Testimony Before the Subcommittee on Cybersecurity and Infrastructure Protection
Committee on Homeland Security, U.S. House of Representatives

In Defense of Defensive Measures: Reauthorizing Cybersecurity Information Sharing Activities That Underpin U.S. National Cyber Defense

Diane Rinaldo
May 15, 2025

Chairman Garabino, Ranking Member Swalwell, and Members of the Subcommittee:

Thank you for the opportunity to appear before you today. As someone who was closely involved in the development and passage of the Cybersecurity Act of 2015, I am grateful to speak to the urgent need for its reauthorization and modernization. This Act, which included the Cybersecurity Information Sharing Act (CISA) remains a critical legislative framework that has enabled meaningful cooperation between the public and private sectors. Yet the threat environment has grown dramatically more complex—and our approach must evolve accordingly.

The Growing Cyber Threat Landscape

When the original legislation was drafted in 2012, growing concerns about the frequency and sophistication of cyberattacks were already taking shape. In hindsight, those early warnings significantly underestimated the scale and complexity of today's cyber threat landscape. Over the past decade, threat actors have become more capable and emboldened, exploiting zero-day vulnerabilities, bypassing multi-factor authentication, compromising third-party vendors, and outpacing both legislative safeguards and defensive technologies. High-profile attacks—from the SolarWinds breach to the Colonial Pipeline ransomware incident, from Salt Typhoon to incursions targeting the Office of the Comptroller of the Currency—have made it abundantly clear: no sector, public or private, is immune.

Today, cyber threats are not only more pervasive but also more destructive. Ransomware, state-sponsored espionage, supply chain infiltration, and AI-driven attack vectors now pose existential risks to critical infrastructure, national security, and economic stability.

The proliferation of artificial intelligence promises to supercharge this already volatile landscape. AI enables the creation of life-like audio and imagery, more convincing spear-phishing campaigns, and advanced social engineering tactics. Large language models allow adversaries to write malware and exploit code at unprecedented speed and scale, lowering the technical barriers for would-be attackers. State-backed intelligence and military units are now leveraging these tools to target critical infrastructure, enhance surveillance capabilities, and support offensive cyber operations.

At the heart of the legislation—and what remains just as urgent today—is China's unrelenting assault on the U.S. economy through cyber-enabled espionage. Chinese cyber hacking stands out as one of the most strategically dangerous and persistent threats to national security. For over a decade, state-sponsored actors tied to the People's Liberation Army and China's Ministry of State Security have conducted a sweeping and coordinated cyber-espionage campaign targeting U.S. companies, research institutions, and government agencies. These operations have resulted in the theft of massive troves of intellectual property, trade secrets, source code, and sensitive defense technologies. This is not random or opportunistic—it is a deliberate strategy to fuel China's economic and military ambitions, with cyber capabilities serving as a core instrument of statecraft and industrial policy.

In this evolving threat environment, the need for real-time, bidirectional information sharing between government and industry has never been more critical.

The Legacy of the Cybersecurity Act of 2015

The cyber information sharing laid the foundation for improved collaboration between government agencies and private entities by creating a legal framework for voluntary information sharing. It offered liability protections to encourage private companies to share threat indicators and defensive measures with the federal government and, most importantly, business to business. Our thought was simple: see something, say something.

That framework helped normalize, and de-stigmatize, cyber threat information sharing across industries. The Department of Homeland Security's Automated Indicator Sharing (AIS) program and the role of Information Sharing and Analysis Centers (ISACs) and Organizations (ISAOs) are direct outgrowths of the Act.

The legislation was the product of four years of intensive effort, including over 100 meetings with stakeholders ranging from Fortune 100 companies to small and medium-sized businesses, privacy advocates, and academic institutions. It also reflected countless consultations with government agencies and underwent three major rewrites based on the feedback received. From the outset, the Committee recognized the critical need to strike the right balance between privacy and security. With so much at stake, we knew we had to get it right.
However, while the law was forward-thinking at the time, the pace of technological change and the growing complexity of cyber threats have outpaced some of its provisions.

Despite progress, several key gaps remain:

1. **Limited Participation**: Many private-sector entities, particularly small and mid-sized businesses, still hesitate to share information due to uncertainty about liability protections and limited resources.

2. **Speed and Relevance**: The timeliness and utility of shared data can be inconsistent. Automated platforms are underutilized, and actionable intelligence does not always flow quickly enough to prevent or mitigate attacks.

3. **Lack of Bidirectional Flow**: While private entities are encouraged to share data with the government, the feedback loop is often one-way. Companies need useful, contextualized threat intelligence in return.

4. **Inconsistent Standards**: Threat data is not always shared in a standardized, machine-readable format, limiting its utility at scale.

5. **Trust Deficit**: Public trust in government handling of sensitive data—particularly in sectors like finance and healthcare—remains a concern. Transparency, oversight, and accountability must be strengthened.

Reauthorizing the Cybersecurity Information Sharing Act gives Congress the opportunity to strengthen and scale its original vision. To strengthen national cybersecurity, Congress should expand and clarify liability protections to encourage broader information sharing. Businesses, particularly those outside of traditionally designated "critical infrastructure" sectors, need clear legal assurances that they will be shielded when acting in good faith. The scope of protected activities must be explicitly defined to eliminate ambiguity and foster participation. Small and medium enterprises, which often lack dedicated personnel or technical expertise, should be supported for training, toolkits, and access to threat-sharing ecosystems like Information Sharing and Analysis Centers (ISACs). Additionally, federal agencies such as CISA must be required—not merely allowed—to share timely, relevant, and declassified intelligence with the private sector. Trust and engagement improve significantly when companies see tangible reciprocity.

Cybersecurity is no longer a technical issue; it is a national security imperative that requires whole-of-nation coordination. No single company, agency, or state can defend against these threats alone. The adversaries we face—whether criminal networks or foreign governments—exploit our silos. We must instead leverage our strengths: diversity of talent, innovation, and democratic collaboration.

The reauthorization of information sharing presents a generational opportunity. We can reinforce our values, secure our systems, and create a more resilient digital economy by recommitting to a collaborative model built on transparency, accountability, and mutual support.

In closing, I urge this committee to quickly modernize and reauthorize this critical function. Let us affirm the importance of information sharing, strengthen the incentives and protections for participants, and build the trusted, interoperable, and actionable threat-sharing ecosystem our future demands.

Thank you again for the opportunity to testify.