Written Testimony of Karl Schimmeck, Chief Information Security Officer of Northern Trust, on behalf of the Securities Industry and Financial Markets Association (SIFMA)

Before the U.S. House of Representatives

Committee on Homeland Security

Cybersecurity and Infrastructure Protection Subcommittee

Hearing Entitled:

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

May 15, 2025

Introduction

Chairman Garbarino, Ranking Member Swalwell and distinguished members of the Subcommittee, thank you for the opportunity to testify today in favor of the reauthorization of the *Cybersecurity Information Sharing Act of 2015* ("CISA 2015" or the "Act").[1] My name is Karl Schimmeck. I am an Executive Vice President and Chief Information Security Officer of Northern Trust, responsible for the design and management of the bank's information security, cybersecurity, and data protection programs. I am here today as a representative of the Securities Industry and Financial Markets Association ("SIFMA") where I am a member of the Cybersecurity Committee. I am also on the Board of Directors of the Financial Services Information Sharing and Analysis Center ("FS-ISAC").

Prior to my current position at Northern Trust, I served as Chief Information Security Officer and Head of Technology Risk and Resilience for Morgan Stanley's U.S. banks. Prior to that, I was Managing Director of Cybersecurity, Business Resiliency & Operational Risk at SIFMA from 2011 to 2016, during which I was involved in the advocacy efforts for CISA 2015. During that time, I was also on the executive committee of the Financial Services Sector Coordinating Council ("FSSCC").

SIFMA is the leading trade association for broker-dealers, investment banks, and asset managers operating in the U.S. and global capital markets. SIFMA advocates on legislation, regulation and business policy affecting financial markets and serves as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency.

As part of its critical role as a coordinating body and as it relates to this hearing, SIFMA hosts an bi-annual cybersecurity exercise known as Quantum Dawn which brings together public and private sector participants for a series of exercises that simulate the operational impacts that a systemic cyber-attack could have on financial firms, critical third parties, and the global financial ecosystem due to a large scale attack. Last year's exercise included more than 1000 participants from 20 countries. The goal of the exercise is to improve response and recovery plans and strengthen global coordination and information sharing mechanisms which are necessary for quickly responding to significant operational outages, including cyber events.[2]

Certain key provisions of CISA 2015 are set to expire in September if Congress does not reauthorize them. SIFMA is calling for a clean reauthorization of the expiring provisions of CISA 2015 as soon as possible so that participating institutions will have the necessary assurances that the existing protections will continue. These expiring provisions include liability protections for private companies when sharing information pursuant to the Act – protections that are

[1] Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, Div. N, Title I—Cybersecurity Information Sharing Act of 2015, 129 Stat. 2935 (2015), 6 U.S.C. § 1501; S. Rep. No. 114–32, at 2 (2015).

[2] Press release, SIFMA Cybersecurity Exercise, Quantum Dawn VII After-Action Report (May 1, 2024), https://www.sifma.org/resources/general/cybersecurity-exercise-quantum-dawn-vii/

essential to the collective protection of the US via the enhanced situational awareness that information sharing provides. It is critical that Congress reauthorize these provisions to preserve information sharing before they expire.

CISA 2015 Background and Reauthorization

Since its bipartisan passage ten years ago, CISA 2015 has become a vital part of cyber defense by providing a robust legal and operational framework for voluntarily sharing information between the public and private sector in the United States. The financial services industry has since become reliant on the Act's legal framework and protections, which have proven necessary on many occasions. In the decade since its enactment, the law has meaningfully improved the capacity and speed with which we can respond to large-scale cyber incidents while establishing clear expectations for privacy and confidentiality. This includes building the structures used by private sector cyber defenders to inform government partners of ongoing cyber threats from malicious actors.

The Act provides a formalized foundation for firms to voluntarily collaborate with both the federal government and other institutions to share necessary information to protect investors and the financial markets from cybercriminals seeking financial gain and nation states seeking to disrupt orderly markets and critical infrastructure. This foundation is largely based on legal and liability protections granted to the private sector to further promote voluntary sharing of cyber threat indicators and defensive measures to help prevent imminent cyber threats. Public and private sector participants primarily share this information through the Cybersecurity and Infrastructure Security Agency's ("CISA") Automated Indicator Sharing Program ("AIS") which operates a server that allows public and private participants to share cyber threat indicators.[3] Once that information is analyzed and appropriately sanitized including the removal of personally identifiable information ("PII"), AIS shares indicators or defensive measures submitted by government agencies and private sector entities with all AIS participants. This information may also be compared and used in conjunction with post-incident information reporting required under the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA") to prevent future incidents.[4] Further, information sharing under CISA 2015 benefits financial institutions of all sizes and business models, not just large firms.

