McCRARY INSTITUTE
FOR CYBER AND CRITICAL INFRASTRUCTURE SECURITY

Testimony of Frank J. Cilluffo
Director, McCrary Institute for Cyber and Critical Infrastructure Security
Auburn University

Before the U.S. House of Representatives Subcommittee on
Cybersecurity and Infrastructure Protection

Sector Down: Ensuring Critical Infrastructure Resilience

June 27, 2024

Introduction
Chairman Garbarino, Ranking Member Swalwell, and distinguished subcommittee members thank you for the opportunity to testify before you today on a subject that is clearly of national importance. Your oversight in examining these critical topics is commendable.

In my remarks today, I aim to provide an overview of the landscape of cyber threats, highlighting their growing complexity and seriousness. The cyber threat can no longer be treated in isolation, because it plays a central role in global crises and flashpoints. It's impossible to examine cyber issues without an appreciation for the geopolitical environment and global crises in all contexts. Cyber threats have evolved from a niche concern to a core issue in all conflicts. I will shed light on the various players involved, including nation-states and cybercriminals, along with their advanced strategies like leveraging proxies and employing "living off the land" tactics.

Furthermore, my testimony will delve into the impact of National Security Memorandum 22 (NSM 22) and its guidelines for identifying Systemically Important Entities. This will highlight the significance of adopting a cybersecurity approach that considers the interconnectedness within our infrastructure framework.

Moreover, I will discuss the pressing need to revamp and strengthen our private partnerships. By reviewing initiatives such as the Joint Cyber Defense Collaborative and Project Fortress, I hope to demonstrate how these models can be expanded and customized to establish resilient and proactive defense mechanisms across various sectors.

Lastly, I will discuss how the insurance industry can encourage improved cybersecurity practices and the potential for a national strategy to deal with severe cyber risks. By assessing the landscape of cyber insurance and suggesting ways to better calibrate government involvement, I aim to highlight the delicate balance between private sector creativity and essential government assistance.

It is important to note that our historical cybersecurity posture has been largely reactive, primarily focused on responding to incidents and putting out fires. This approach is no longer sufficient in the face of evolving and sophisticated threats. We cannot simply “firewall” our way out of the problem. Instead, we must shift towards a more proactive defense strategy that focuses on managing risks, minimizing potential impacts, and building resilience across our critical infrastructure and key sectors.

Going forward, our approach to cybersecurity needs to be adaptable, cooperative, and forward-looking. The time is ripe for decisive efforts to move beyond reactive measures. By fostering stronger collaborations between the public and private sectors and taking strategic government actions, we can bolster our country's ability to anticipate, prevent, and mitigate cyber threats rather than merely responding to them after the fact. This proactive stance is essential to effectively protect our national security, economic interests, and public safety in the digital age.

Overview of the Cyber Threat Landscape

The cyber threat landscape facing the United States is becoming increasingly complex and dangerous, with nation-state actors, cybercriminals, and other malicious entities creating significant risks to our national security, economic prosperity, and public safety.

In today's geopolitical environment, it's increasingly difficult to imagine any conflict without a significant cyber element. Cyber capabilities have become integral to modern warfare and geopolitical strategy, whether through direct cyberattacks, espionage for target selection, intelligence preparation of the battlefield (pre-positioning), or the use of disinformation and misinformation to create a fog of war.

While cyber threats come in various shapes, sizes, and forms, Nation-state threats remain at the forefront of our concerns. The People's Republic of China is "the most active and persistent cyber threat to U.S. Government, private sector, and critical infrastructure networks."[1] Chinese state-sponsored actors, such as Volt Typhoon, have shown a growing willingness to compromise and hold at risk critical infrastructure systems, even those without inherent espionage value.[2] This shift from traditional espionage to pre-positioning is a concerning escalation.

