systems.
Threats. Threat actors—such as nation-states, criminal groups, and terrorists—have become increasingly capable of carrying out cyberattacks on critical infrastructure.
Impacts. Federal and industry data indicate that cyberattacks—including those affecting critical infrastructure—generally have increased in frequency and cost.

Source: Prior GAO reports and GAO analysis of agency and industry documentation.

The effects of cyber incidents can spill over from the initial target to economically linked firms—magnifying damage to the economy. For example, in May 2021 the Colonial Pipeline Company learned that it was the victim of a cyberattack that led to short-lived gasoline shortages.

Cyber insurance and the Terrorism Risk Insurance Program (TRIP)—the government backstop for losses from terrorism—are both limited in their ability to cover potentially catastrophic losses from systemic cyberattacks. Cyber insurance can offset costs from some of the most common cyber risks, such as data breaches and ransomware. However, private insurers have been taking steps to limit their potential losses from systemic cyber events. For example, insurers are excluding coverage for losses from cyber warfare and infrastructure outages. TRIP covers losses from cyberattacks if they are considered terrorism, among other requirements. However, cyberattacks may not meet the program's criteria to be certified as terrorism, even if they resulted in catastrophic losses. For example, attacks must be violent or coercive in nature to be certified.

The Department of the Treasury's Federal Insurance Office (FIO) and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) both have taken steps to understand the financial implications of growing cybersecurity risks. However, they have not assessed the extent to which risks to critical infrastructure from catastrophic cyber incidents and potential financial exposures warrant a federal insurance response. CISA is the primary risk advisor on critical infrastructure and FIO the federal monitor of the insurance sector. Accordingly, they are well-positioned to jointly perform such an assessment. Doing so and reporting the results to Congress can inform deliberations on whether a federal insurance response is warranted.

If such a response were deemed necessary, GAO's framework for providing federal assistance to private market participants (GAO-10-719) could help inform its design. The framework notes the need to define the problem, mitigate moral hazard (that the existence of a federal backstop could result in entities taking greater risks), and protect taxpayer interests. Consistent with these elements, any federal insurance response should include clear criteria for coverage, specific cybersecurity requirements, and a dedicated funding mechanism with concessions from all market participants.

Contents

Tables

Figure

Abbreviations

CISA	Cybersecurity and Infrastructure Security Agency
DHS	Department of Homeland Security
DOJ	Department of Justice
FBI	Federal Bureau of Investigation
FIO	Federal Insurance Office
GRU	Main Intelligence Directorate (Glavnoye razvedyvatel'noye upravleniye) [of the General Staff of the Armed Forces of the Russian Federation]
NAIC	National Association of Insurance Commissioners
ODNI	Office of the Director of National Intelligence
TRIA	Terrorism Risk Insurance Act
TRIP	Terrorism Risk Insurance Program

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

June 21, 2022

The Honorable Sherrod Brown
Chairman
The Honorable Patrick J. Toomey
Ranking Member
Committee on Banking, Housing, and Urban Affairs
United States Senate

The Honorable Maxine Waters
Chairwoman
The Honorable Patrick McHenry
Ranking Member
Committee on Financial Services
House of Representatives

Cyber threats to critical infrastructure represent a significant risk to the nation's economic stability. Recent incidents—such as the ransomware attack on Colonial Pipeline and attacks targeting health care and other essential services during the COVID-19 pandemic—illustrate the importance of preparing for future cyberattacks and their financial toll.[1] Since 1997, we have designated cybersecurity as a government-wide high-risk area.[2]

Certain hazards with the potential for catastrophic losses can limit insurers' willingness to offer coverage. For example, after the terrorist attacks on September 11, 2001, insurers generally stopped covering terrorism risk because they determined the risk of loss was unacceptably

[1]On May 7, 2021, Colonial Pipeline, a pipeline system that originates in Houston, Texas, and carries gasoline and jet fuel mainly to the southeastern United States, suffered a ransomware cyberattack that affected computerized equipment managing the pipeline. See GAO, *Colonial Pipeline Cyberattack Highlights Need for Better Federal and Private-Sector Preparedness*, infographic (Washington, D.C.: May 18, 2021). In May 2020, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency released a joint alert with the United Kingdom's National Cyber Security Centre on advanced persistent threat groups exploiting COVID-19 to target health care and essential services and collect bulk personal information, intellectual property, and intelligence. See GAO, *Cybersecurity: HHS Defined Roles and Responsibilities, but Can Further Improve Collaboration*, GAO-21-403 (Washington, D.C.: June 28, 2021).

[2]GAO, *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas*, GAO-21-119SP (Washington, D.C: Mar. 2, 2021). We expanded this area to include the protection of critical cyber infrastructure in 2003.

high, relative to the premiums they could charge. In November 2002, Congress enacted the Terrorism Risk Insurance Act of 2002 (TRIA) to help ensure the continued availability and affordability of commercial property/casualty insurance for terrorism risk and to address concerns that the lack of terrorism risk insurance could have significant effects on the economy.[3] TRIA established the Terrorism Risk Insurance Program (TRIP), administered by the Department of the Treasury, in which the federal government shares some losses with private insurers in the event of an act of terrorism certified by the Secretary of the Treasury, in consultation with the Secretary of Homeland Security and the Attorney General.

Federal policy has recognized the importance of addressing all hazards that could affect safety, national security, and the economy. Presidential Policy Directive 21, issued in February 2013, shifted the nation's focus from protecting critical infrastructure against terrorism to protecting and securing it and increasing its resilience against all hazards, including cyberattacks.[4] This directive and federal law also call for the Department of Homeland Security (DHS) to coordinate the overall federal effort to secure and protect against critical infrastructure risks.[5] As part of these responsibilities, DHS conducts critical infrastructure risk assessments to support policy making and risk-management decisions.

Some private insurance companies offer businesses and other entities cyber insurance to protect against losses stemming from cyberattacks.[6] However, growing cyber risks have created uncertainty in the evolving

[3]Pub. L. No. 107-297, 116 Stat. 2322 (2002). TRIA was reauthorized in 2005, 2007, 2015, and 2019. See Terrorism Risk Insurance Extension Act of 2005, Pub. L. No. 109-144, 119 Stat. 2660 (2005); Terrorism Risk Insurance Program Reauthorization Act of 2007, Pub. L. No. 110-160, 121 Stat. 1839 (2007); Terrorism Risk Insurance Program Reauthorization Act of 2015, Pub. L. No. 114-1, 129 Stat. 3 (2015); and Terrorism Risk Insurance Program Reauthorization Act of 2019, Pub. L. No. 116-94, 133 Stat. 2534, 3026 (2019).

[4]The nation's critical infrastructure refers to the systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of them would have a debilitating impact on U.S. security, economic stability, public health or safety, or any combination of these factors. 42 U.S.C. § 5195c(e).

[5]The Homeland Security Act of 2002 created DHS and gave the agency responsibilities for coordinating national critical infrastructure protection efforts. See generally Pub. L. No. 107-296, tit. II, 115 Stat. 2135, 2145.

[6]Cyber insurance generally refers to policies that address losses to a policyholder and losses to a policyholder's client or customer as a result of an event that jeopardizes the confidentiality, integrity, and availability of an information system.

cyber insurance market. For example, we reported in May 2021 that the limited availability of historical loss and cyber event data, lack of common definitions in policy language, and potential for cyber incidents to incur aggregated losses continue to challenge the cyber insurance industry.

In addition, we and others have raised questions about the extent to which the TRIA might help address cyber losses. For example, we previously reported that some industry participants were unsure about the likelihood of the Department of the Treasury certifying cyberattacks as acts of terrorism. This was because the department has never certified any event under TRIA and cyberattack characteristics may not readily meet the act's certification requirements.[7]

The Further Consolidated Appropriations, 2020 includes a provision for us to review overall vulnerabilities and potential costs of cyberattacks to U.S. critical infrastructure, and the adequacy of the federal backstop for terrorism risk insurance.[8] This report examines the extent to which (1) cybersecurity risks for U.S. critical infrastructure exist; (2) private insurance covers catastrophic cyber losses and TRIP provides a backstop for such losses; and (3) cognizant federal agencies have assessed a potential federal insurance response for cyberattacks. The focus of this report is cyber insurance provided to businesses and other entities and not to individual consumers.

For the first objective, we reviewed our prior work and public- and private-sector reporting on the financial harms and costs of cybersecurity incidents that affected critical infrastructure. In particular, we identified vulnerable technologies that could be attacked by reviewing our past work on critical infrastructure cybersecurity and documents from DHS' Cybersecurity and Infrastructure Security Agency (CISA) and MITRE

[7]GAO, *Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market*, GAO-21-477 (Washington, D.C.: May 20, 2021).

[8]Further Consolidated Appropriations Act, 2020, Pub. L. No. 116-94, § 502, 133 Stat. 2534, 3027 (2019). In response to the mandate, in June 2020 we provided Congressional members and staff with preliminary observations on our ongoing work. This report expands on our preliminary observations.

Corporation.[9] We developed a list of actors that could pose a threat to critical infrastructure based on our prior work and threat assessment documents from the Office of the Director of National Intelligence, National Security Agency, DHS, and the Department of Justice.[10] To identify potential impacts of cyberattacks, we reviewed our prior work on critical infrastructure cybersecurity, public- and private-sector reports, and publicly available data on past cyber incidents.[11] We also interviewed CISA officials about cybersecurity risks to critical infrastructure.

For the second objective, we reviewed insurance industry reports and other publicly available literature, and interviewed industry participants and academic researchers. We met with four insurers to obtain their perspectives on cybersecurity risks and the market for cyber insurance. We selected the four insurers in our sample based on the different types of insurance offered and their large market share. We also interviewed other industry participants, including associations representing property/casualty insurers, surplus lines insurers, and critical infrastructure operators from four selected sectors (health care, energy, communications, and financial services). The information we obtained from the industry participants and researchers may not represent the views or practices of all industry participants or researchers. To assess

[9]GAO, *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges*, GAO-21-288 (Washington, D.C.: Mar. 24, 2021); and *Electricity Grid Cybersecurity: DOE Needs to Ensure Its Plans Fully Address Risks to Distribution Systems*, GAO-21-81 (Washington, D.C.: Mar. 18, 2021). Also see Cybersecurity and Infrastructure Security Agency, *Cyber Threats to Critical Manufacturing Sector Industrial Control Systems* (Washington, D.C.: December 2021); and MITRE Corporation, "Adversarial Tactics, Techniques, and Common Knowledge (MITRE ATT&CK®)," last accessed on March 18, 2022, at https://attack.mitre.org/.

[10]Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (Washington, D.C.: Feb. 7, 2022); and National Security Agency and Cybersecurity and Infrastructure Security Agency, *NSA and CISA Recommend Immediate Actions to Reduce Exposure Across all Operational Technologies and Control Systems*, U/OO/154383-20 and PP-20-0622 (July, 2020). Also see Department of Justice, *ISIL-Linked Hacker Arrested in Malaysia on U.S. Charges* (Washington, D.C.: Oct. 15, 2015); *Indictment: Kansas Man Indicted for Tampering with a Public Water System* (Topeka, K.S.: Mar. 31, 2021); and *Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe* (Washington, D.C.: Feb. 17, 2021).

[11]For example, we reviewed publicly available reports from 2016 through 2021 that described the frequency and costs of cyberattacks—specifically, the Federal Bureau of Investigation's Internet Crime Reports, Verizon's Data Breach Investigations Reports, and an IBM Cost of a Data Breach Report. We reviewed the data for obvious errors in accuracy and completeness and determined the data were sufficiently reliable for our purposes.

the extent to which private insurance and TRIP might cover and exclude cyberattack losses, we reviewed reports by Treasury and insurance industry organizations and interviewed insurance, cyber risk, and academic stakeholders.

For the third objective, we reviewed reports on cybersecurity risks, Treasury's assessments of TRIP effectiveness, and past GAO work, including our framework for providing federal assistance to market participants. We also reviewed Treasury's data call to insurers writing terrorism coverage and associated guidance, including revisions to its 2022 data call. We interviewed Treasury and CISA officials. For more information on our scope and methodology, see appendix I.

We conducted this performance audit from March 2020 to June 2022 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Critical Infrastructure and CISA's Related Responsibilities

Critical infrastructure refers to 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.[12] These sectors rely on electronic systems and data to support their missions.

[12]42 U.S.C. § 5195c(e). See *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001* (*USA PATRIOT Act*).

Figure 1: Examples of Critical Infrastructure

Source: (L to R) anekoho/stock.adobe.com, Sergiy Serdyuk/stock.adobe.com, yelantsevv/stock.adobe.com, Federico Rostagno/stock.adobe.com. | GAO-22-104256

CISA, within DHS, is the lead federal agency for coordinating efforts to understand and manage risks to critical infrastructure. Since the passage of the Cybersecurity and Infrastructure Security Agency Act of 2018, CISA's National Risk Management Center has led the agency's risk-identification and analysis functions.[13] In particular, the center performs risk assessments, modeling, and data management to understand crosscutting critical infrastructure risks and support policy making, process enhancements, and risk-management decisions.

