ITI Promoting Innovation Worldwide

Written Testimony of

John Miller
Senior Vice President of Policy and General Counsel
Information Technology Industry Council (ITI)

Before the

Committee on Homeland Security
Subcommittee on Cybersecurity and Infrastructure Protection

United States House of Representatives

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

May 15, 2025

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

Written Testimony of
John Miller
Senior Vice President of Policy and General Counsel
Information Technology Industry Council (ITI)

Before the
Committee on Homeland Security
Subcommittee on Cybersecurity and Infrastructure Protection
United States House of Representatives

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

May 15, 2025

Chairman Garbarino, Ranking Member Swalwell, and Distinguished Members of the Subcommittee on Cybersecurity and Infrastructure Protection, thank you for the opportunity to testify today. My name is John Miller, Senior Vice President of Policy and General Counsel at the Information Technology Industry Council (ITI).[1]

ITI represents eighty of the world's leading information and communications technology (ICT) companies. We promote innovation worldwide, serving as the ICT industry's premier advocate and thought leader in the United States and around the globe. ITI's membership comprises leading innovative companies from all corners of the technology sector, including hardware, software, digital services, semiconductor, network equipment, cloud, artificial intelligence (AI), cybersecurity and other internet and technology-enabled companies that rely on ICT to evolve their businesses. Our companies service and support the global ICT marketplace via complex supply chains in which products are developed, made, and assembled in multiple countries, and service customers across all levels of government and the full range of global industry sectors, including financial services, healthcare, and energy. We, thus, not only acutely understand the importance of cybersecurity as a global priority for governments, companies, and customers and critical to our collective security, but our members can also attest to the complexities of demonstrating compliance with diverging or duplicative regulations in the U.S. and around the world.

I lead ITI's Trust, Data, and Technology policy team, including our work on cybersecurity, supply chain resiliency, privacy, artificial intelligence, data, and related policy issues in the United States (U.S.) and globally. I have deep experience working on public-private initiatives with the Department of Homeland Security (DHS), the Cybersecurity and Infrastructure Security Agency (CISA), and other federal agencies. Currently, I serve as the co-chair of the CISA-sponsored Information and Communications Technology

[1] The Information Technology Industry Council (ITI) is the premier global advocate for technology, representing the world's most innovative companies. Founded in 1916, ITI is an international trade association with a team of professionals on four continents. We promote public policies and industry standards that advance companies on and innovation worldwide. Our diverse membership and expert staff provide policymakers the broadest perspective and thought leadership from technology, hardware, software, services, manufacturing, and related industries. Visit https://www.itic.org/ to learn more.

Supply Chain Risk Management Task Force (ICT SCRM Task Force) and on the Executive Committee of the Information Technology Sector Coordinating Council (IT-SCC), the principal IT sector partner to CISA on critical infrastructure protection and cybersecurity policy. I have also previously served as an industry representative to the Enduring Security Framework (ESF), and on multiple National Security and Telecommunications Advisory Committee (NSTAC) subcommittees, most recently as an appointee to the Subcommittee on Addressing the Misuse of Domestic Infrastructure by Foreign Malicious Actors.

Introduction

I am honored to testify before you today on an issue that is critical to our collective national and cybersecurity, as well as an issue of personal interest for me given my long-standing experience as an industry representative to many public-private partnerships where information sharing is a foundational, core goal. Like the other cybersecurity policy and legal experts appearing on this witness panel and many others, I spent several years discussing, debating, and working with policy makers, as well as industry and civil society representatives, on the statute that would ultimately become the *Cybersecurity Information Sharing Act of 2015* (hereinafter CISA 15). I will recount some of those challenges later in my testimony in the hopes of illustrating the progress gained from the hard-won compromises that led CISA 15 to become a cornerstone of the modern cyber threat information sharing ecosystem.

Over the last decade, CISA 15 has strengthened America's cyber defenses by incentivizing and facilitating the sharing of cyber threat information. Any lapse of CISA 15 would create significant uncertainty, weaken the U.S. cybersecurity posture, and undermine a decade of progress in building trust between national security, law enforcement, critical infrastructure owners and operators and others in industry. It is axiomatic that in cybersecurity, no single company or agency has a complete picture of the threat; it is, thus, the real-time aggregation of threat intelligence from many sources that allows us to detect, counter, or mitigate new attacks before they spread.