At the time of passage, there were some concerns about protecting the privacy of individuals when cyber threats were reported under CISA 2015. After 10 years of activity, no AIS participants (public or private) have been known to report PII that was not directly related to a cybersecurity incident pursuant to CISA 2015.[5] The participants in this system have a

[3] Cong. Rsch. Serv., *The Cybersecurity Information Sharing Act of 2015: Expiring Provisions* (Apr. 8, 2025), https://www.congress.gov/crs_external_products/IF/PDF/IF12959/IF12959.4.pdf.
[4] 6 U.S.C. §§ 681a-681b.
[5] Dep't of Homeland Sec. Off. of the Inspector Gen., *CISA Faces Challenges Sharing Cyber Threat Information as Required by the Cybersecurity Act of 2015*, OIG 24-60 (Sept. 25, 2024), https://www.oig.dhs.gov/sites/default/files/assets/2024-09/OIG-24-60-Sep24.pdf.

responsibility to ensure that the only information submitted to AIS is directly related to a cybersecurity threat. All AIS participants are responsible for scrubbing any PII not directly related to cybersecurity threats prior to submission. Further, CISA has additional automated controls to identify potential PII in reports prior to dissemination through the AIS. Flagged information is reviewed and approved by designated CISA staff before it is sent out through AIS.

The U.S. Government and the private sector face daily cyber threats that require cross-sector information sharing to capably combat.

The reality of the ongoing threats to financial institutions, federal and state governments, and the general public cannot be overstated. Nation-state hackers have launched numerous attacks on U.S. critical infrastructure[6] including our communications systems—signaling they are positioning for bigger, more disruptive attacks. Federal agencies have similarly been targeted—most recently the Treasury Department in the BeyondTrust breach[7], the SolarWinds incident in which nine agencies were compromised[8], and the Office of the Comptroller of the Currency email breach this year.[9] Unfortunately, foreign cybercriminals continue to target U.S. companies through various tactics, such as phishing and ransomware, making information sharing essential to defending our critical infrastructure against such threats.[10] Further, a recent report found that two-thirds of financial institutions faced cyber-attacks in 2024.[11] The threat is real, its increasing in volume, speed and sophistication; effective information sharing is one of the best ways we can work together against this growing risk.

---

[6] Dustin Volz et al., *How Chinese Hackers Graduated From Clumsy Corporate Thieves to Military Weapons*, WALL ST. J. (Jan. 4, 2025), https://www.wsj.com/tech/cybersecurity/typhoon-china-hackers-military-weapons-97d4ef95; Nat'l Counterintelligence and Sec. Ctr. & Off. of Cybersecurity Exec, *SolarWinds Orion Software Supply Chain Attack* (Aug. 19, 2021), https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/SolarWinds%20Orion%20Software%20Supply%20Chain%20Attack.pdf.

[7] Arielle Waldman, *CISA: BeyondTrust breach affected Treasury Department only*, TECHTARGET (Jan. 7, 2025), https://www.techtarget.com/searchsecurity/news/366617777/CISA-BeyondTrust-breach-impacted-Treasury-Department-only.

[8] Nat'l Counterintelligence and Sec. Ctr. & Off. of Cybersecurity Exec., *SolarWinds Orion Software Supply Chain Attack* (Aug. 19, 2021), https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/SolarWinds%20Orion%20Software%20Supply%20Chain%20Attack.pdf.

[9] Office of the Comptroller of the Currency, *OCC Notifies Congress of Incident Involving Email System*, News Rel. 2025-30 (April 8, 2025), https://occ.gov/news-issuances/news-releases/2025/nr-occ-2025-30.html.

[10] Office of the Dir. Of Nat'l Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community*, (March 18, 2025). https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf

[11] Tom Kellerman, *Modern Bank Heists Report 2025*: *Executive Summary*, at 4 (Contrast Sec. 2025).

Legal protections under CISA 2015 are necessary to facilitate information sharing by and among private companies.

CISA 2015 provides legal and liability protection for entities that share cyber threat indicators pursuant to the Act. Prior to CISA 2015, existing laws did not clearly shield private entities from regulatory enforcement actions, civil actions, or antitrust enforcement actions when sharing cyber threat information. Likewise, the law did not explicitly preserve legal protections, like attorney-client privilege, or safeguards for trade secrets and proprietary information shared with the government or with other private entities for the purpose of preventing cyber-attacks. CISA 2015 provided a clearer legal framework, outlining what information can be shared and how that information should be shared to retain these legal protections. Such protections encourage voluntary information sharing, which has become necessary for defending against cyber threats.