Cyber Insurance and Treasury's Related Responsibilities

Some insurance companies offer businesses cybersecurity coverage, or cyber insurance, to share the risk of losses from an event that jeopardizes the confidentiality, integrity, and availability of an information system. The insurance can be provided through a stand-alone policy with only cyber coverage or as a part of a packaged policy with multiple types of coverage. Cyber insurance coverage is available for both first-party (policyholder) and third-party liability losses (policyholder's clients or customers).[14] According to data from NAIC, cyber insurance coverage represents less than 1 percent of the premiums written in the property and casualty insurance market.

[13]Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115-278, § 2, 132 Stat. 4168, 4169 (codified as amended at 6 U.S.C. § 652).

[14]Admitted, captive, and surplus line insurers offer cyber insurance. Admitted insurers are licensed or admitted in a state as a prerequisite for selling property/casualty insurance products. Captive insurers are wholly owned and controlled by those they insure. Surplus line insurers serve as an alternative marketplace: they are nonlicensed or non-admitted domestic and foreign insurers that provide coverage for exposures not readily available from the admitted market. Reinsurers, or insurers of insurers, are also involved in this market; insurers passed on approximately 35—45 percent of cyber coverage premiums they wrote to reinsurers, as reported in 2021 by ratings company S&P Global Ratings.

In the United States, the states and territories are the primary regulators of the business of insurance, including for cyber insurance. The regulators seek to ensure that insurance policy provisions comply with state law, are reasonable and fair, and do not contain major gaps in coverage that might be misunderstood by consumers and leave them unprotected.

The Federal Insurance Office (FIO) was established in Treasury by the Dodd-Frank Wall Street Reform and Consumer Protection Act. The office is headed by a director appointed by the Secretary of the Treasury. Among other things, FIO monitors all aspects of the insurance industry (including by identifying issues or gaps in insurance regulation that could contribute to systemic risk in the insurance industry) and helps develop federal policy on prudential international insurance matters, but is not an insurance supervisor. The office also serves as an information resource for the federal government and coordinates with federal regulators, state insurance regulators, and the National Association of Insurance Commissioners (NAIC); and FIO is authorized to collect information on and from the insurance industry. The FIO Director (appointed by the Secretary of the Treasury) is a non-voting member of the Financial Stability Oversight Council. FIO also represents the United States in the International Association of Insurance Supervisors and coordinates federal efforts on international prudential insurance matters. FIO assists the Secretary of the Treasury in the administration of TRIP, created under TRIA.

Terrorism Risk Insurance Act

The purpose of TRIA is to (1) protect consumers by addressing market disruptions and ensuring the continued widespread availability and affordability of commercial property/casualty insurance for terrorism risk; and (2) allow for a transitional period for private markets to stabilize, resume pricing of such insurance, and build capacity to absorb any future losses, while preserving state insurance regulation and consumer protections. TRIA requires insurers to make terrorism coverage on certain lines of property/casualty insurance (such as fire, workers compensation, and liability) available to commercial policyholders (such as businesses) but does not require the policyholders to buy it.

TRIA requires Treasury to administer TRIP, in which the federal government shares some losses with private insurers in the event of a certified act of terrorism. The federal government does not collect an up-

front charge from insurers.[15] However, under TRIA the government may recoup at least some of its losses following a certified act of terrorism, as discussed below.

For insurers to start submitting claims and receiving payments to partially reimburse losses under terrorism coverage, Treasury must first certify an event as an act of terrorism under TRIA. Certification requires the Secretary of the Treasury to evaluate the event and determine that it meets all requirements for two criteria:

- **Nonmonetary definition:** The event would have to be determined to have been (1) "committed by an individual or individuals as part of an effort to coerce the civilian population of the United States or to influence the policy or affect the conduct of the United States Government by coercion"; (2) a "violent act or an act that is dangerous" to human life, property, or infrastructure; and (3) have resulted in damage within the United States or in certain defined areas outside the United States.[16] As part of this determination, the Secretary of the Treasury must consult with the Attorney General and Secretary of the Department of Homeland Security before certifying an event.
- **Monetary (loss) threshold:** The event would had to have caused at least $5 million in insurance losses in TRIA-eligible lines of insurance. TRIA prohibits the Secretary of the Treasury from certifying acts of terrorism unless insurance losses exceed this threshold.

To date, the federal government has not incurred financial liabilities (no act has been certified), but the program could require large, previously unbudgeted expenditures by the government if such an event occurred.

Finally, an individual insurer seeking reimbursement for losses resulting from a certified act of terrorism must satisfy a deductible to be eligible for federal payments. After the insurer pays its deductible, the government reimburses the insurer for 80 percent of its additional losses. Annual

[15]We reported in 2019 that the federal government has multiple programs that can provide compensation to specific third parties if they suffer certain losses from future adverse events and may not always charge premiums for accepting this risk of loss. GAO, *Fiscal Exposures: Federal Insurance and Other Activities That Transfer Risk or Losses to the Government*, GAO-19-353 (Washington, D.C.: Mar. 27, 2019).

[16]The act must not be part of the course of a war declared by Congress, except for workers' compensation claims.

coverage for losses is capped—neither private insurers nor the federal government cover aggregate industry insured losses above $100 billion.

U.S. Critical Infrastructure Faces Growing and Significant Cybersecurity Risks

U.S. critical infrastructure faces significant cybersecurity risks. This infrastructure is becoming more vulnerable to cyberattacks and threat actors have become increasingly capable of exploiting these vulnerabilities to carry out such attacks. These attacks generally have increased in frequency and cost, and recent attacks illustrate the potential for systemic cyber incidents.

Critical Infrastructure Has Become More Vulnerable to Cyberattacks

Key cybersecurity risks to U.S. critical infrastructure include its increasing vulnerability to cyberattacks. Systems and networks supporting critical infrastructure are composed of, and connected to, enterprise IT systems and industrial control systems.[17] These systems provide numerous benefits to critical infrastructure owners and operators. However, they are also vulnerable to cyberattacks for reasons including their complexity and interconnections with other systems (see table 1).

[17]Enterprise IT systems encompass traditional IT computing and communications hardware and software components that may be connected to the internet. Industrial control systems monitor and control sensitive processes and physical functions, such as the opening and closing of circuit breakers on the grid.

Table 1: Technology Used by Critical Infrastructure and Associated Vulnerabilities

Technology	Technology description	Vulnerabilities
Enterprise IT systems	Traditional IT computing and communications hardware and software components that may be connected to the internet.	The complexity of enterprise IT systems—including their diverse technology and geographic dispersion—increases the difficulty of identifying, managing, and protecting the numerous operating systems, applications, and devices comprising the systems and networks. Compounding the risk, systems and networks used by critical infrastructure also are often interconnected with other internal and external systems and networks, including the internet.
Industrial control systems	Vital systems that monitor and control sensitive processes and physical functions, such as the opening and closing of circuit breakers on the grid.	Increased access to industrial control systems, particularly through remote means and connections to enterprise IT systems, offers benefits to system operators, such as easier maintenance and more detailed systems data, but also make these systems more vulnerable to cyberattacks. Industrial control systems often rely on older legacy components that were not designed with cybersecurity protections. Systems components often must be taken offline so that owners and operators can apply security patches to address known cybersecurity vulnerabilities. However, this may not happen in a timely manner for certain sectors (such as the energy sector) because the devices must remain highly available to support critical functions (reliable operation of the grid).

Source: GAO. | GAO-22-104256

In addition, critical infrastructure owners and operators continue to expand their use of these systems. For example, according to CISA, the COVID-19 pandemic has led critical infrastructure entities to increase their use of remote-based technologies for industrial control systems. This has in turn created a larger “attack surface”—that is, more points in a network that attackers can try to enter. Thus, these systems are more vulnerable to cyberattacks.

Cyber adversaries use a variety of tactics and techniques to exploit vulnerabilities and attack these systems. According to MITRE’s ATT&CK® Framework—a cybersecurity knowledgebase of adversary tactics and techniques—-attackers tend to follow common methodologies to compromise targets and achieve their goals. Appendix II includes additional information about cyberattack tactics and techniques associated with enterprise IT and industrial control systems.

Cyber Threat Actors Have Become Increasingly Capable of Attacking Critical Infrastructure

Key cybersecurity risks to U.S. critical infrastructure also include the growing attack capabilities of threat actors. These threat actors include nation-states—particularly China, Russia, Iran, and North Korea—and nonstate actors—criminal groups, hackers and hacktivists, insiders, and terrorists.[18]

- **Nation-States.** These actors include groups or programs sponsored or sanctioned by nation-states that use cyber tools as part of their information-gathering and espionage activities (see app. III). According to the *2022 Annual Threat Assessment of the U.S. Intelligence Community*, China, Russia, Iran, and North Korea pose the greatest cyberattack threats to the nation's critical infrastructure.[19] For example, CISA has warned that Russia's invasion of Ukraine could affect organizations both within and beyond the region, to include the United States, and that every organization must be prepared to respond to disruptive cyber activity.
- **Nonstate actors.** Criminal groups, hackers and hacktivists, insiders, and violent extremists also pose a threat (see app. IV). These actors have a range of capabilities—from those that use existing tools to exploit known vulnerabilities to organized criminal actors who are highly technical and well-funded professionals working in teams to discover and use new means of attack. In particular, the 2022 *Annual Threat Assessment of the U.S. Intelligence Community* noted that, of nonstate actors, criminal groups pose the greatest cyberattack threat to the United States.

In addition, threat actors are becoming increasingly capable of conducting damaging cyberattacks. For example, hackers and hacktivists no longer need a great amount of skill to compromise IT systems because of the growing availability of public and commercial cyberattack tools. Additionally, in 2022, the Federal Bureau of Investigation (FBI) observed that several ransomware groups developed code designed to stop critical

[18]China is officially referred to as the People's Republic of China. We refer to it as China in this report. North Korea is officially referred to as the Democratic People's Republic of Korea. We refer to it as North Korea in this report. Hacktivists are ideologically motivated actors who use cyber exploits to further political goals.

[19]*Annual Threat Assessment of the U.S. Intelligence Community* (February 2022).

infrastructure or industrial processes. Furthermore, threat actors may become even more capable—particularly with advances in artificial intelligence.[20]

Moreover, according to the National Security Agency and CISA, cyber threat actors have demonstrated their willingness to conduct cyberattacks against critical infrastructure.[21] Those agencies added that civilian infrastructure is an attractive target for foreign powers attempting to harm U.S. interests or retaliate for perceived U.S. aggression. Notably, in March 2022, the President issued a written statement warning that the Russian government was exploring options for potential cyberattacks and the Deputy National Security Advisor for Cyber and Emerging Technologies explained those cyberattacks may be aimed at the nation's critical infrastructure.[22]

Cybersecurity Incidents Have Multiplied and Future Incidents Could Have Devastating Impacts

Cyber Incidents Generally Increased in Frequency and Cost

Although federal agencies do not have a comprehensive inventory of cybersecurity incidents, several key federal and industry sources show (1) an increase in most types of cyberattacks across the United States—including those affecting critical infrastructure, and (2) significant and increasing costs for cyberattacks.[23]

[20]According to the National Security Commission on Artificial Intelligence, the expanding application of existing artificial intelligence capabilities will make cyberattacks more precise and tailored, further accelerate and automate cyber warfare, enable stealthier and more persistent cyber weapons, and make cyber campaigns more effective on a larger scale. The National Security Commission on Artificial Intelligence, *Final Report* (March 2021).

[21]*NSA and CISA Recommend Immediate Actions to Reduce Exposure Across all Operational Technologies and Control Systems* (July 2020).

[22]White House, *Statement by President Biden on our Nation's Cybersecurity*, March 21, 2022; and *Press Briefing by Press Secretary Jen Psaki and Deputy NSA for Cyber and Emerging Technologies Anne Neuberger*, March 21, 2022.

[23]In a written response, CISA stated that it generally does not have unclassified data that describe the prevalence of types of cyberattacks by sector. CISA explained that the voluntary nature of information gathering from sector partners complicates the availability of information generally, and the applicability and utility of available information.