A failure to renew CISA 15 could be interpreted by malicious actors as the U.S. "dropping its guard" and would be an unforced error in a dangerous and evolving moment of cyber risk for the U.S. The lapse of CISA 15 would remove the legal protections underlying the trust mechanisms and relationships that underpin the cyber threat information sharing that is fundamental to our collective cyber defense. The one guarantee of a lapse in the CISA 15 authority is that attackers would be in a better position to capitalize on any resulting confusion and uncertainty caused by a lapse in CISA 15.

I urge Congress to act swiftly to reauthorize the Cybersecurity Information Sharing Act of 2015 and preserve an authority that is foundational to many collaborative cybersecurity activities in the U.S.

How CISA 15 Became Law

Prior to the passage of CISA 15, cyber threats were escalating at an alarming rate. Meanwhile, legal uncertainty often constrained the ability of incident responders to communicate with one another. Many companies feared that sharing indictors of compromise, technical information on vulnerabilities, defensive measures, or other cybersecurity information could violate privacy laws, antitrust or disclosure rules, or create regulatory exposure. In short, the legal uncertainties surrounding private-sector cyber threat information sharing created a chilling effect that constrained some companies from

sharing threat data and intelligence that could prevent or mitigate potential targets from becoming victims.

The pre-CISA 15 era was marked by strong consensus among cybersecurity professionals, industry stakeholders, and policymakers in both Congress and the executive branch that something needed to be done to improve the threat information sharing ecosystem in the U.S. However, that shared recognition of the problem did not quickly result in passage of the much-needed law. Finding agreement on cyber threat information sharing policy among national security, law enforcement, and homeland security stakeholders was a challenge unto itself. The challenge was only exacerbated when balancing those equities against the interests of a wide array of stakeholders across industry and the privacy and civil liberties communities.

A. CISPA and Privacy Concerns

The push for cybersecurity information sharing legislation began in earnest around 2011.[2] The first major legislative effort, the *Cyber Intelligence Sharing and Protection Act (CISPA)*, had broad bipartisan support with 111 Republican and Democratic co-sponsors in the House.[3] The bill stalled in the Senate after President Obama threatened to veto the bill arguing that "the law repeals important provisions of electronic surveillance law without instituting corresponding privacy, confidentiality and civil liberties safeguards."[4]

The tech sector strongly supported the concept of voluntary information sharing and argued it could and should be done in a way that protected privacy. In April 2012, ITI helped organize a coalition of major technology associations to urge Congress to move forward with a "balanced threat information sharing system" as part of a national cybersecurity strategy.[5] We emphasized that cybersecurity was not a partisan issue and that "from the perspective of America's major innovators, there is no Republican cybersecurity or Democratic cybersecurity. There is only American cybersecurity, where urgent action is needed."

While proponents of CISPA argued that information sharing would help stem the "hemorrhaging" of U.S. company data to China and Russia, privacy and civil liberty groups raised legitimate concerns that the

---

[2] In May 2011, the Administration unveiled a legislative proposal. The proposal contained problematic regulatory elements, which the Administration later abandoned when it issued EO 13636. However, the commitment to incentivizing greater information sharing was a bipartisan, public-private constant at this time, from all quarters - Admin, Congress, and industry. Howard A. Schmidt, The Administration Unveils its Cybersecurity Legislative Proposal, The White House, posted May 12, 2011, available at https://obamawhitehouse.archives.gov/blog/2011/05/12/administration-unveils-its-cybersecurity-legislative-proposal.

[3] Cyber Intelligence Sharing and Protection Act of 2011, H.R. 3523, H.Rept. 112-445. 112th Congress, available at https://www.congress.gov/bill/112th-congress/house-bill/3523.

[4] Cybersecurity bill CISPA passes US House, bbc.com, posted April 27, 2012, available at https://www.bbc.com/news/world-us-canada-17864539.