The Volt Typhoon hackers have been particularly active in targeting American facilities in Guam, a strategically important U.S. territory in the Pacific.[3] This focus on Guam, along with other critical infrastructure both inside and outside the country, highlights the group's potential to disrupt U.S. military operations and response capabilities in the event of a conflict in the region, such as over Taiwan.[4]

Recent advisories from CISA and partner agencies highlight the urgency of this threat.[5] Volt Typhoon successfully compromised organizations across American critical infrastructure sectors, including Communications, Energy, Transportation Systems, and Water and Wastewater Systems. Their "living off the land" techniques and exploitation of valid accounts

[1] Office of the National Cyber Director, "2024 Report on the Cybersecurity Posture of the United States" (Washington, D.C., May 2024), https://www.whitehouse.gov/wp-content/uploads/2024/05/2024-Report-on-the-Cybersecurity-Posture-of-the-United-States.pdf.

[2] "Countering the Cyberthreat from China," May 15, 2024, https://docs.house.gov/meetings/GO/GO12/20240515/117309/HHRG-118-GO12-Wstate-EvaninaW-20240515.pdf.

[3] David DiMolfetta and Frank Konkel, "Some Volt Typhoon Victims 'Won't Know They're Impacted,' Mandiant CEO Says," *Nextgov.Com (Online)* (Washington: Government Executive Media Group, April 11, 2024), 3037102859, ProQuest Central, http://search.proquest.com.ezp-prod1.hul.harvard.edu/magazines/some-volt-typhoon-victims-won-t-know-they-re/docview/3037102859/se-2?accountid=11311.

[4] CISA et. al., "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure | CISA," February 7, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a; CISA et. al., "PRC State-Sponsored Cyber Activity: Actions for Critical Infrastructure Leaders," 2024.

[5] CISA et. al., "PRC State-Sponsored Cyber Activity: Actions for Critical Infrastructure Leaders"; CISA et. al., "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure | CISA."

allow for long-term, undiscovered persistence, sometimes maintaining access to compromised environments for five years or more.[6]

While China poses the most significant threat, Russia, Iran, and North Korea are also conducting malicious cyber activities against U.S. interests. These and other adversaries are increasingly extending geopolitical conflict into the cyber domain for geopolitical conflict, further amplifying risks to U.S. and allied critical infrastructure.[7]

Beyond direct nation-state threat actors, nation-states are increasingly turning to proxies to conduct their cyber operations.[8] The use of proxies allows a given nation-state to mask their identity and skirt international law while maintaining plausible deniability. This tactic blurs the lines between state-sponsored activities and cybercrime, making attribution and response more challenging. For instance, Russia has become a safe haven for ransomware criminals by allowing these actors to operate with impunity on their soil, complicating international efforts to combat this growing threat. Further, the use of proxies complicates our ability to defend against and deter such attacks and raises significant policy challenges around how to respond and hold accountable the true orchestrators of these cyber activities.

The ransomware threat continues to grow and has effectively democratized the threat landscape, putting a target on everyone's back. No longer is this threat confined to large corporations or high-profile targets; it now impacts organizations of all sizes across every sector. In 2023, nearly 5,200 organizations reported ransomware attacks, and countless more attacks have likely gone unreported.[9] Ransomware’s impact extends beyond financial losses, with such attacks disrupting critical services and potentially threatening lives. For instance, a November 2023 attack on Ardent Health Services, a 30-hospital system, put lives at risk by forcing diversions across three states.[10]

Financially, the costs are significant. Ransom payments in the first half of 2023 were estimated to be $449 million, while individual attacks on major corporations resulted in hundreds of millions in losses.[11] The MGM Resorts attack in September 2023 is estimated to have cost at least $100 million, while the August 2023 Clorox attack is estimated to have cost at least $356 million.[12] Further, the systemic risk to critical infrastructure cannot be overstated. As

[6] CISA et. al., “PRC State-Sponsored Cyber Activity: Actions for Critical Infrastructure Leaders.”
[7] Office of the National Cyber Director.
[8] Mannan.
[9] Matt Kapko, “Elevated Ransomware Activity Hit Nearly 5,200 Organizations in 2023,” Cybersecurity Dive, January 12, 2024, https://www.cybersecuritydive.com/news/elevated-ransomware-activity-2023-rapid7/704476/.
[10] Emsisoft Malware Lab, “The State of Ransomware in the U.S.: Report and Statistics 2023,” Emsisoft | Cybersecurity Blog, January 2, 2024, https://www.emsisoft.com/en/blog/44987/the-state-of-ransomware-in-the-u-s-report-and-statistics-2023/.
[11] Emsisoft Malware Lab.
[12] Emsisoft Malware Lab.