- **Increase in frequency.** According to the FBI, some of the most common and damaging types of cyberattacks result in incidents involving business email compromise, data breaches, denial of service, and ransomware. The FBI noted an increase in cybersecurity incidents across the four most common types of cybersecurity incidents in the past 4 years—from 19,060 in 2016 to 26,074 in 2021 (see table 2).[24] CISA, the National Security Agency, Australia, and the United Kingdom observed an increase in sophisticated, high-impact ransomware incidents against critical infrastructure entities globally in 2021.[25]

  In addition, certain industry sources indicate that the four most common types of cyber incidents have been increasing in frequency.[26] For example, Verizon reported that data breaches nearly doubled in recent years, increasing from 2,260 in 2016 to 5,258 in 2021. Further, CrowdStrike Intelligence, a cybersecurity organization, observed an 82 percent increase in ransomware-related data breaches from 2020 to 2021.[27]

- **Significant and increased costs.** Costs associated with cybersecurity incidents—both to the overall economy and to affected organizations—are significant. However, cost estimates for these incidents vary widely. For example, in 2018 the Council of Economic Advisers estimated that malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016.[28] According to a 2018 RAND report, cyber incidents could have cost the economy

[24]Although the FBI encourages organizations to report all incidents to the FBI, not all do so. As such, these data do not reflect all cybersecurity incidents that affect U.S. organizations.

[25]Cybersecurity and Infrastructure Security Agency, *2021 Trends Show Increased Globalized Threat of Ransomware*, AA22-040A (Washington, D.C.: February 2022).

[26]In a written response, CISA explained that the increase in cyber incidents may be partially attributed to organizations' improvements in detecting incidents.

[27]Crowdstrike, *2022 Global Threat Report.* Data breaches can occur when criminal groups steal an organization's data as part of a ransomware attack and threaten to make the data publicly available unless the victim organization pays a ransom.

[28]The Council based this estimate on changes in company stock prices following cyber incident disclosures. According to the report, a cyberattack typically triggers a range of immediate and relatively easily observable costs that include expenditures on forensics, cybersecurity improvements, data restoration, and legal fees. Council of Economic Advisers, *The Cost of Malicious Cyber Activity to the U.S. Economy* (Washington, D.C.: Feb. 16, 2018).

more than $242 billion per year.[29] A 2020 CISA study, based on data from several datasets published in 2015–2020, reported that the median cost of a cyber incident to a U.S. organization might range from $56,000 to $1.7 million.[30]

FBI data indicate that costs across the most common types of cybersecurity incidents increased from $470 million in 2016 to more than $2.5 billion in 2021. The average cost of these incidents also increased from $26,000 to $100,000 in the same time period (see table 2).[31] For example, although the frequency of data breaches decreased since 2016, the average cost of a data breach to an organization increased more than fourfold from 2016 to 2021 (from $28,000 to $118,000). Of the most common types of cybersecurity incidents, only denial-of-service and distributed-denial-of-service incidents decreased in average cost from 2016 to 2021.

Federal and industry data also indicate that the costs of cyber incidents generally have been increasing. For example, IBM reported that the average total cost of a data breach grew from $4 million in 2016 to $4.24 million in 2021.[32] Additionally, Treasury reported that in 2020, ransomware payments reached over $400 million, more than four times the level in 2019.[33] Further, Treasury's Financial Crimes Enforcement Network reported that the total value of suspicious

[29]Paul Dreyer, et al., *Estimating the Global Cost of Cyber Risk: Methodology and Examples* (Santa Monica, Calif.: RAND Corporation, 2018). Accessed at https://www.rand.org/pubs/research_reports/RR2299.html.

[30]Cybersecurity and Infrastructure Security Agency, *Cost of a Cyber Incident: Systematic Review and Cross-Validation* (Washington, D.C. Oct. 26, 2020). The reported estimates from the studies analyzed by CISA vary widely based on the assumptions and estimated methods used. Also see NetDiligence, *NetDiligence 2017 Cyber Claims Study* (2017); and Christian Biener, Martin Eling, and Jan Hendrik Wirfs, "Insurability of Cyber Risk: An Empirical Analysis" *Geneva Papers on Risk and Insurance*, vol. 40, no. 1 (2015): 131-158.

[31]As previously mentioned, the voluntary nature of information gathering from sector partners complicates the availability, applicability, and utility of that information. Accordingly, CISA does not collect costs incurred by victims and did not have information on trends in the costs of cyberattacks.

[32]IBM includes direct expenses (such as engaging forensic experts, outsourcing hotline support, and providing customers with free credit-monitoring subscriptions) and indirect costs (including in-house investigations and loss of customers) in its calculation of the average total cost of a data breach.

[33]Treasury, *Treasury Takes Robust Actions to Counter Ransomware*, September 21, 2021, accessed June 6, 2022, https://home.treasury.gov/news/press-releases/jy0364.

activity during the first 6 months of 2021 was $590 million, which exceeds the value reported for the entirety of 2020 ($416 million).[34]

Table 2: Frequency, Total Costs, and Per-Incident Costs of the Most Common Types of Cybersecurity Incidents According to the FBI, 2016-2020

Dollars in millions

	FBI's reported cybersecurity incidents	2016 incidents			2021 incidents		
Type	**Description**	**Quantity**	**Total cost**	**Cost per incident**	**Quantity**	**Total cost**	**Cost per incident**
Business email	A scam that involves compromising email accounts to conduct unauthorized transfer of funds.	12,005	**360.514**	0.030	19,954	**2,395.953**	0.120
Data breach	An unauthorized or unintentional exposure, disclosure, or loss of an organization's sensitive information.	3,403	**95.870**	0.028	1,287	**151.568**	0.118
Denial of service and distributed denial of service	An attack that prevents or impairs use of networks, systems, or apps. The distributed variant uses numerous hosts to perform the attack.	979	**11.214**	0.011	1,104	**0.218**	0.000
Ransomware	A type of malware used to deny access to IT systems or data and hold systems or data hostage until a ransom is paid.[a]	2,673	**2.431**	0.001	3,729	**49.208**[b]	0.013[b]
Total		**19,060**	**470.029**	**0.025**	**26,074**	**2,596.947**	**0.100**

Source: Prior GAO reports and GAO analysis of Federal Bureau of Investigation (FBI) reports. | GAO-22-104256

[a]Malware is software or code intended to damage or disable computers and computer systems.

[b]This number does not include estimates of lost business, time, wages, files, or equipment, or any third-party remediation services acquired by a victim, according to the FBI. In some cases, victims do not report any loss amount to the FBI, thereby creating an artificially low overall ransomware loss rate. Lastly, the number only represents what victims report to the FBI via the IC3 system and does not account for victim direct reporting to FBI field offices/agents.

[34]Financial Crimes Enforcement Network, *Financial Trend Analysis: Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021,* 2021. Retrieved from https://www.fincen.gov/news/news-releases/fincen-issues-report-ransomware-trends-bank-secrecy-act-data.

Recent Attacks Illustrate the Potential for Systemic Cyber Incidents

Recent attacks illustrate that the effects of cyber incidents can spill over from the initial target to economically linked firms—thereby magnifying the damage to the economy (see sidebar). For example:

NotPetya

In June 2017, the Main Intelligence Directorate of the General Staff of the Armed Forces of the Russian Federation (commonly known as the GRU) conducted the "NotPetya" malware attacks. Specifically, the GRU compromised the development environment of a Ukrainian company that produces tax accounting software to deploy malware on systems where the software was installed. After NotPetya infected a machine on which that software was installed, it was capable of automatically spreading through a network and infecting other machines. NotPetya spread worldwide, damaged computers used in critical infrastructure, and is estimated to have caused about $10 billion in damages globally.

Source: Department of Justice and Department of Homeland Security | GAO 22 104256

- In May 2021, the Colonial Pipeline Company learned that it was the victim of a ransomware attack against its IT network. As a safety measure, the company disconnected certain industrial control systems, resulting in a temporary halt to all pipeline operations. This in turn led to short-lived gasoline shortages throughout the southeast United States.
- In July 2021, Kaseya—a provider of IT and security management solutions for managed service providers and small- to medium-sized businesses—reported that its tools were compromised and used to conduct ransomware attacks that affected about 1,500 organizations.
- In February 2022, Viasat, Inc. began experiencing outages with its European satellite internet service near the start of the Russian invasion of Ukraine, according to press reporting. According to Viasat, the disruption was triggered by an attacker running destructive commands against Viasat network devices. In its forensic analysis of the incident, Sentinel Labs noted that the malware used in this attack shares some similarities with malware used in attacks attributed to the Russian government. As a result of the attack, a German wind turbine manufacturer explained that remote operation of more than 5,000 turbines had been affected. In March 2022, CISA and the FBI warned critical infrastructure and other organizations of possible threats to U.S. and international satellite communication networks.

These examples illustrate the potential for future systemic cyber incidents—that is, the possibility that a single cyber incident could ripple

across critical infrastructure with catastrophic consequences.[35] Although the severity of these incidents pales in comparison to the severity of noncyber systemic events (such as the COVID-19 pandemic or the 2008 financial crisis), they could have been much more damaging than they were. For example, had the gasoline shortages caused by the Colonial Pipeline incident lasted longer, they could have had cascading effects on other sectors, with potentially devastating consequences.

We previously warned that future cyber incidents could result in systemic risks for the United States. For example, in March 2021, we highlighted the rapidly evolving and grave cyber threats to the country and their consequences.[36] In September 2020, we noted that a successful cyberattack with systemic effects could erode public confidence in financial institutions, deny businesses and individuals access to their funds, result in the loss of funds, or affect the integrity of financial information.[37]

Cyber Insurance and TRIA Are Limited in Their Ability to Cover Systemic Cyber Incidents

Cyber insurance provides coverage for common cyber risks to help companies mitigate losses related to cyber incidents and can encourage policyholders to manage cyber risk. But cyber insurers have been limiting their exposure to systemic losses (including by limiting coverage), and the

[35]Bateman, et. al, *Systemic Cyber Risk: A Primer* (Carnegie Endowment for International Peace and the Aspen Institute: Washington, D.C., 2022). Although there is not a commonly accepted definition for systemic cyber incidents, this definition, offered by the authors of this report broadly covers other definitions offered by the cybersecurity and insurance industries. For example, the report reviews CISA's definition, which is as follows: "Systemic risk occurs when risk is spread across interdependent systems so that a failure of one component has consequences system wide, amplifying the impact of the incident. In this context, [CISA] is looking to identify and understand the ways that cyber risks or incidents in individual pieces or components of critical infrastructure or National Critical Functions could create far-reaching cascading impacts, leading to system-wide functional degradation or failure." CISA, *Systemic Cyber Risk Reduction Venture*, https://www.cisa.gov/sites/default/files/publications/FS_Systemic-Cyber-Risk-Reduction_508.pdf, last accessed on May 23, 2022.

[36]GAO, *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges*, GAO-21-288 (Washington, D.C.: Mar. 24, 2021).

[37]GAO, *Critical Infrastructure Protection: Treasury Needs to Improve Tracking of Financial Sector Cybersecurity Risk Mitigation Efforts*, GAO-20-631 (Washington, D.C.: Sept. 17, 2020).

cyber insurance market may not fully cover losses from a systemic event with catastrophic losses. Moreover, while cyber incidents could be covered under TRIP, certifying these incidents as acts of terrorism could be challenging.

Cyber Insurance Covers Common Cyber Losses and Can Incentivize Cyber Resilience

Cyber insurance generally covers costs associated with the following common cyber risks:

- **Breaches.** Cyber policies generally cover costs related to data and security breaches, such as notification expenses, data restoration, forensic investigation, and credit monitoring. One example of a recent data breach against a U.S. critical infrastructure operator is the 2021 attack against T-Mobile (a communications operator). The company reported in August of 2021 that unauthorized individuals accessed the personal information—including Social Security numbers and names—of more than 47 million current, former, and prospective customers and that insurance may cover some of the costs related to this event, such as notification and customer service expenses.
- **Ransomware.** Cyber policies generally cover incident response expenses and extortion costs related to ransomware attacks. The attack against the Colonial Pipeline announced in May 2021 is an example of a recent ransomware attack against the nation's critical infrastructure. In June 2021, Colonial's President and Chief Executive Officer testified before the House Committee on Homeland Security that the company's insurance was expected to cover the $4.4 million ransom paid to the perpetrators.[38] As of June 2021, ransomware was involved in 75 percent of all cyber insurance claims, according to AM Best.
- **Business interruption.** Cyber policies generally cover costs related to business interruption resulting from a cyberattack, including loss of income and expenses that exceed those from normal business

[38]House Committee on Homeland Security, *Cyber Threats in the Pipeline: Using Lessons from the Colonial Ransomware Attack to Defend Critical Infrastructure, 117th* Cong. (2021); statement of Joseph Blount, President and Chief Executive Officer, Colonial Pipeline.

operations.[39] Any number of cyber incidents, including ransomware, can interrupt the normal operations of a business and trigger an insurance claim. According to Allianz, a global insurer, business interruption losses are the main driver behind cyber losses, accounting for over 50 percent of the losses on the insurer's cyber-related claims from January 2015 through June 30, 2021.[40]

In addition to covering costs associated with common risks, cyber insurance can encourage policyholders to manage their cyber risk and increase cyber resilience, according to several government entities and researchers.[41] Fitch Ratings told us that because insurers may include a cybersecurity risk assessment during the underwriting process, companies generally will work to mitigate their cyber risks before they purchase coverage to obtain more favorable pricing. Some government entities and researchers also have noted that the insurance market can encourage implementation of cybersecurity best practices by linking premiums with the policyholder's cybersecurity practices.