1. Protection from Civil Liability

Under the Act, if a private entity shares a cyber threat indicator or a defensive measure in accordance with CISA's procedures, it is protected from civil lawsuits that might otherwise arise from such sharing.[12] The conditions for civil liability protections include sharing information in compliance with the Act's privacy and data handling requirements and when sharing information with the federal government, doing so only through CISA's prescribed process. As a result, if a financial institution sends an IP address associated with malware to AIS in compliance with the Act, the firm cannot be held liable for a breach of privacy or other civil right of action in connection with that information sharing.

2. Protection from Antitrust Liability

CISA 2015 provides critical protection from antitrust liability for private entities that share covered information with the federal government or other private entities in accordance with the Act.[13] As with the other legal protections provided under the Act, the information must be shared only in accordance with CISA 2015 and only used for the purpose of cybersecurity. In particular, the Act's antitrust exemption and associated protections have provided important assurances and therefore also facilitated broader cyber information sharing between private companies.

3. Protection from Regulatory Enforcement Action

CISA 2015 provides that sharing cyber threat information or defensive mechanisms shall not be used by federal regulators to take enforcement action against the sharing entity. This protection encourages financial institutions to share information voluntarily by providing assurance that such information will not be used against them in an enforcement proceeding brought by the

[12] 6 U.S.C. §1505.
[13] 6 U.S.C. § 1503(e)(1).

Securities and Exchange Commission or other prudential regulators so long as that information is shared within the Act's stated parameters.

4. No Waiver of Privileges or Protections

Sharing cyber threat information under CISA does not waive any applicable privilege or legal protection, including attorney-client privilege and protections for trade secrets and proprietary business information. These provisions ensure that institutions can share indicators without fearing loss of legal protections over that information.

5. Controlled Government Use

Information shared under the Act may be retained and used by the federal government only for limited purposes including for cybersecurity, investigating or prosecuting certain crimes (e.g., cybercrime, identity theft, or serious violent crimes), and certain national security matters. This provision provides assurances to the private sector that the information they share voluntarily will not be used for purposes other than what was intended when disclosed.

Public-private information sharing has been beneficial to the financial services industry.

There are many examples where public-private information sharing has helped to mitigate significant cybersecurity threats impacting financial institutions. For example, during the SolarWinds incident SIFMA, FSSCC, and other organizations were able to quickly identify the impact areas thanks to information sharing among members but also with CISA and other federal agencies. Even risks posed by non-malicious events in the CrowdStrike software update which caused a widespread outage in the financial services industry. This event demonstrated how well CISA's sharing and notification systems helped to improve resilience in the financial services industry and beyond.[14] The ability to fend off imminent cyber threats through information sharing cannot be emphasized enough and these are just two examples of such events.

A lapse in the legal framework provided in the Act could discourage essential information sharing.

A lapse in the legal framework provided in the Act could limit cyber threat information sharing. These communication channels formalized under CISA 2015 are essential for enhancing overall awareness of national security threats and quickly responding to incidents.

Without these legal safeguards, the flow of information would slow significantly, leaving critical vulnerabilities and awareness of malicious activity unreported. Because information shared under the Act is related to cyber threats, that information may help prevent imminent cyber events before they happen, preserving time and resources that would be expended on the

[14] Kapko, Mike, *CrowdStrike snafu was a 'dress rehearsal' for critical infrastructure disruptions, CISA director says*, Cybersecurity Dive (Aug. 8, 2024), https://www.cybersecuritydive.com/news/crowdstrike-critical-infrastructure-resiliency-cisa/723712/.

resolution of the event. While post-incident reporting also helps to prevent future attacks, such information may not be as useful for protecting against an impending threat.

In addition, these statutory provisions have been incorporated by reference to other significant cyber laws like CIRCIA—making reauthorization all the more critical.[15]

Conclusion

In closing, SIFMA and the financial services industry remain committed to strengthening the cybersecurity of our nation's critical infrastructure. CISA 2015 has been a vital tool in building the trust, structure, and legal certainty needed for effective, real-time collaboration between the private sector and government. It has made our institutions more resilient, our responses more coordinated, and our defenses more adaptive.

Allowing the Act to lapse would weaken one of the most constructive public-private partnerships in cybersecurity policy to date. We respectfully urge this Subcommittee and Congress to act swiftly to reauthorize CISA 2015.

[15] *See* 6 U.S.C. § 681a.