demonstrated by the ICBC attack in late 2023, even a relatively small entity can have an outsized impact on critical systems like the U.S. Treasury market.[13]

The emergence of artificial intelligence (AI) presents both opportunities and risks in the cybersecurity landscape.[14] While AI can enhance defensive capabilities, it also provides cybercriminals with more efficient means of conducting attacks[15]. The potential for AI-generated deepfakes, particularly in audio and video impersonation, presents a new frontier of cyber threats that could compromise authentication systems and facilitate social engineering attacks.

As we confront this evolving threat landscape, it is clear that our approaches to cybersecurity need to evolve, too. The increasing sophistication, scale, and potential impact of cyber threats demand a reimagining of our defense strategies, particularly public-private partnerships. We must move beyond reactive postures and information sharing to more proactive, collaborative approaches that leverage the full spectrum of national capabilities.

Systemically Important Entities

We must identify and prioritize protecting entities whose compromise could have cascading effects on our national security, economic stability, and public health and safety. The concept of Systemically Important Entities (SIEs) emerged as a crucial framework for understanding and addressing the interconnected and interdependent nature of our critical infrastructure.

The recently issued National Security Memorandum 22 (NSM-22) introduces the concept of SIEs, acknowledging that specific organizations and systems have far-reaching impacts that extend beyond their immediate sectors.[16] This recognition is a significant step forward in our national cybersecurity strategy, as it aims to mitigate the potential for widespread disruption that could result from attacks on these key entities.

The criteria for designating SIEs, as outlined in NSM-22, are based on the potential for an entity's disruption or malfunction to cause nationally significant and cascading adverse effects. This updated approach reflects a more current understanding of the complex interdependencies within our critical infrastructure ecosystem. Considering sectors in isolation is no longer sufficient, we must adopt a holistic view that accounts for the ripple effects of cyber incidents across our interconnected systems.

[13] *Treasury's Cyber Defenses and AI Future with Todd Conklin*, 2024, https://www.youtube.com/watch?v=ZaxENpjsTeg.

[14] "How Ransomware Could Cripple Countries, Not Just Companies," *The Economist*, December 31, 2023, https://www.economist.com/international/2023/12/31/how-ransomware-could-cripple-countries-not-just-companies.

[15] *Innovating at Speed: Advancing AI with Teresa Shea and Glenn Gaffney*, 2024, https://www.youtube.com/watch?v=T6Ii0HnqSgQ.

[16] The White House, "National Security Memorandum on Critical Infrastructure Security and Resilience," The White House, April 30, 2024, https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/.

One example is the "tri-sector" approach, which emphasizes the critical and interrelated nature of the finance, energy, and telecommunications sectors.[17] These sectors form the backbone of our modern economy and society, and their resilience is paramount to our national security. The energy sector warrants particular attention due to its fundamental role in enabling all other critical infrastructure operations.

It is important to note that the designation of SIEs extends beyond these three sectors. The designation and support processes must be dynamic and adaptive as threats and technology change. For instance, the increasing reliance on cloud computing and space-based assets necessitates reevaluating what constitutes critical infrastructure in the 21st century. This flexibility allows for the inclusion of other functions that may not fall neatly into traditional sector definitions, ensuring a comprehensive approach to critical infrastructure protection.

While considering what constitutes critical infrastructure in the 21st century, it's crucial to recognize emerging domains that play an increasingly vital role in national and economic security. One such domain is space. The space sector underpins a wide range of critical services, from communication and navigation to surveillance and weather forecasting. Space infrastructure is vital to civil and military operations, making it a prime candidate for designation as a critical infrastructure sector. While NSM-22 takes significant strides in updating our approach to critical infrastructure protection, the omission of space as a designated sector represents a missed opportunity that should be addressed in future policy updates.[18]

Regardless, the identification and protection of SIEs require robust public-private partnerships. Government and industry must actively collaborate to secure these entities. This collaboration must go beyond the traditional “information sharing” approach and move into joint threat analysis, coordinated incident response, and shared responsibility for risk mitigation. Now is the time to reimagine and deepen our public-private cyber partnerships.