However, there is no standard cybersecurity risk assessment across providers or for all insureds, and some assessments are more comprehensive than others. For example, NAIC told us that insurers generally require less cybersecurity information from smaller companies than larger companies. According to a report by the Royal United Services Institute, a British security think tank, insurers conduct risk assessments to collect information such as the business' size and geography, security controls, and incident history.[42] However, the report notes differences in the breadth and depth of the risk assessments, depending on a business' size. For example, smaller businesses may only be required to answer a short questionnaire of as few as four questions, while larger businesses may be subject to a more robust assessment that includes site visits, interviews, and examination of hardware. According to the insurance firm Gallagher and other market

[39]According to insurance firm Gallagher, business interruption can take place when a company's network goes down or is significantly impaired for a sustained period.

[40]Allianz Global Corporate & Specialty, *Cyber Insights: Ransomware Trends: Risks and Resilience* (Munich, Germany: October 2021).

[41]In contrast, some security researchers have suggested that the cyber insurance industry's coverage of ransomware payments has encouraged criminal organizations to engage in more ransomware attacks.

[42]Jamie MacColl, Jason R. C. Nurse, and James Sullivan, *Cyber Insurance and the Cyber Security Challenge* (London, U.K.: Royal United Services Institute, June 2021).

participants, risk assessment protocols have been evolving as underwriting guidelines grow more stringent in response to the growing cyber risk.

Insurers Have Been Limiting Their Exposure to Systemic Losses

Insurers have been limiting their exposures to systemic losses from cyber incidents. As previously noted, the consequences of cyberattacks could spread to linked entities, causing systemic and potentially catastrophic losses. The risk of a systemic event is difficult for insurers to evaluate in part because of the large number of widely used software and hardware platforms, according to global think tank, EastWest Institute. It is also challenging for the insurance market to determine its financial exposure to this type of loss, according to insurance experts we met. Consequently, losses associated with a systemic event could be beyond what the insurance industry can cover.

To help limit their exposure to systemic losses under cyber coverages, insurers can reduce their exposure through

- **Lower policy limits.** Treasury officials told us that some insurers have reduced limits for cyber coverage, which reduces the insurers' loss exposure. According to several industry participants, the cyber insurance coverage available in 2021 had significantly lower limits than previously available. For example, the Council of Insurance Agents & Brokers reported that cyber insurance carriers reduced limits from $10 million to about $5 million in the second quarter of 2021.[43] These reduced limits protect insurers from large, aggregated losses in the case of a widespread attack, but could leave policyholders lacking in coverage. Insurers also have begun adding sub-limits and coinsurance related to ransomware claims to further

[43]The Council of Insurance Agents & Brokers, *Commercial Property/Casualty Market Index: Q2/2021* (Washington, D.C.: 2021).

limit coverage, according to two brokers and the Council of Insurance Agents & Brokers.[44]

- **Higher premium rates.** Many insurers also have increased premium rates in response to increasing losses. Various sources show considerable increases in cyber insurance premium rates in the past year. For example, according to NAIC, premiums increased 29 percent in 2020, and the Council of Insurance Agents & Brokers reported a more than 34 percent increase in cyber premium rates from the third to the fourth quarter of 2021.[45]
- **Exclusions for potential systemic events.** Insurance policies generally exclude losses from events with potential catastrophic and systemic effects, such as acts of war.[46] Cyber insurers also have been taking steps to reduce their exposure to systemic cyber events. For example, in November 2021, Lloyd's Market Association introduced specific exclusions for cyber war, and, according to media reports, at least one other large insurer is planning to adopt similar exclusions.

  Other exclusions also may limit insurers' exposure in the case of a systemic cyber event. For example, some cyber insurers exclude losses from outages of critical infrastructure services that are not under the control of the policyholder. Systemic losses can result from outages of electric utilities and telecommunications, including electrical or mechanical failures; any electrical power interruption, surge, brownout, or blackout; and any failure of telephone lines, data transmission lines, and other telecommunications or networking

[44]According to Corvus Insurance, sublimits refer to limitations on how much coverage is available for a specific type of loss. For example, a policy may have an overall limit of $100,000 in coverage but may limit ransomware coverage to $50,000. Coinsurance requires policyholders to share a defined percentage of the claim cost with the carrier. For example, a policy can stipulate that a policyholder must pay a certain percentage of a ransomware claim. The Council of Insurance Agents & Brokers, *Commercial Property/Casualty Market Index: Q4/2020* (Washington, D.C.: 2021).

[45]The Council of Insurance Agents & Brokers, *Commercial Property/Casualty Market Index: Q4/2021* (Washington, D.C.: 2022). The Council also reported this was the first time after September 11, 2001, that premiums for a line of business increased more than 30 percent.

[46]According to Carnegie, acts of war, including cyber war, can have cascading consequences across entire systems. One federal statutory definition of "act of war" is any act occurring in the course of (1) declared war; (2) armed conflict, whether or not war has been declared, between two or more nations; or (3) armed conflict between military forces of any origin. 18 U.S.C. § 2331(4); however, contractual definitions of "act of war" vary. "Act of war" exclusions are generally found in policies issued in most lines of insurance, including cyber.

infrastructure. These events can spread to multiple systems, disrupting businesses and supply chains. They also can pose a risk of accumulated losses that are challenging for insurers to manage, according to some researchers and government entities.

In addition, cyber policies may exclude losses from physical damage. According to the World Economic Forum, cyberattacks on critical systems can have cascading physical consequences.[47] Furthermore, the President's National Infrastructure Advisory Council has identified cyber-physical attacks—a cyberattack that affects the physical environment—as a threat against the national power grid.[48]

- **Limiting coverage for critical infrastructure sectors.** Some carriers may specifically limit the coverage they offer to certain critical infrastructure sectors, according to EastWest Institute and two insurers.[49] Cyberattacks against critical infrastructure operations have the potential for widespread harm. One insurer told us it opted not to insure the energy sector because (1) energy operations can be attacked in multiple ways, and (2) because it is concerned that energy operators do not follow robust cybersecurity protocols.[50] Another insurer said that its appetite to provide coverage to certain industries—including electric grid operators and airlines—is limited. However, the extent to which insurers have begun limiting or excluding critical infrastructure operators from coverage is unclear; critical infrastructure operators told us that to date, they have not had difficulty obtaining coverage.

The extent to which these steps by insurers have contributed to limited availability in the cyber insurance market remains uncertain. According to NAIC, the cyber insurance market continues to grow, with a 29 percent increase in premiums collected in 2020, compared with 2019. However, according to industry sources and academics, increasing risks of

[47]World Economic Forum, *The Global Risks Report 2022,* 17th ed. (Geneva, Switzerland: Jan. 11, 2022).

[48]The President's National Infrastructure Advisory Council, *Surviving a Catastrophic Power Outage: How to Strengthen the Capabilities of the Nation* (Washington, D.C.: December 2018).

[49]EastWest Institute, *Cyber Insurance and Systemic Market Risk* (New York City, New York:2019).

[50]According to AON's 2021 Cyber Risk Report, the average energy, utilities, or natural resources organization has only a basic level of cybersecurity maturity and lacks formalized risk management.

aggregated losses has resulted in lower coverage limits. In addition, in January 2022, Gallagher noted that while there has not been an exodus of insurers from the cyber market, concerns about systemic exposures led them to lower limits in 2021.[51] If rising risks of aggregated losses and concerns about systemic exposures from cyber events lead insurers to further limit coverage and increase premiums, critical infrastructure operators may find themselves lacking coverage and unable to continue operations in the wake of a catastrophic cyberattack.

Furthermore, it is uncertain whether, as aggregated losses from systemic cyberattacks become an increasing risk, insurers will begin to consider such attacks to be uninsurable. Generally, commercial insurance works by pooling risk from limited and randomly occurring events and distributes the associated expected costs over a large pool of policyholders. The reinsurance market facilitates this risk distribution, pooling the risk over the global financial markets. But the commercial insurance model does not work well for events like systemic cyberattacks, where the effects could be widespread without a clear maximum, affecting millions of policyholders globally.

We previously reported that certain risks, such as nuclear, biological, chemical, and radiological risks, may not be insurable because of the (1) potential for catastrophic losses, (2) a lack of knowledge about long-term consequences, and (3) a lack of historical experience with such attacks in the United States.[52] Similarly, measuring and predicting systemic cyber risks that result in catastrophic losses may present a distinct challenge to insurers and the insurance market might be unable or unwilling to provide very large amounts of coverage for certain risks that are hard to estimate or might never have occurred before.

TRIA Backstop Designed for Terrorism, Not Readily Applicable to Cyberattacks

TRIP covers terrorism losses on eligible policies. To be eligible for the program, a policy's terrorism coverage must not differ materially from the terms, amounts, and other coverage limitations applicable to losses

[51]Gallagher, *Cyber Market Conditions: January 2022* (January 2022).

[52]GAO, *Terrorism Insurance: Measuring and Predicting Losses from Unconventional Weapons Is Difficult, but Some Industry Exposure Exists*, GAO-06-1081 (Washington, D.C.: Sept. 25, 2006).

arising from other events. However, policyholders can decline the coverage if offered.[53] Treasury issued a final rule in 2021 clarifying that TRIP can cover terrorism losses on eligible cyber policies.[54] Among policyholders with cyber policies written in TRIP-eligible lines of insurance, 56 percent elected to purchase terrorism coverage in 2020, according to Treasury's 2021 TRIP report.[55]

However, because TRIA was designed specifically as a federal backstop for losses from acts of terrorism, only losses from cyberattacks certified by Treasury as acts of terrorism would have TRIA coverage. As a result, even very large cyberattacks to the nation's critical infrastructure that could result in catastrophic losses and risk to national security (even if covered for terrorism under TRIP-eligible cyber policies) would not be covered under TRIA if they are not certified as acts of terrorism.

Even if losses from cyberattacks meet TRIA's financial thresholds for losses, certifying cyberattacks under TRIA can be challenging for three key reasons.

- First, cyberattacks may not meet TRIA's requirement that attacks be violent or dangerous to human life, property, or infrastructure. Although some cyberattacks can cause physical damage to property and infrastructure and endanger lives, according to some insurers and other experts, many cyberattacks are not violent acts or acts that are dangerous to human life, property, or infrastructure.[56] For example, a data breach or denial of service attack may result in stolen data or IT

[53]Cyber policies also may provide coverage for terrorism or cyberterrorism losses that are not eligible for TRIA.

[54]Terrorism Risk Insurance Program Updated Regulations in Light of the Terrorism Risk Insurance Program Reauthorization Act of 2019, and for Other Purposes, 86 Fed. Reg. 30537 (June 9, 2021). In December 2016, Treasury issued interim guidance confirming that certain stand-alone cyber coverage written in a TRIP-eligible line of insurance was within the scope of TRIP, so that insurers were obligated to adhere to the ''make available'' and disclosure requirements under TRIA for such coverage. The 2021 final rule codified in regulation Treasury's 2016 guidance.

[55]Department of the Treasury, Federal Insurance Office, *Study of Small Insurer Competitiveness in the Terrorism Risk Insurance Marketplace* (Washington, D.C.: June 2021).

[56]Some cyberattacks can cause physical damage, while others can endanger lives. For example, a 2014 cyberattack on an IT system at a German steel mill caused massive damage to a blast furnace and a 2021 cyberattack on a water treatment plant in Oldsmar, Florida, attempted to poison the city's water supply.

system disruption, but may not necessarily be a violent act or dangerous to human life, property, or infrastructure.

- Second, cyberattacks may not readily meet the TRIA criterion that attacks be part of an effort to coerce the civilian population of the United States or to coerce the U.S. government or influence policy.[57] Although it is possible for threat actors to use cyberattacks to coerce U.S. policy or affect the conduct of the U.S. government, many cyberattacks such as ransomware apparently may be motivated only by financial gain.[58] As previously noted, the recent rise in ransomware cyberattacks has resulted in total ransom and extortion costs amounting to millions of dollars per year.
- Third, cyberattacks may not meet the TRIA requirement that damage occur in the United States or in specific enumerated areas outside the United States. Several industry stakeholders cited the potential example of a cyberattack affecting a U.S. company with a server in an overseas location as one that likely would not meet TRIA's certification criteria.

Agencies Have Not Fully Assessed Whether Risk of Systemic Cyber Incident Warrants an Expanded Federal Insurance Response

CISA and FIO both have taken steps to better understand the financial implications of growing cybersecurity risks. However, the agencies have not fully assessed the extent to which the risks to the nation's critical infrastructure from catastrophic cyber incidents, and the potential financial exposures from these risks, warrant a federal insurance response. Performing such an assessment and reporting the results to Congress can inform deliberations on whether an expanded federal insurance response is needed. Should such a response be deemed necessary, our framework for providing federal assistance to private market participants could help ensure a prudently designed response.