[5] Tech Sector Unites Behind Cybersecurity Plan, ITI Press Release, dated April 18, 2012, available at https://itic.genb.pro/news-events/news-releases/tech-sector-unites-behind-cybersecurity-plan#:~:text=WASHINGTON%2C%20D,balanced%20threat%20information%20sharing%20system.

new authorities could be used for "nefarious purpose[s]."[6] Civil liberties groups feared that information sharing might become a backdoor for government surveillance, funneling personal data to intelligence agencies. ITI recognized early on that those concerns were not without merit and advocated that trust had to be built into any information-sharing framework by safeguarding privacy and civil liberties. We actively engaged with privacy advocates to help find common ground, and publicly lauded the efforts of CISPA's sponsors to work with groups like the Center for Democracy and Technology (CDT) to make sure that important privacy safeguards were included in any information sharing bill. When CDT announced it would not oppose CISPA's progress after key changes, ITI praised the "constructive dialogue between bill sponsors and privacy groups" that improved the bill and helped "balance privacy concerns."[7]

B. Cybersecurity Act of 2012 and Passage of CISA 15

The House did pass an information sharing bill in 2012 but the leading comprehensive, bipartisan Senate bill, the Cybersecurity Act of 2012 (S.3414) failed to overcome a filibuster.[8] Opposition to the Senate bill was due in part to a lack of consensus on how to craft a balanced legal regime for information sharing. Nonetheless, information sharing was the constant element with bipartisan support across legislative efforts and proposals from the Obama administration.

The next few years saw both progress and new challenges. Cyber-attacks on U.S. companies and government agencies continued unabated, keeping pressure on lawmakers to act. President Obama, via multiple executive orders, encouraged voluntary information sharing.[9] But Congress needed to legislate to address removing the real and perceived legal barriers so as to incentivize increased information sharing. By mid-2013, revelations about U.S. government surveillance programs had come to light, eroding trust in sharing information with government more broadly. Many in the public and Congress became wary of any bill that might inadvertently expand intelligence agencies' access to private data.

To address these concerns, one of the core principles ITI pushed for was to channel information sharing through a civilian agency – specifically, the Department of Homeland Security (DHS) – rather than directly to intelligence agencies. In ITI's view, having DHS serve as the "civilian interface" for the program would help reassure the public that information was not simply feeding into a black box at the

---

[6] Hayley Tsukayama, CISPA: Who's for it, who's against it and how it could affect you, The Washington Post, dated April 27, 2012, available at https://www.washingtonpost.com/business/technology/cispa-whos-for-it-whos-against-it-and-how-it-could-affect-you/2012/04/27/gIQA5ur0lT_story.html.

[7] ITI Applauds Privacy Agreement between CISPA Sponsors and CDT, ITI Press Release, dated April 24, 2012, available at https://www.itic.org/news-events/news-releases/iti-applauds-privacy-agreement-between-cispa-sponsors-and-cdt#:~:text=Dean%20Garfield%2C%20President%20and%20CEO,%E2%80%9D.

[8] Michael S. Schmidt, Cybersecurity Bill Is Blocked in Senate by G.O.P. Filibuster, The New York Times, dated August 2, 2012, available at https://www.nytimes.com/2012/08/03/us/politics/cybersecurity-bill-blocked-by-gop-filibuster.html.

[9] President Obama Signs Executive Order on Cybersecurity Information Sharing, hunton.com, posted February 17 2015, available at https://www.hunton.com/privacy-and-information-security-law/president-obama-signs-executive-order-cybersecurity-information-sharing See Executive Order 13636, February 12, 2013, available at https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity and Executive Order 13691, February 13, 2015, available at https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari.

National Security Agency (NSA). By 2014, this concept had gained traction as the 113th Congress drew to a close. To further bolster the privacy protections in the bill, ITI also pressed for provisions to ensure that any shared data would be "anonymized" or stripped of personal information to the extent possible prior to sharing. The goal was to share threat indicators (like malicious IP addresses, signatures of malware, etc.), not personal information about individuals.

The 114th Congress took up the effort with fresh urgency, partly spurred by high-profile breaches like the massive OPM federal data breach in mid-2015. Throughout 2015, as the bill advanced, ITI advocated for key provisions that we believed would make the information-sharing framework both effective and responsible – notably voluntary participation, multi-directional sharing (private to government, government to private, and private to private sharing), and protecting privacy through data minimization.[10]

The result was a bill that addressed the private sector's needs to incentivize greater sharing (by providing liability protections and clarity that it was lawful for the private sector to share data) while building in the privacy safeguards and civilian government oversight that many stakeholders demanded. By late 2015, a bipartisan consensus had finally coalesced around this balanced approach. CISA 15 was passed by the Senate with strong bipartisan support and was ultimately enacted in the year-end omnibus funding bill.