Furthermore, we must recognize that the concept of SIEs has international implications. Cyber threats do not respect national boundaries, and many critical systems are globally interconnected. As such, our approach to protecting SIEs must include international cooperation and alignment of cybersecurity standards and practices.

Identifying and protecting SIEs represent an essential evolution in our national cybersecurity strategy. By focusing our resources and efforts on these key nodes within our critical infrastructure, we can more effectively mitigate the risk of catastrophic cyber incidents. However, as mentioned, this approach demands both a reimagining of public-private partnerships and a commitment to continuous adaptation in the face of evolving threats.

[17] CISA Cybersecurity Advisory Committee, “Building Resilience and Reducing Systemic Risk to Critical Infrastructure” (Cybersecurity and Infrastructure Security Agency (CISA), September 13, 2022).

[18] Frank Cilluffo and Alison King, “How to Fine-Tune the White House’s New Critical Infrastructure Directive,” *CyberScoop* (blog), May 1, 2024, https://cyberscoop.com/how-to-fine-tune-the-white-houses-new-critical-infrastructure-directive/.

Rethinking the Public-Private Partnership

As we confront the evolving landscape of cyber threats to our critical infrastructure, it is imperative that we fundamentally reimagine and deepen our approach to public-private partnerships in cybersecurity. While valuable, the traditional model of more information sharing is no longer sufficient to address the sophisticated and persistent threats we face today.

We must acknowledge a stark reality: no company, regardless of size or sector, entered the market expecting to defend itself against the significant strength of foreign military and intelligence services. Yet, this is precisely the challenge our critical infrastructure operators now face. This asymmetry demands a new paradigm of collaboration between government and industry.

The Joint Cyber Defense Collaborative (JCDC), established by the Cybersecurity and Infrastructure Security Agency (CISA), represents a positive step towards more integrated cooperation.[19] It's worth noting that the concept of such a collaborative effort was initially recommended by the Cyberspace Solarium Commission, which led to the creation of the Joint Cyber Planning Office (JCPO) through the FY2021 National Defense Authorization Act.[20]

JCDC, evolving from the JCPO concept, is an operational entity that brings together public and private sector partners to enhance the nation's cyber defenses. JCDC is exceptionally effective at rallying stakeholders around specific crises, such as the Log4j vulnerability. But, there is also an opportunity to enhance day-to-day collaboration and information sharing to further strengthen the collective cybersecurity posture between crises. It's important to recognize that JCDC is still in its early stages and has limitations. It currently involves a relatively small number of members, and there's a clear need to scale this model as we confront increasingly complex and widespread threats.

While JCDC provides a framework for collaboration, more is needed to address the full spectrum of cybersecurity challenges we face. To genuinely have trust and operationalize these partnerships, we need to develop sector-specific approaches that can address different industries' unique challenges and needs.

One promising example of a sector-specific approach is Project Fortress, recently launched by the U.S. Department of Treasury. This initiative aims to enhance cybersecurity in the financial sector by moving beyond a purely defensive posture to a more proactive defense model that includes offensive capabilities.[21]. By creating automated intelligence-sharing pipelines between the U.S. government and the financial sector, Project Fortress demonstrates the potential for deeper, more dynamic public-private collaboration.

[19] Lamar Johnson, “CISA Launching Joint Cyber Planning Office ‘Shortly,’” July 27, 2021, https://www.meritalk.com/articles/cisa-launching-joint-cyber-planning-office-shortly/.

[20] Cyberspace Solarium Commission, “Cyberspace Solarium Commission - NDAA Press Release,” December 3, 2020, https://www.solarium.gov/press-and-news/ndaa-press-release.

[21] *Treasury’s Cyber Defenses and AI Future with Todd Conklin*.

As we consider expanding such models to other critical infrastructure sectors, we must be mindful of small and medium-sized businesses' unique challenges. These enterprises form the backbone of our economy but often lack the resources to participate fully in sophisticated cybersecurity partnerships. We must develop scalable solutions that allow these smaller entities to benefit from and contribute to our collective defense.