[57]Cyberattacks may be used to coerce nongovernmental entities as well. For example, North Korea's 2014 cyberattack on Sony Pictures Entertainment, in combination with threats of physical violence, resulted in releasing the movie *The Interview* through online distribution channels and a limited number of theaters.

[58]In other cases, there might be insufficient evidence to determine whether the act was part of an effort to do so, according to Treasury officials.

CISA and FIO Have Taken Some Steps to Understand Financial Implications of Increased Cybersecurity Risks

In response to the increasing frequency of cyber incidents and the potential for severe economic consequences, CISA and FIO both have taken steps to better understand the financial implications of growing cybersecurity risks.

CISA. As previously discussed, in 2020 CISA issued a report on costs and losses from cyber incidents.[59] The report analyzed three sets of cyber incident studies, which estimated per-incident, nationally aggregated, or scenario-based costs and losses. The estimated impact of these scenarios ranged from $2.8 billion to $1 trillion per event for the United States.[60] The studies were helpful for understanding worst-case outcomes, such as the possibility of high-consequence, low-probability cyber events (for example, malware disrupting 50 power generators and destabilizing the electric grid of the Northeast), according to the report. In 2018, CISA also issued a report assessing the cyber insurance market, which identified the core challenges constraining the cyber insurance market, including a lack of data, methodological limitations, and a lack of information-sharing.[61]

FIO. FIO has continued work to improve its understanding of the cyberterrorism insurance market by collecting more information from insurers on cyber policy premiums, limits, and coverages. In November 2021, Treasury proposed revisions to its TRIP 2022 data call to insurers for additional information on the availability and affordability of cyber insurance coverage. Treasury has been conducting the 2022 TRIP data call pursuant to these expanded requests, which include collecting information on premiums and limits of cyber insurance (whether TRIP-eligible or not), and coverage provided for—and losses from—

[59]*Cost of a Cyber Incident: Systematic Review and Cross-Validation.*

[60]CISA's report noted that even the highest of these hypothetical scenario-based estimates was only a fraction of two other estimates. For example, a 2015 Bank of America Merrill Lynch report considered a potential worst-case 2020 "cybergeddon" scenario and stated that adversarial cyber activity could put up to $3 trillion of global economic value at risk. Bank of America Merrill Lynch, *Thematic Investing: You've Been Hacked! – Global Cybersecurity Primer* (September 2015). In turn, that estimate was only half of the $6 trillion annual loss projected for 2021 by Cybersecurity Ventures. Cybersecurity Ventures, *2017 Cybercrime Report* (2017).

[61]Cybersecurity and Infrastructure Security Agency, *Assessment of the Cyber Insurance Market* (Washington, D.C.: Dec. 21, 2018).

ransomware. FIO also has engaged with both private and public entities to better understand insurance issues and the current cyberattack landscape, including by meeting with market participants through its work with a federal advisory committee, according to FIO officials.

The missions and responsibilities of CISA and FIO make the agencies well-positioned to jointly assess the risks to the nation's critical infrastructure from catastrophic cyber incidents, the potential financial exposures from these risks, and the extent to which a federal insurance response might be needed.

- CISA's mission is to lead the national effort to understand, manage, and reduce risks to cyber and physical critical infrastructure. According to the CISA Director, identifying and understanding risk is key to CISA's success, especially risk that is systemic to critical networks and infrastructure.[62]
- FIO has the authority to monitor all aspects of the insurance sector, is a nonvoting member of the Financial Stability Oversight Council, and advises the Secretary of the Treasury on important national and prudential international insurance matters. Treasury officials stated that they consider it Treasury's role to inform policymakers on the potential need for an expanded federal insurance response (such as a backstop) for catastrophic cyber events. They also believe their proposed additional data collection could help inform Treasury's administration of TRIP.

Furthermore, the Organisation for Economic Co-operation and Development recommends that governments manage the financial effects of disasters on public finances by evaluating the potential financial exposures of government and developing plans.[63] One method for evaluating the potential financial exposures and developing related plans is to use a risk-management process—specifically, to perform a risk assessment and evaluate alternatives for addressing the risks.

[62]House Homeland Security Committee, *Evolving the U.S. Approach to Cybersecurity: Raising the Bar Today to Meet the Threats of Tomorrow*, 117th Cong. (Nov. 3, 2021); statement of Jen Easterly, Director, Cybersecurity and Infrastructure Security Agency, Department of Homeland Security.

[63]Organisation for Economic Cooperation and Development, O*ECD Recommendation on Disaster Risk Financing Strategies* (Paris, France: February 2017).

According to DHS's *Risk Management Fundamentals*, risk-management principles can be used to build capabilities that can respond to risks that have been realized—such as systemic cyber incidents.[64] DHS's risk-management process includes activities relating to assessing identified risks (to include their likelihood and impact), using that assessment to identify evaluative alternatives for addressing the risks, and selecting which alternative to implement.

CISA and FIO Have Not Fully Assessed Extent to Which Risks Warrant a Federal Insurance Response

Neither CISA nor FIO have used a risk-management process to assess whether cybersecurity risks warrant an additional federal insurance response. Such an assessment could include risks associated with systemic cyber incidents and alternative federal insurance responses for addressing that risk. It also could include how such responses would be funded, how they might be triggered, or the appropriate amount of federal support or financial assistance. Such information could be helpful to Congress for considering policy options and tradeoffs.

- **Funding mechanism.** Federal responses, such as risk transfer (insurance) activities, could include various types of funding mechanisms, each of which would have differing implications for private-sector entities (insurers and policyholders) and the federal government. In a prior review, we found that all five federal insurance programs we reviewed collected premiums, assessments, or fees, but differed in the extent to which they relied on them as a funding source.[65]
  - Federal crop insurance premiums are federally subsidized by law; premiums collected do not cover all costs.
  - The Pension Benefit Guaranty Corporation is expected to fund itself entirely through premiums and other nonfederal sources, and does not receive taxpayer funds or borrow funds from the U.S. Treasury.

[64]Department of Homeland Security, *Risk Management Fundamentals: Homeland Security Risk Management Doctrine* (April 2011).

[65]See GAO-19-353. For the purposes of the report's analysis, TRIP was not considered a federal insurance program, but its exposures were considered under another type of risk-transfer category.

- The federal government does not collect an up-front charge from insurers for the government's coverage of terrorism risk under TRIP. Instead, it uses a recoupment mechanism to recover some amount of any government payments made through surcharges imposed upon commercial policyholders that are collected by property/casualty insurance providers and then remitted by them to the U.S. Treasury.
- The federal government uses the Disaster Relief Fund to provide disaster relief assistance without collecting premiums or other fees from entities receiving the funds before or after an event occurs, and without knowing beforehand who might receive compensation.[66]

- **Trigger for government intervention.** Determining at what point the government should intervene to provide financial assistance involves balancing federal fiscal exposure against private-sector exposures and losses, among other considerations. For example, by increasing the TRIA program trigger in recent years, Congress potentially reduced the number of events that qualify for federal payments, decreasing federal fiscal exposure, but increasing insurer exposure.
- **Backstop size.** The size of any set-aside fund or risk-sharing backstop would involve consideration of policy trade-offs between public fiscal exposures and private-sector exposures and losses, including a consideration of how much of the federal government's implicit exposure to make explicit. For example, in the event of a certified act of terrorism, the government and insurers share losses above the program trigger of $200 million and below the program cap of $100 billion. These amounts limit federal fiscal exposure, because policyholders would be expected to cover any losses above the program cap.

[66]The Federal Emergency Management Agency's Disaster Relief Fund is the primary source of federal disaster assistance for state and local governments when the President declares a major disaster pursuant to the Stafford Act.

Implicit federal exposures to a systemic cyber incident could be enormous.[67] The federal response to the COVID-19 pandemic provides an example: before the pandemic, no federal insurance, reinsurance, or other financial assistance program existed to address lost business revenue from a global health catastrophe. Since March 2020, Congress and the administration have spent trillions of dollars to fund pandemic response and recovery efforts.[68] A similar expectation for federal financial assistance—especially for critical infrastructure—may arise in the event of a catastrophic cyberattack with systemic effects.

CISA and FIO officials said one reason they have not yet assessed the need for a federal response to systemic cyber events is that they lack the data to do so. However, CISA and FIO have not evaluated what additional data they might need to fully consider whether cyber risks warrant a federal response. We asked FIO officials whether its 2022 TRIP data call could be used to help assess how TRIP would respond to cyberterrorism, and whether additional federal assistance might be needed. They said that because the first year of the expanded data collection would not be complete until May 2022, they had not yet reached conclusions about whether or how to use the data for these purposes.

In addition, in March 2022, Congress passed the Cyber Incident Reporting for Critical Infrastructure Act of 2022, which requires CISA to promulgate rules requiring certain critical infrastructure entities to report certain cybersecurity incidents and ransom payments. As noted by CISA's cyber incident cost estimate report, these disclosures could help

[67]Any catastrophic event presents both explicit and implicit fiscal exposure for the federal government. Fiscal exposures are responsibilities, programs, and activities that legally may commit the federal government to future spending or create the expectation for future spending. Explicit exposures are commitments that the government is legally required to fund, while implicit exposures arise not from a legal commitment, but from current policy, past practices, or other factors that may create the expectation for future spending. Events can present a combination of explicit and implicit exposures. See GAO, *Fiscal Exposures: Improving Cost Recognition in the Federal Budget*, GAO-14-28 (Washington, D.C.: Oct. 29, 2013).

[68]GAO, *The Nation's Fiscal Health: After Pandemic Recovery, Focus Needed on Achieving Long-Term Fiscal Sustainability*, GAO-21-275SP (Washington, D.C.: Mar. 23, 2021).

CISA develop quality data on the cost of cybersecurity incidents, which would inform future cybersecurity investments.[69]

Defined Criteria and Security Requirements Are among Key Elements for a Federal Insurance Response

As of May 2022, legislation had not been introduced in Congress to create a federal insurance response to help address systemic or catastrophic cyber events.[70] However, if Congress were to consider such legislation in the future, our previously developed framework for providing federal assistance to private market participants could help inform its design (see table 3).[71]

[69]*Cost of a Cyber Incident: Systematic Review and Cross-Validation.*

[70]Some countries have taken steps to address losses from cyberattacks. For example, in 2018 Singapore launched the first government-funded cyber risk pool to provide capacity for cyber coverage and strengthen resilience against growing cyber threats.

[71]GAO, *Financial Assistance: Ongoing Challenges and Guiding Principles Related to Government Assistance for Private Sector Companies*, GAO-10-719 (Washington, D.C.: Aug. 3, 2010). Building on lessons learned from prior financial crises, we identified guiding principles to help serve as a framework for evaluating large-scale federal assistance efforts and provided guidelines for assisting failing companies.

Table 3: GAO Framework for Providing Federal Assistance to Private Market Participants

Principles	Description
Identify and define the problem	Separation of issues that require an immediate response from the structural challenges that will take longer to resolve.
Determine national interests and set clear goals and objectives	Determination of whether a legislative solution or other government intervention best serves the national interest.
Protect government's interests	Actions to ensure not only that financial markets continue to function effectively, but also that any investment provides the highest possible return. Examples include requiring concessions from all parties, placing controls over management, obtaining collateral when feasible, and being compensated for risk.
Coordinate actions on a global and comprehensive basis	Financial crises that are international in scope require comprehensive, global actions, and government interventions must be closely coordinated by the parties providing assistance—including U.S. and foreign governments—to help ensure that limited resources are used effectively.
Mitigate perceived or potential conflicts	Any action that results in the government having an ownership interest in private-sector companies requires that the government's strategy for managing its investments include plans to mitigate perceived or potential conflicts that may arise from its newly acquired role as shareholder or creditor and its existing role as regulator, supervisor, or policymaker.
Ensure adequate transparency by establishing an effective communication strategy	Federal intervention in private markets requires a strategy to help ensure open and effective communication with Congress and taxpayers. An effective communication strategy is important during changing market events and could help the public understand the policy goals that the government is trying to achieve and its rationale for spending public funds.
Establish a strong system for accountability	A system of accountability helps ensure that the interests of the government and taxpayers are adequately protected and the programs' objectives are achieved efficiently and effectively. Monitoring and other internal controls can help prevent and detect fraud.
Take steps to mitigate moral hazard	Federal financial assistance may create moral hazard or encourage market participants to expect similar emergency actions—the "too big to fail" perception. The government should ensure that financial assistance to private-market participants include terms that make it a last resort and specify when the assistance will end.