One key takeaway relevant to today's hearing is this: even in the face of an urgent need and rising threats, it took half a decade of work to get to finally enact an information sharing law. Along the way, Congress and other stakeholders had to navigate legitimate concerns about privacy and the role of intelligence agencies, amongst others. Since its passage, CISA 15 has become a cornerstone legal authority that underpins a multitude of information sharing organizations, forums, and activities both within the private sector and between the private sector and the public sector.

While privacy concerns were constantly at the forefront of the cybersecurity information sharing conversation in the years leading up to CISA 15, looking back we can see that the carefully negotiated and constructed privacy provisions[11] have proven effective. DHS[12] and the Intelligence Communities[13]

---

[10] *Id.*

[11] U.S. Department of Homeland Security and U.S. Department of Justice, Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015, dated April 2025, available at https://www.cisa.gov/sites/default/files/2025-04/CISA%202015%20PCL%20Final%20Guidelines%20Periodic%20Review%20%28April%202025%29%20Final-508.pdf.

[12] U.S. Department of Homeland Security Office of Inspector General, CISA Faces Challenges Sharing Cyber Threat Information as Required by the Cybersecurity Act of 2015, dated September 25, 2024, available at https://www.oig.dhs.gov/sites/default/files/assets/2024-09/OIG-24-60-Sep24.pdf?utm_source.

[13] Office of the Inspector General of the Intelligence Community, Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015, dated December 12, 2023, available at https://www.oversight.gov/sites/default/files/documents/reports/2024-01/Joint-Report-Implementation-Cybersecurity-Information-Sharing-Act-2015AUD-2023-002Unclassified.pdf#:~:text=civil%20liberties%20of%20United%20States,adverse%20effects%20were%20not%20necessary.

Inspectors General both investigated the CISA 15 program in 2023 and 2024 and found no evidence of adverse privacy and civil liberty effects of the law. The fact is that zero reported incidents regarding leakage of personal data over the course of nearly 10 years provide convincing evidence to demonstrate the effectiveness of the statute's privacy safeguards.

How CISA 15 Enables Information Sharing and What's at Stake if Congress Does Not Act

Since its enactment, CISA 15 has meaningfully improved the capacity and speed with which we can respond to cyber incidents while establishing clear expectations for privacy and confidentiality. CISA 15 helped foster and expand a vast network of cyber information sharing organizations at the federal, state, and local levels, in addition to 28 Information Sharing and Analysis Centers (ISACs) for specific industry sectors.[14] ISACs serve as trusted entities to exchange and share cyber and physical threat information, allowing for sector-wide situational awareness, 24/7 threat warnings, incident reporting, and response.[15] ISACs also share with each other, including through the National Council of ISACs and directly with each other to facilitate and coordinate cross-sector sharing and collaboration. The Multi-State ISAC additionally facilitates sharing and collaboration amongst state, local, tribal and territorial government entities. This network of ISACs, and other Information Sharing and Analysis Organizations (ISAOs), non-governmental organizations, and security operations centers does more than improve visibility into hackers' activities. These networked entities enhance our ability to mitigate risks, conduct threat hunting activities, and close technical vulnerabilities.

Relatedly, I understand there has been criticism of the Automated Indicator Sharing (AIS) program authorized by CISA 15, specifically for the apparent decrease in participants and volume of threat indicators shared through the platform. However, such criticisms overlook the fact that back in 2015, widespread automated sharing of threat indicators at scale was an aspiration that CISA 2015 helped turn into a reality. As Scott Algeier, Executive Director of the IT-ISAC, recently argued, "While measuring the number of companies directly sharing is interesting, it doesn't necessarily reflect how the industry shares information. Thousands of companies belong to ISACs, including the IT-ISAC and many of our peers in the National Council of ISACs who participate in the DHS AIS program. Leveraging the ISACs and our collective member companies provides scale for DHS to share with thousands of companies. Any assessment of industry's participation should include the thousands of companies who participate through ISACs."[16] The fact is that AIS as envisioned by CISA 15 laid the groundwork for countless public and private organizations to share automated indicators at scale, and there now exist a multitude of forums and venues to conduct threat sharing that did not exist in 2015 and are reliant upon the protections and mechanisms established by CISA 15.[17]

---

[14] National Council of ISACs website, last visited May 12, 2025, https://www.nationalisacs.org/. "Formed in 2003, the [National Council of ISACs (NCI0)] today comprises 28 organizations. It is a coordinating body designed to maximize information flow across the private sector critical infrastructures and with government. Critical infrastructure sectors and subsectors that do not have ISACs are invited to contact the NCI to learn how they can participate in NCI activities."