To truly turbocharge our public-private partnerships, we should consider establishing collaborative environments that go beyond information sharing to include joint threat hunting, coordinated incident response, and shared defensive operations. These environments could leverage government and industry partners' unique capabilities and perspectives, creating a force multiplier effect against sophisticated adversaries.

Furthermore, we must explore innovative models for risk-sharing between the public and private sectors. This could include new insurance frameworks, government backstops for catastrophic cyber incidents, and incentives for companies that adopt enhanced security measures and participate in collaborative defense efforts.

As we develop these sector-specific approaches, it's important to note that improved harmonization across regulatory and reporting frameworks can help all these efforts while supporting our posture. Harmonization is also particularly important for small and medium-sized businesses, which often lack the resources to navigate complex regulatory structures. Harmonizing will help reduce redundancy and organizational burden while supporting a more effective cybersecurity posture. We cannot afford a check-the-box or lowest-common-denominator harmonization solution. Our approach must be dynamic and focused on continuous improvement rather than merely meeting minimum standards.

As we move forward, it is crucial to recognize that this reimagined partnership is not about shifting all responsibility to the government. Instead, it is about creating an ecosystem where public and private sector strengths are synergistically combined to enhance national cyber resilience. This approach requires transparency, trust-building, and continuous adaptation as the threat landscape evolves.

Insurance and Cybersecurity

The cyber insurance market has experienced significant growth in recent years[22], with global premiums reaching approximately $20 billion by 2025.[23] However, this figure belies the true

[22] Graham Steele, “Remarks by Assistant Secretary Graham Steele at the Federal Insurance Office and NYU Stern Volatility and Risk Institute Conference on Catastrophic Cyber Risk and a Potential Federal Insurance Response,” U.S. Department of the Treasury, June 18, 2024, https://home.treasury.gov/news/press-releases/jy1922.

[23] Sasha Romanosky et al., “Content Analysis of Cyber Insurance Policies: How Do Carriers Price Cyber Risk?,” *Journal of Cybersecurity* 5, no. 1 (January 1, 2019): tyz002, https://doi.org/10.1093/cybsec/tyz002.

extent of organizations' cyber risk exposure.[24] The current state of the market is characterized by underinsurance, with many businesses lacking adequate coverage for the full spectrum of cyber threats they face.[25]

While the insurance industry has made strides in developing cyber risk products, it faces substantial challenges in addressing threats from nation-state actors. These sophisticated adversaries possess capabilities that often exceed the scope of traditional insurance policies, creating a coverage gap that leaves many organizations vulnerable.[26] This limitation is particularly concerning given the increasing frequency and severity of state-sponsored cyber attacks targeting critical infrastructure.[27]

Industry perspectives on the role of cyber insurance and potential government intervention are varied. Some industry leaders have supported a federal framework to address catastrophic cyber risks. At the November 2023 conference co-hosted by the Federal Insurance Office (FIO) and NYU's Volatility and Risk Institute, several insurance executives expressed the need for government involvement in managing systemic cyber risks.[28] However, others in the industry caution against premature government intervention, arguing that the market is still evolving and growing.[29]

The insurance sector has responded to the challenges posed by nation-state threats and potential systemic risks by introducing exclusions for war, nation-state actions, and attacks on critical infrastructure.[30] While these exclusions protect insurers' balance sheets, they leave a significant gap in coverage for the most severe cyber incidents, potentially shifting the burden to policyholders or, ultimately, to the government in the event of a catastrophic attack.

[24] Christiaan Beek, “2023 Ransomware Stats | Rapid7 Blog,” Rapid7, January 12, 2024, https://www.rapid7.com/blog/post/2024/01/12/2023-ransomware-stats-a-look-back-to-plan-ahead/.

[25] Matthew Lerner, “Systemic Cyber Cat Event Could Top Cover Due to Aggregation: Experts,” Business Insurance, November 20, 2023, https://www.businessinsurance.com/article/20231120/NEWS06/912361138/Systemic-cyber-cat-event-could-top-cover-due-to-aggregation-Experts-.