Source: GAO. | GAO-22-104256

Drawing from lessons learned from financial crises of prior decades, the eight principles aim to protect taxpayer interests when the government intervenes in private markets to avert a systemic crisis. The following three principles may be particularly important in any consideration of a federal insurance mechanism for cybersecurity risk:

- **Problem definition and identification are critical.** For a federal response for losses from cyberattacks, defining the problem could include establishing criteria for the type and magnitude of cyberattack the federal program would cover. Like TRIP's certification criteria for acts of terrorism, any criteria established for covered cyberattacks would need to balance risks to critical infrastructure operations with the potential level of federal exposure in the longer term.

- **Interventions should protect government—and thus taxpayer—interests.** Ensuring that any federal intervention in the cyber insurance market protects government and taxpayer interests could involve minimizing exposure and losses by collecting an up-front fee or premium or establishing an industrywide recoupment mechanism, as TRIA requires. Measures also could involve ensuring that companies, particularly those with critical infrastructure functions, take appropriate steps to manage their cybersecurity risks.
- **In providing assistance, the government should take steps to mitigate moral hazard.** Moral hazard occurs when entities take more risk than they otherwise would because of the presence of insurance or other financial assistance. For example, consumers may choose not to purchase flood insurance because they overestimate the adequacy of federal assistance they would expect to receive after a disaster.[72] In general, mitigating moral hazard requires that federal assistance include terms to help ensure that private-market recipients do not take excessive risk because of the presence of that assistance. A federal insurance backstop without any cybersecurity requirements or incentives could result in some policyholders relying on promised federal assistance rather than investing in strong cybersecurity controls. One option that has been proposed is to tie federal assistance for cyber-related losses to cybersecurity requirements.[73]

If such a response were deemed necessary, it would be important to consider the principles outlined above in the design of any response—the principles help ensure that any federal assistance given to private-sector entities protects national interests.

Conclusions

Cybersecurity risks facing U.S. critical infrastructure are significant and growing. Cyber insurance is one tool policyholders can use to help offset some of the losses that result from cyber incidents. However, it is a tool

[72]GAO, *Flood Insurance: Comprehensive Reform Could Improve Solvency and Enhance Resilience,* GAO-17-425 (Washington, D.C.: Apr. 27, 2017).

[73]For example, see National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Gaithersburg, Md.: February 2014). Version 1.1 of the framework was issued on April 16, 2018. Also see *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, Special Publication 800-37, Revision 2 (Gaithersburg, Md.: December 2018); and *Security and Privacy Controls for Information Systems and Organizations*, SP 800-53, Revision 5 (Gaithersburg, Md.: Sept. 2020).

that has been calibrated for non-catastrophic events. Whether insurers will continue to make coverage available for large cyberattacks with systemic effects resulting from the connectivity of interconnected systems is uncertain.

Both CISA and FIO have taken some steps to assess the financial implications of catastrophic cyberattacks, but they have not fully assessed the extent to which the risks to the nation's critical infrastructure from catastrophic cyber incidents, and the potential financial exposures from these risks, warrant a federal insurance response. An assessment that joins CISA's analysis of the cyber risks facing critical infrastructure with FIO's insight and data on the private insurance market could inform Congress in its future deliberations. In the event that Congress later decided to create or expand a federal mechanism to help cover such losses, applying our framework for providing federal assistance would help ensure that any response balanced and appropriately safeguarded public and private interests.

Recommendations for Executive Action

We are making two recommendations, one each to CISA and FIO. Specifically,

The Director of the Cybersecurity and Infrastructure Security Agency should work with the Director of the Federal Insurance Office to 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. (Recommendation 1)

The Director of the Federal Insurance Office should work with the Director of the Cybersecurity and Infrastructure Security Agency to 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. (Recommendation 2)

Agency Comments

We provided a draft of this report to DHS, Treasury, Department of Justice, and NAIC for review and comment. DHS and Treasury provided

written comments, which are reproduced in appendixes V and VI, respectively, and discussed below. The Department of Justice provided a technical comment, which we incorporated as appropriate. NAIC did not have comments.

In their comments, DHS and Treasury both concurred with our recommendations and described how they planned to address them. DHS stated that it will review the aggregate data generated by incident disclosures under the Cyber Incident Reporting for Critical Information Act of 2022 once available, and work with Treasury in the interim to determine other data needed. Treasury stated that it had reached out to DHS to begin collaboration on this effort. We are sending copies of this report to the Secretary of the Treasury, Secretary of Homeland Security, the Attorney General, NAIC, and other interested parties. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact Daniel Garcia-Diaz at (202) 512-8678 or garciadiazd@gao.gov, or Kevin Walsh at (202) 512-6151 or walshk@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix VII.

Daniel Garcia-Diaz
Managing Director, Financial Markets and Community Investment

Kevin Walsh
Director, Information Technology and Cybersecurity

Appendix I: Objectives, Scope, and Methodology

This report examines the extent to which (1) cybersecurity risks for U.S. critical infrastructure exist; (2) private insurance covers catastrophic cyber losses and the Terrorism Risk Insurance Program (TRIP) provides an adequate backstop for such losses; and (3) cognizant federal agencies have assessed a potential federal insurance response for cyberattacks. The focus of this report is cyber insurance provided to businesses and other entities and not to individual consumers.

To assess cybersecurity risks for U.S. critical infrastructure, we examined and summarized publicly available public- and private-sector information on the financial harms and costs of incidents that affected critical infrastructure. We identified vulnerable technologies, developed a list of actors who could pose a threat to critical infrastructure, and reviewed the potential impacts of cyberattacks. Specifically, to identify critical infrastructure cybersecurity vulnerabilities and threat actor tactics and techniques, we summarized our prior work on critical infrastructure cybersecurity, documents from the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA), and from MITRE Corporation.[1] To develop the list of threat actors, we reviewed our prior work and national threat assessment documents from the Office of

[1]GAO, *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges*, GAO-21-288 (Washington, D.C.: Mar. 24, 2021); and *Electricity Grid Cybersecurity: DOE Needs to Ensure Its Plans Fully Address Risks to Distribution Systems*, GAO-21-81 (Washington, D.C.: Mar. 18, 2021). Also see Cybersecurity and Infrastructure Security Agency, *Cyber Threats to Critical Manufacturing Sector Industrial Control Systems* (Washington, D.C.: Dec. 2021); and Mitre Corporation, "Adversarial Tactics, Techniques, and Common Knowledge (MITRE ATT&CK®), last accessed on March 18, 2022, https://attack.mitre.org/.

the Director of National Intelligence, National Security Agency, CISA, and the Department of Justice.[2]

To identify potential impacts of cyberattacks on critical infrastructure, we reviewed our prior work on critical infrastructure cybersecurity and public- and private-sector reports by CISA, Lloyd's of London, and the RAND Corporation.[3] Additionally, we reviewed publicly available reports from 2016 through 2021 that described the frequency and costs of cyberattacks—specifically, the Federal Bureau of Investigation's Internet Crime Reports, Verizon's Data Breach Investigations Reports, and an IBM Cost of a Data Breach Report.[4] We also interviewed CISA officials about the cybersecurity risks facing critical infrastructure.

To ensure the reliability of the cost and frequency data, we reviewed it for obvious errors in accuracy and completeness and considered the extent to which the data in each report independently corroborated evidence found in other reports. We determined that these data were sufficiently reliable for the purposes of this report, which was to describe overall trends in the frequency and costs of cyberattacks in the United States in 2016—2021.

To assess the extent to which private insurance and TRIP might cover and exclude cyberattack losses, we reviewed reports by the Department of the Treasury and insurance industry stakeholders. We also reviewed

[2]GAO-21-288, GAO-21-81; Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (Washington, D.C.: Feb. 7, 2022); National Security Agency and Cybersecurity and Infrastructure Security Agency, *NSA and CISA Recommend Immediate Actions to Reduce Exposure Across all Operational Technologies and Control Systems*, U/OO/154383-20 and PP-20-0622 (July 22, 2020). See Department of Justice, *ISIL-Linked Hacker Arrested in Malaysia on U.S. Charges* (Washington, D.C.: Oct. 15, 2015); *Indictment: Kansas Man Indicted for Tampering with a Public Water System* (Topeka, K.S.: Mar. 31, 2021); and *Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe* (Washington, D.C.: Feb. 17, 2021).

[3]See GAO-21-288. Also see Cybersecurity and Infrastructure Security Agency, *Cost of a Cyber Incident: Systematic Review and Cross-Validation* (Washington, D.C.: Oct. 26, 2020);Lloyd's and University of Cambridge Centre for Risk Studies, *Emerging Risk Report – 2015: Business Blackout: The insurance implications of a cyberattack on the US power grid* (Cambridge, UK: 2015). RAND, *Estimating the Global Cost of Cyber Risk: Methodology and Examples* (Santa Monica, C.A.: 2018).

[4]See Federal Bureau of Investigation, *2016 Internet Crime Report* (Washington, D.C.: 2016) and *Federal Bureau of Investigation Internet Crime Report 2021* (Washington, D.C.: 2021). See also Verizon, *2016 Data Breach Investigations Report* (New York, N.Y.: 2016) and *2021 Data Breach Investigations Report* (New York, N.Y.: 2021). Also see IBM Security, *2021 Cost of a Data Breach Report* (Armonk, N.Y.: 2021).

past GAO work and literature on cyber insurance coverage from selected insurers to obtain perspectives on cyberattack risk and the market for cyber insurance. We obtained information from four insurers, two insurance brokers, several academic experts, the U.S. Cyberspace Solarium Commission, National Association of Insurance Commissioners, Wholesale and Specialty Insurance Association, and American Property Casualty Insurance Association.

We selected the four insurers in our sample based on the different types of insurance offered and their large market share measured by dollar amount of premiums written. We selected insurance industry groups, risk experts, and academic researchers knowledgeable on issues related to insurance coverage, cyberattack risk, and the potential for TRIA to cover for such attacks. We identified these sources based on our review of the literature and recommendations from interviewees. The information we obtained from these industry participants and researchers may not represent the views or practices of all industry participants or researchers. We also interviewed officials from Treasury and CISA. In these interviews, we asked participants about the types and availability of insurance that would cover cyberattacks, including the extent to which insurance would cover catastrophic events and attacks with systemic risk.

We also interviewed six critical infrastructure operators in the health care, energy, communications, and financial services sectors to determine the types of cyberattack risk they faced and insurance coverage that could address that risk. We focused on these four sectors because they were deemed to be the most critical and cyber-dependent by Presidential Policy Directive 21 on Critical Infrastructure Security and Resilience, DHS's Cyber Dependent Infrastructure Identification Working Group, the Homeland Security Advisory Council, and feedback from industry experts with whom we met. We initially contacted eight operators—two from each of our four sectors—and six of the eight responded to our request and agreed to meet with us. We identified the operators using a snowball sampling technique in which we identified contacts through referrals from sector associations and internal GAO experts.

To assess the extent to which TRIP would cover catastrophic cyber losses, we reviewed the program's requirements in Treasury's guidance and rules. We also reviewed past GAO work, and information from academic researchers and organizations such as the Centers for Better Insurance, Insurance Information Institute, and Brookings Institution to understand how the program is applied. We then assessed the extent to which TRIP likely would cover losses from a systemic attack resulting in

catastrophic losses by comparing the program requirements to the characteristics of cyberattacks.

To determine the extent to which CISA and Treasury have assessed a potential federal insurance response to cyberattacks, we reviewed reports on the extent of cyberattack risk, and Treasury's assessments of TRIP's effectiveness. We reviewed Treasury's TRIA data call and associated guidance, including proposed revisions to its 2022 data call. In addition, we interviewed Treasury and CISA officials. We reviewed the agencies' missions and various sources of guidance on managing and evaluating financial exposures, including the Department of Homeland Security's *Risk Management Fundamentals*, and compared the agencies' actions against these sources.[5] We also reviewed our framework for providing federal assistance to private market participants and assessed its applicability to a potential federal insurance response for catastrophic cyberattacks.[6]

We conducted this performance audit from March 2020 to June 2022 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[5]Department of Homeland Security, *Risk Management Fundamentals: Homeland Security Risk Management Doctrine* (Washington, D.C.: April 2011). Organisation for Economic Cooperation and Development, *OECD Recommendation on Disaster Risk Financing Strategies* (Paris, France: February 2017).

[6]GAO, *Financial Assistance: Ongoing Challenges and Guiding Principles Related to Government Assistance for Private Sector Companies*, GAO-10-719 (Washington, D.C.: Aug. 3, 2010).

Appendix II: Cyberattack Tactics and Techniques Associated with Enterprise IT and Industrial Control Systems

Attackers may use various tactics, such as gaining an initial foothold on target systems, running malicious code, and moving through various systems—to exploit vulnerabilities and position themselves to achieve their ultimate goals (see table 4).

Table 4: Summary of Cyberattack Tactics and Techniques Associated with Enterprise IT and Industrial Control Systems

Technology	Summary of cyberattack tactics and techniques
Enterprise IT systems	Attackers often begin cyberattacks on enterprise systems by • performing reconnaissance, such as scanning for vulnerabilities in target hosts or applications; then, • establishing resources that can be used to support their operations, such as developing malicious software.[a] Subsequently, attackers will seek to gain initial access to a target network by • using spearphishing-emails, or • exploiting weaknesses on public-facing webservers. After gaining an initial foothold, attackers will often use a variety of tactics and techniques to achieve their objectives, such as • trying to run malicious code, • attempting to steal account names and passwords to gain higher-level permissions, and • moving throughout a network to find and gain access to their target.

Industrial control systems	Attackers can gain initial access to industrial control systems[b] by • exploiting internet-accessible system devices; • compromising the supply chain of the system by manipulating products (such as hardware or software) or delivery mechanisms before receipt by the end consumer[c]; or • gaining access to enterprise IT systems, then leveraging this access to target industrial control systems. After gaining initial access to industrial control systems, attackers may use other tactics to position themselves to achieve their goals, such as • running malicious code, • avoiding detection, and • moving throughout the industrial control systems environment. Attackers will then attempt to manipulate or interrupt operations of industrial control systems to achieve their goals, including by • damaging or destroying infrastructure, equipment, and the surrounding environment; • preventing operators from controlling industrial operations, even after the malicious interference has subsided; and • reducing productivity and revenue by disrupting or damaging the availability and integrity of control system operations, devices, and related processes.

Source: Prior GAO reports and GAO analysis of MITRE ATT&CK® Matrix for Enterprise and Matrix for Industrial Control Systems. | GAO 22-104256

[a]MITRE Corporation, "MITRE ATT&CK® Matrix for Enterprise," last accessed on April 25, 2022, at https://attack.mitre.org/matrices/enterprise/. The MITRE Corporation is a not-for-profit organization chartered to work in the public interest. MITRE has done extensive research for the federal government on cybersecurity issues.

[b]MITRE Corporation, "MITRE ATT&CK® Matrix for Industrial Control Systems, last accessed on April 25, 2022 at https://attack.mitre.org/matrices/ics/.

[c]The supply chain is a linked set of resources and processes that begins with the design of products and services and extends through development, sourcing, manufacturing, handling, and delivery of products and services to the acquirer.

Appendix III: Summary of Nation-State Actors and Previous Attacks

Table 5: Summary of Nation-State Actors and Previous Attacks

Nation-State	Description of capabilities and associated threat groups	Examples of past cyberattacks
China	In February 2022, the Intelligence Community assessed that China presents the broadest, most active, and persistent cyber espionage threat to the United States.	• China's Ministry of State Security exploited vulnerabilities in Microsoft Exchange Server before the vendor released security updates in March 2021. The malicious actor was able to compromise tens of thousands of computers worldwide. • According to the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI), state-sponsored Chinese actors conducted a spearphishing and intrusion campaign from December 2011 to 2013 targeting U.S. oil and natural gas pipeline companies. Of the 23 targeted pipeline operators, 13 were confirmed compromises and eight had an unknown depth of intrusion.
Iran	Iran's expertise and willingness to conduct aggressive cyber operations make it a significant threat to U.S. security, according to the intelligence community.	• In August 2012, malicious cyber actors attacked Saudi Aramco, the world's largest oil producer, and deleted information on about 30,000 workstations on the company's network. The attackers likely used the Shamoon malware, which the U.S. government has attributed to Iranian nation-state cyber actors. • According to the Office of the Director of National Intelligence, Iran was responsible for multiple cyberattacks between April and July 2020 against Israeli water facilities. They caused unspecified short-term effects, according to press reporting.
North Korea	North Korea's cyber program poses a sophisticated and agile espionage, cybercrime, and attack threat, according to the intelligence community.	• In May 2017, North Korean nation-state cyber actors used the WannaCry ransomware variant to infect and extort victim organizations. The ransomware infected hundreds of thousands of computers in over 150 countries, including computers used by England's National Health Service to access electronic patient records and clinical systems. • According to CISA and the Department of Justice (DOJ), in November 2014 North Korean state-sponsored cyber actors allegedly launched an attack against Sony Pictures Entertainment in an apparent attempt to prevent the release of a movie critical of the North Korean government. The attackers stole confidential data, threatened Sony Pictures Entertainment executives and employees, and damaged thousands of computers.

Russia	In February 2022, the Intelligence Community assessed that Russia will remain a top cyber threat.	• In February 2022, the Main Intelligence Directorate (also known as the GRU) of the General Staff of the Armed Forces of the Russian Federation conducted a distributed denial of service attack against the Ukrainian Ministry of Defense and state-owned banks. The attacks temporarily brought down targeted websites and disrupted banking services throughout the country. • In December 2015, Russian nation-state cyber actors conducted a cyberattack on the Ukrainian power grid that systematically disconnected substations, resulting in a power outage that lasted 1–6 hours. • In June 2017, the GRU conducted the NotPetya malware attacks against hundreds of victims around the world. The malware spread worldwide, damaged computers used in critical infrastructure, and caused an estimated $10 billion in damages globally.

Source: GAO analysis of press reporting and documentation from the White House, CISA, DOJ, FBI, and ODNI. | GAO-22-104256

Appendix IV: Summary of Nonstate Actors and Past Cyberattacks

Table 6: Summary of Nonstate Actors and Past Cyberattacks

Threat actor type	Description and potential motivation	Examples of past cyberattacks
Criminal groups	Criminal groups seek to attack systems for monetary gain, such as profiting from the sale of stolen information. The line between nation-state and criminal actors is increasingly blurry as nation-state actors turn to criminal groups to carry out cyberattacks as proxies of the state.	In May 2021, the Colonial Pipeline Company learned it was the victim of a ransomware attack against its IT network. As a safety measure, the company disconnected certain industrial control systems, resulting in a temporary halt to all pipeline operations. This in turn led to gasoline shortages throughout the southeast United States. In June 2021, the White House and the Department of Agriculture announced that a meat processing company had been targeted with ransomware that affected the company's operations. The company reportedly paid $11 million in ransom.
Hackers and hacktivists	Hackers break into networks for reasons including the challenge, revenge, stalking, or monetary gain. In contrast, hacktivists are ideologically motivated actors who use cyberattack tools to further political goals.	According to press reporting, in 2016, hacktivist groups Anonymous and GhostSquadHackers conducted cyberattacks against financial institutions across the world. As a result, websites for some targets, including several central banks, were temporarily taken offline. According to press reporting, in January 2022 hacktivists infected Belarus' state-run railway system with ransomware to disrupt its operations. The attackers allegedly offered to decrypt the infected systems if Belarus' government met their demands.
Insiders	Insiders are individuals (such as employees, contractors, or vendors) with authorized access to an information system or enterprise and who have the potential to cause harm, wittingly or unwittingly, through destruction, disclosure, or modification of data, or through denial of service.	According to a Department of Justice (DOJ) announcement, in March 2019 a Kansas man allegedly accessed the Ellsworth County Rural Water District's protected computer system without authorization. The indictment alleges he used that access to shut down processes that affect cleaning and water-disinfecting procedures. According to press reporting, the man was a former employee of the utility he allegedly targeted. Between March and July 2019, an attacker exfiltrated personal data, including credit card information, of over 100 million people from a major bank's cloud-hosted database. DOJ charged a former engineer who worked for the cloud provider that hosted the database for the attack.

Violent extremists	Violent extremists or terrorists could obtain and disclose compromising or personally identifiable information through cyber operations, and they could use such disclosures to coerce, extort, or inspire and enable physical attacks against their victims. Violent extremists could produce some disruptive effects, such as executing denial-of-service attacks against poorly protected networks.	According to a DOJ announcement, between June and August 2015 a Kosovo citizen gained unauthorized access to a U.S. company's network and stole the personally identifiable information of thousands of individuals. He then provided the information of over 1,000 U.S. service members and federal employees to the Islamic State of Iraq and the Levant.

Source: Prior GAO reports, and GAO analysis of press reporting and documentation from DOJ. | GAO-22-104256

Appendix V: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

June 2, 2022

Daniel Garcia-Diaz
Managing Director, Financial Markets and Community Investment
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Kevin Walsh
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Management Response to Draft Report GAO-22-104256, "CYBER INSURANCE: Action Needed to Assess Potential Federal Response to Catastrophic Attacks"

Dear Messrs. Garcia-Diaz and Walsh:

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS or the Department) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

The Department is pleased to note GAO's recognition of the role of the Cybersecurity and Infrastructure Agency (CISA) and its efforts to secure the nation's critical infrastructure and National Critical Functions, to include CISA's efforts during the past five years to better understand the financial implications of growing cybersecurity risks through analysis and reporting on costs of cyber incidents and an assessment of the cyber insurance market. DHS remains committed to leading the national effort to understand, manage, and reduce risk to the nation's cyber and physical infrastructure.

The draft report contained two recommendations, including one for CISA with which the Department concurs. Enclosed, please find our detailed response to the recommendation. DHS previously submitted technical comments under a separate cover for GAO's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,

JIM H CRUMPACKER

Digitally signed by JIM H CRUMPACKER
Date: 2022.06.02 09:04:31 -04'00'

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Enclosure

2

Enclosure: Management Response to Recommendation Contained in GAO-22-104256

GAO recommended that the Director of CISA:

Recommendation 1: Work with the Director of the Federal Insurance Office [FIO] to 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.

Response: Concur. CISA's Office of the Chief Economist (OCE) has previously collaborated with Department of Treasury's FIO on work such as CISA's "Incentives Study Analytic Report," dated June 12, 2013, in support of Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," dated February 12, 2013, and will expand upon that collaboration. For example, CISA's study "Cost of a Cyber Incident: Systematic Review and Cross-Validation," dated October 26, 2020, analyzed per-incident, nationally aggregated, and scenario-based costs and losses from cyber incidents, including those likely to be considered catastrophic. Further, CISA's study "Assessment of the Cyber Insurance Market," dated December 21, 2018, identified core challenges constraining the cyber insurance market, including a lack of data, methodological limitations, and a lack of information sharing.

CISA's Office of Strategy, Policy, and Planning (SPP) and CISA's OCE, with support from CISA's National Risk Management Center, will review the aggregate data generated by the incident disclosures required by the "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) of 2022" (Pub. Law No. 117-103), which requires CISA to promulgate rules requiring "covered entities" to report "covered cyber incidents" and ransom payments. These disclosures could help CISA SPP and OCE to develop the data needed to assess whether a federal insurance response is warranted. CIRCIA requires a Notice of Proposed Rulemaking (NPRM) to be promulgated within 24 months of the statute's enactment (i.e., by March 2024) and a final rule to be promulgated within 18 months of the NPRM's publication (i.e., no later than September 2025).

In the interim, CISA SPP and CISA OCE will work with the Director of the FIO to evaluate what additional data may be needed to consider whether cyber risks warrant a federal insurance response, which should be complete by September 29, 2023. Overall Estimated Completion Date: December 31, 2026.

3

Text of Appendix V: Comments from the Department of Homeland Security

June 2, 2022

Daniel Garcia-Diaz

Managing Director, Financial Markets and Community Investment

U.S. Government Accountability Office

441 G Street, NW

Washington, DC 20548

Kevin Walsh

Director, Information Technology and Cybersecurity

U.S. Government Accountability Office 441 G Street, NW

Washington, DC 20548

Re: Management Response to Draft Report GAO-22-104256, “CYBER INSURANCE: Action Needed to Assess Potential Federal Response to Catastrophic Attacks”

Dear Messrs. Garcia-Diaz and Walsh:

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS or the Department) appreciates the

U.S. Government Accountability Office’s (GAO) work in planning and conducting its review and issuing this report.

The Department is pleased to note GAO’s recognition of the role of the Cybersecurity and Infrastructure Agency (CISA) and its efforts to secure the nation’s critical infrastructure and National Critical Functions, to include CISA’s efforts during the past five years to better understand the financial implications of growing cybersecurity risks through analysis and reporting on costs of cyber incidents and an assessment of the cyber insurance market. DHS remains committed to leading the

national effort to understand, manage, and reduce risk to the nation's cyber and physical infrastructure.

The draft report contained two recommendations, including one for CISA with which the Department concurs. Enclosed, please find our detailed response to the recommendation. DHS previously submitted technical comments under a separate cover for GAO's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,

JIM H. CRUMPACKER, CIA, CFE

Director

Departmental GAO-OIG Liaison Office

Enclosure

Enclosure: Management Response to Recommendation Contained in GAO-22-104256

GAO recommended that the Director of CISA:

Recommendation 1: Work with the Director of the Federal Insurance Office [FIO] to 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.