[26] Gianchandani et al., “Dear Colleague Letter: IUCRC Proposals for Research and Thought Leadership on Insurance Risk Modeling and Underwriting Related to Terrorism and Catastrophic Cyber Risks: A Joint NSF and U.S. Department of the Treasury Federal Insurance Office Call (Nsf24082) | NSF - U.S. National Science Foundation”; Lerner, “Systemic Cyber Cat Event Could Top Cover Due to Aggregation”; Federal Insurance Office, “Update on the Federal Insurance Office’s Assessment of a Potential Federal Insurance Response to Catastrophic Cyber Incidents.”

[27] Michael Martina et al., “US Officials Deliver Warning That Chinese Hackers Are Targeting Infrastructure,” *Reuters*, January 31, 2024, sec. Cybersecurity, https://www.reuters.com/technology/cybersecurity/chinese-hackers-are-targeting-us-infrastructure-fbi-chief-testify-2024-01-31/.

[28] Federal Insurance Office, “Update on FIO/NYU Conference on Catastrophic Cyber Risk and a Potential Federal Insurance Response and FIO’s Catastrophic Cyber Insurance Work.”

[29] None, “Tiernan: Systemic Cyber Event Would Undermine Societal Role of the Industry,” Cyber Risk Insurer, June 13, 2024, https://www.cyberrisk-insurer.com/news/tiernan-systemic-cyber-event-would-undermine-societal-role-of-the-industry/.

[30] Jan Larson, “The State Of The Insurance Market For Cyber Incidents - Important Developments From 2023 And Looking Ahead In 2024,” *Mondaq Business Briefing*, February 16, 2024, Gale Business: Insights.

Despite these challenges, the insurance industry is crucial in promoting better cybersecurity practices. Insurers can encourage organizations to implement more robust security controls and improve cyber hygiene through underwriting requirements and pricing incentives. This market-driven approach should significantly enhance the cybersecurity posture of businesses across various sectors.

However, market forces alone are insufficient to address the full spectrum of cyber risks, particularly those posed by nation-state actors. The potential for a catastrophic cyber event that could overwhelm private sector capabilities necessitates considering the government's role in cyber risk management.

One potential solution is developing a cyber insurance framework similar to the Terrorism Risk Insurance Act.[31] Such a program could position the government as an insurer of last resort for catastrophic cyber attacks, providing a backstop for the private insurance market and ensuring that critical infrastructure operators have access to coverage for even the most severe incidents.

It's important to note that any government intervention should be carefully designed to complement private sector efforts rather than replace them. A well-structured program could help grow market capacity and provide stability while still incentivizing businesses to invest in robust cybersecurity measures.

A pilot project could be initiated, focusing on a specific critical infrastructure sector such as energy and power utilities. This pilot could involve collaboration with existing mutual insurance organizations like AEGIS, which already has significant experience in insuring utility companies.[32] By starting with a targeted approach, we can assess the effectiveness of a public-private insurance model and refine it before considering broader applications.

The Office of the National Cyber Director, along with strong partners in the Treasury Department through its Federal Insurance Office and the Department of Homeland Security through the Cybersecurity and Infrastructure Security Agency, would be key players in developing and implementing such a program.[33] Their involvement would ensure the initiative aligns with broader national cybersecurity strategies and critical infrastructure protection efforts.

Creating a robust cyber insurance system also presents a strong business case for enhanced cybersecurity. By setting clear standards for insurance sector involvement and coverage, we can incentivize organizations to improve their security practices. This approach leverages

[31] Larson, "The State Of The Insurance Market For Cyber Incidents - Important Developments From 2023 And Looking Ahead In 2024"; U.S. Department of the Treasury, "Potential Federal Insurance Response to Catastrophic Cyber Incidents," Federal Register, September 29, 2022, https://www.federalregister.gov/documents/2022/09/29/2022-21133/potential-federal-insurance-response-to-catastrophic-cyber-incidents.

[32] Cullen (Associated Electric & Gas Insurance Services Limited) to Ifft (Federal Insurance Office).

[33] Federal Insurance Office, "Summary of Comments on Request for Comment: Federal Insurance Response to Catastrophic Cyber Incidents."

market forces to drive better cybersecurity outcomes, with the government providing support where private sector solutions fall short.