Response: Concur. CISA's Office of the Chief Economist (OCE) has previously collaborated with Department of Treasury's FIO on work such as CISA's "Incentives Study Analytic Report," dated June 12, 2013, in support of Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," dated

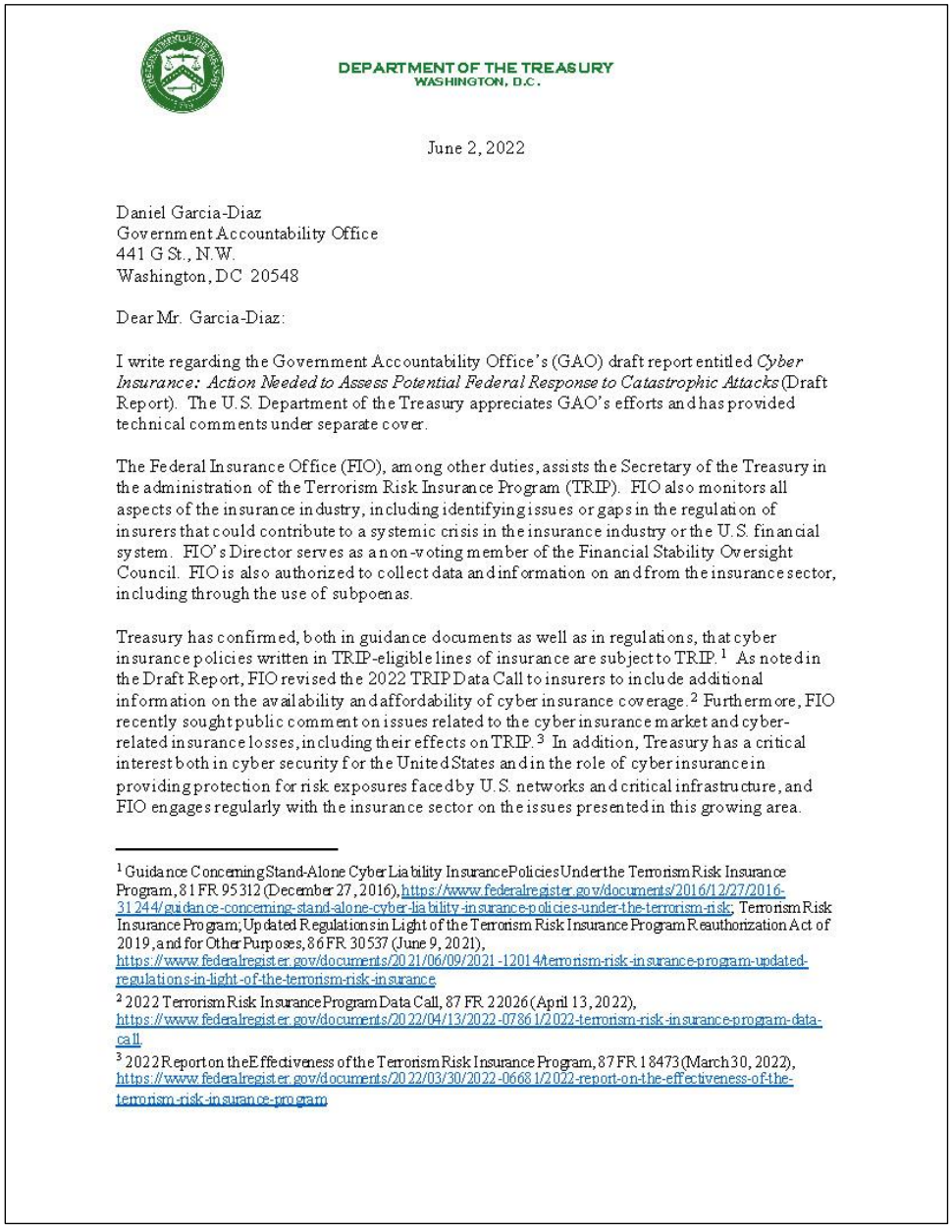
February 12, 2013, and will expand upon that collaboration. For example, CISA's study "Cost of a Cyber Incident: Systematic Review and Cross-Validation," dated October 26, 2020, analyzed per-incident, nationally aggregated, and scenario-based

costs and losses from cyber incidents, including those likely to be considered catastrophic. Further, CISA's study "Assessment of the Cyber Insurance Market," dated December 21, 2018, identified core challenges constraining the cyber insurance market, including a lack of data, methodological limitations, and a lack of information sharing.

CISA's Office of Strategy, Policy, and Planning (SPP) and CISA's OCE, with support from CISA's National Risk Management Center, will review the aggregate data generated by the incident disclosures required by the "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) of 2022" (Pub. Law No. 117- 103), which requires CISA to promulgate rules requiring "covered entities" to report "covered cyber incidents" and ransom payments. These disclosures could help CISA SPP and OCE to develop the data needed to assess whether a federal insurance response is warranted. CIRCIA requires a Notice of Proposed Rulemaking (NPRM) to be promulgated within 24 months of the statute's enactment (i.e., by March 2024) and a final rule to be promulgated within 18 months of the NPRM's publication (i.e., no later than September 2025).

In the interim, CISA SPP and CISA OCE will work with the Director of the FIO to evaluate what additional data may be needed to consider whether cyber risks warrant a federal insurance response, which should be complete by September 29, 2023. Overall Estimated Completion Date: December 31, 2026.

Appendix VI: Comments from the Department of Treasury



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

June 2, 2022

Daniel Garcia-Diaz
Government Accountability Office
441 G St., N.W.
Washington, DC 20548

Dear Mr. Garcia-Diaz:

I write regarding the Government Accountability Office's (GAO) draft report entitled *Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks* (Draft Report). The U.S. Department of the Treasury appreciates GAO's efforts and has provided technical comments under separate cover.

The Federal Insurance Office (FIO), among other duties, assists the Secretary of the Treasury in the administration of the Terrorism Risk Insurance Program (TRIP). FIO also monitors all aspects of the insurance industry, including identifying issues or gaps in the regulation of insurers that could contribute to a systemic crisis in the insurance industry or the U.S. financial system. FIO's Director serves as a non-voting member of the Financial Stability Oversight Council. FIO is also authorized to collect data and information on and from the insurance sector, including through the use of subpoenas.

Treasury has confirmed, both in guidance documents as well as in regulations, that cyber insurance policies written in TRIP-eligible lines of insurance are subject to TRIP.[1] As noted in the Draft Report, FIO revised the 2022 TRIP Data Call to insurers to include additional information on the availability and affordability of cyber insurance coverage.[2] Furthermore, FIO recently sought public comment on issues related to the cyber insurance market and cyber-related insurance losses, including their effects on TRIP.[3] In addition, Treasury has a critical interest both in cyber security for the United States and in the role of cyber insurance in providing protection for risk exposures faced by U.S. networks and critical infrastructure, and FIO engages regularly with the insurance sector on the issues presented in this growing area.

[1] Guidance Concerning Stand-Alone Cyber Liability Insurance Policies Under the Terrorism Risk Insurance Program, 81 FR 95312 (December 27, 2016), https://www.federalregister.gov/documents/2016/12/27/2016-31244/guidance-concerning-stand-alone-cyber-liability-insurance-policies-under-the-terrorism-risk; Terrorism Risk Insurance Program; Updated Regulations in Light of the Terrorism Risk Insurance Program Reauthorization Act of 2019, and for Other Purposes, 86 FR 30537 (June 9, 2021), https://www.federalregister.gov/documents/2021/06/09/2021-12014/terrorism-risk-insurance-program-updated-regulations-in-light-of-the-terrorism-risk-insurance

[2] 2022 Terrorism Risk Insurance Program Data Call, 87 FR 22026 (April 13, 2022), https://www.federalregister.gov/documents/2022/04/13/2022-07861/2022-terrorism-risk-insurance-program-data-call

[3] 2022 Report on the Effectiveness of the Terrorism Risk Insurance Program, 87 FR 18473 (March 30, 2022), https://www.federalregister.gov/documents/2022/03/30/2022-06681/2022-report-on-the-effectiveness-of-the-terrorism-risk-insurance-program

The Draft Report recommends that FIO and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) jointly assess the extent to which the risks to the nation's critical infrastructure from catastrophic cyber incidents and the potential financial exposures from these risks warrant a federal insurance response, and inform the Congress of the results of its assessment. FIO agrees with this recommendation and welcomes the opportunity to work with CISA on the issues presented in the recommendation set forth in the Draft Report. FIO has reached out to its colleagues at CISA and has confirmed that CISA welcomes the opportunity as well.

Thank you again for the opportunity to review the Draft Report and for your consideration of our comments.

Sincerely,

STEVEN E. SEITZ Digitally signed by STEVEN E. SEITZ Date: 2022.06.02 13:22:23 -04'00'

Steven E. Seitz
Director, Federal Insurance Office
U.S. Department of the Treasury

2

Appendix VI: Comments from the Department of Treasury

June 2, 2022

Daniel Garcia-Diaz

Government Accountability Office 441 G St., N.W.

Washington, DC 20548 Dear Mr. Garcia-Diaz:

I write regarding the Government Accountability Office's (GAO) draft report entitled *Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks* (Draft Report). The U.S. Department of the Treasury appreciates GAO's efforts and has provided technical comments under separate cover.

The Federal Insurance Office (FIO), among other duties, assists the Secretary of the Treasury in the administration of the Terrorism Risk Insurance Program (TRIP). FIO also monitors all aspects of the insurance industry, including identifying issues or gaps in the regulation of insurers that could contribute to a systemic crisis in the insurance industry or the U.S. financial system. FIO's Director serves as a non-voting member of the Financial Stability Oversight Council. FIO is also authorized to collect data and information on and from the insurance sector, including through the use of subpoenas.

Treasury has confirmed, both in guidance documents as well as in regulations, that cyber insurance policies written in TRIP-eligible lines of insurance are subject to TRIP.[1] As noted in the Draft Report, FIO revised the 2022 TRIP Data Call to insurers to include additional information on the availability and affordability of cyber

[1] Guidance Concerning Stand-Alone Cyber Liability Insurance Policies Under the Terrorism Risk Insurance Progra m, 81 FR 95312 (December 27, 2016), https://www.federalregister.gov/documents/2016/12/27/2016-31244/guidance-concerning-stand-alone-cyber-liability-insurance-policies-under-the-terrorism-risk; Terrorism Risk Insurance Program; Updated Regulations in Light of the Terrorism Risk Insurance Program Reauthorization Act of 2019, and for Other Purposes, 86 FR 30537 (June 9, 2021), https://www.federalregister.gov/documents/2021/06/09/2021-12014/terrorism-risk-insurance-program-updated-regulations-in-light-of-the-terrorism-risk-insurance.

insurance coverage.[2] Furthermore, FIO recently sought public comment on issues related to the cyber insurance market and cyber-related insurance losses, including their effects on TRIP.[3] In addition, Treasury has a critical interest both in cyber security for the United States and in the role of cyber insurance in providing protection for risk exposures faced by U.S. networks and critical infrastructure, and FIO engages regularly with the insurance sector on the issues presented in this growing area.

The Draft Report recommends that FIO and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) jointly assess the extent to which the risks to the nation's critical infrastructure from catastrophic cyber incidents and the potential financial exposures from these risks warrant a federal insurance response, and inform the Congress of the results of its assessment. FIO agrees with this recommendation and welcomes the opportunity to work with CISA on the issues presented in the recommendation set forth in the Draft Report. FIO has reached out to its colleagues at CISA and has confirmed that CISA welcomes the opportunity as well.

Thank you again for the opportunity to review the Draft Report and for your consideration of our comments.

Sincerely,

Steven E. Seitz

Director, Federal Insurance Office

U.S. Department of the Treasury

[2] 2022 Terrorism Risk Insurance Program Data Call, 87 FR 22026 (April 13, 2022), https://www.federalregister.gov/documents/2022/04/13/2022-07861/2022-terrorism-risk-insurance-program-data- ca ll.

[3] 2022 Report on the Effectiveness of the Terrorism Risk Insurance Program, 87 FR 18473 (March 30, 2022), https://www.federalregister.gov/documents/2022/03/30/2022-06681/2022-report-on-the-effectiveness-of-the- terrorism-risk-insurance-program.

Appendix VII: GAO Contacts and Staff Acknowledgments

GAO Contacts

Daniel Garcia-Diaz, 202-512-8678 or garciadiazd@gao.gov, and Kevin Walsh, 202-512-6151 or walshk@gao.gov.

Staff Acknowledgments

In addition to the contacts named above, Kaelin Kuhn (Assistant Director), Winnie Tsen (Assistant Director), Nathan Gottfried (Analyst in Charge), Evelyn Calderon, Marisol Cruz Cain, Gautam Iyer, Keith Kim, Collin Kindig, Dustin Milne, Barbara Roesmann, John Pendleton, Noah Levesque, Nick Marinos, Jill Naamane, Stephen Ruszczyk, Jessica Sandler, Sukhjoot Singh, Jena Sinkfield, and Andrew Stavisky made significant contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548