It's crucial to strike the right balance between government intervention and private-sector innovation. While a federal backstop can provide necessary security for catastrophic risks, we must be careful not to stifle growth and innovation in the private sector, encompassing services, technology, and the cyber insurance market. The truth is that innovation shouldn't be stifled in the name of security. The goal should be to create an environment where private companies can continue to develop new products, services, and technologies while insurers expand coverage. Government support should focus on addressing systemic risks that exceed market capacity, particularly in areas of catastrophic attacks, without impeding the natural evolution and improvement of private sector solutions.

As we consider these potential solutions, we must also work to address the unique challenges small and medium-sized businesses face. These organizations, which form the backbone of our economy, often lack the resources to invest heavily in cybersecurity or purchase comprehensive cyber insurance. Any federal program should consider how to extend protection and incentives to these smaller entities through targeted initiatives or support for industry-specific insurance pools.

Conclusion

The cyber threat landscape facing our nation has reached a level that demands a fundamental reimagining of our approach to cybersecurity. As I have shared throughout this testimony, our challenges are multifaceted and evolving, requiring a collaborative response from both the public and private sectors.

Identifying and protecting Systemically Important Entities (SIEs) represents a crucial step forward in our national cybersecurity strategy. By focusing our efforts on these key nodes within our critical infrastructure, we can more effectively mitigate the risk of catastrophic cyber incidents that could have far-reaching consequences for our national security, economic stability, and public safety.

However, the designation of SIEs is just the beginning. We must deepen and turbocharge our public-private partnerships to create a more resilient cybersecurity ecosystem. This reimagined collaboration should go beyond traditional information sharing to include joint threat hunting, coordinated incident response, and shared defensive operations. Initiatives like Project Fortress in the financial sector provide a promising model for this enhanced cooperation.

The role of the insurance sector in this new paradigm cannot be overstated. While market forces and private insurance have driven significant improvements in cybersecurity practices, the limitations of the current cyber insurance market's ability to address nation-state threats and potentially catastrophic events is clear. We must seriously consider the development of a federal insurance response to catastrophic cyber incidents similar to the model provided by the

Terrorism Risk Insurance Act. The time to deliberate and think this through is now, not after a catastrophic incident occurs, rather than scrambling to develop solutions in the aftermath. By proactively considering these issues, we can better prepare our nation's cyber systems to withstand catastrophic incidents.

However, any government intervention must be carefully calibrated to complement rather than replace private sector efforts. A well-designed federal backstop could help grow market capacity and provide stability while still incentivizing businesses to invest in robust cybersecurity measures. The proposed pilot project focusing on the energy sector could serve as a valuable testing ground for this approach.

As we move forward, we must remain mindful of the needs of small and medium-sized businesses, ensuring that our strategies for enhancing cybersecurity and cyber insurance are scalable and accessible to organizations of all sizes.

In conclusion, today's cyber threats require a bold, collaborative, and adaptive response. By reimagining our public-private partnerships, leveraging the power of the insurance sector, and providing targeted government support where necessary, we can build a more resilient and secure digital infrastructure for our nation.

We must also recognize that this is not a one-time effort. As highlighted in the recently released National Cyber Director's Posture Report, the cybersecurity landscape is constantly evolving.[34] We must be prepared to consistently recalibrate our approaches, learn from our experiences, improve our strategies, and adapt to new threats as they emerge.

Our efforts to strengthen national cybersecurity should be seen as an ongoing and interactive improvement process. We must move beyond simply reacting to cyber threats and adopt a more proactive, forward-looking stance. This includes developing effective cyber deterrence strategies tailored to different adversaries, as the tactics that work against one nation-state may differ from those needed to counter others or cybercriminal groups.

The time for action is now, but our commitment must be enduring. We must seize this opportunity to strengthen our collective defense against today's cyber threats while remaining vigilant and adaptable to better protect our economic and national security in the face of tomorrow's challenges.

Thank you again for the opportunity to appear before you today. It is a privilege to contribute to this important conversation and I look forward to trying to answer any questions you may have.

[34] Office of the National Cyber Director, “2024 Cybersecurity Posture Report.”