[15] *Id.*

[16] Scott Algeier, A Decade of CISA 2015: Reviewing its Effectiveness, IT-ISAC Blog, posted May 12, 2025, available at https://www.it-isac.org/post/a-decade-of-cisa-2015-reviewing-its-effectiveness.

[17] *Id.*

Equally important, the law's antitrust exemption and associated protections, such as protections from Freedom of Information Act (FOIA) disclosure and regulatory use have facilitated broader cyber information sharing between private sector organizations and set the stage for expanding non-governmental cyber threat sharing organizations. As discussed above, legal ambiguities in privacy and antitrust law and potential regulatory exposure chilled the sharing of cyber threat information prior to the passage of CISA 15. These protections removed those legal barriers to incentivize increased sharing and spurred the modern information sharing ecosystem to grow over the last ten years.

A lapse in CISA 15 liability protections would remove the legal scaffolding that federal, state, and local governments and private sector entities rely on to conduct many of their day-to-day cybersecurity operations. Below, I outline three categories of consequences that such a lapse would have, both legally and operationally, for our nation's cybersecurity.

- **Chilling of Threat Information Sharing:** Companies would lose the liability protections and safe harbors from antitrust rules and regulatory use that currently encourage them to share cyber threat indicators and defensive measures. Without these assurances and the business certainty, stability, and predictability they provide, many organizations will likely, and understandably, become more reluctant to share sensitive threat information due to concerns regarding potential negative legal and regulatory consequences.

- **Loss of Real-Time Visibility and Early Warnings for State, Local and Federal Government:** Government entities – including DHS, law enforcement, and the intelligence community, as well as state, local tribal and territorial government entities – would likely begin to lose access to a great volume of voluntarily shared threat intelligence from private sector partners. Indeed, the CISA 15 framework is now fundamental to how industry and agencies collaborate and work together when cyber incidents arise. Key examples include critical infrastructure sectors from finance to energy which have expanded their role and reach since the passage of CISA 15. The law also enabled the DHS/CISA to establish the Joint Cyber Defense Collaborative (JCDC),[18] which facilitates real-time sharing of threat alerts and coordinated operational collaboration and response planning among public and private partners.

- **Undermining Trust and Deterrence:** A lapse of CISA 15 would signal a broader retreat from coordinated defense. This includes the trust that non-government entities have formed with CISA as the responsible facilitator of cyber information sharing activities in a way that protects privacy, focuses on security over regulatory use, and advances the government's cybersecurity mission. Sending a message of retreat to threat actors including foreign adversaries could have even more troubling consequences.

A. Other Cybersecurity Authorities and Activities Would Be Harmed by a Lapse of CISA 15

A lapse in CISA 15 would also undermine the effectiveness of multiple related laws and programs created since 2015. For example, the liability protections in CISA 15 were incorporated by reference into other significant cyber laws, such as the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA). Similarly, information sharing and operational programs and initiatives across various levels of

[18]CISA website, last visited May 13, 2025, https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative/jcdc-faqs.

government have relied on CISA 15 authorities as a basis on which to build out their own cybersecurity programs. Barring any successor agreements, these programs and initiatives might be weakened or forced to temporarily suspend operations if CISA 15 were allowed to lapse.

CISA 15 also covers information sharing with a "non-federal entity" to include state, tribal, or local governments, as well as their departments or components. This terminology means that state-run cybersecurity organizations, such as the New York Joint Security Operations Center (JSOC) or the California Cybersecurity Integration Center (Cal-CSIC), also rely upon the protections in CISA 15 and would likely lose information from their private sector partners if CISA 15 were to lapse.

Finally, CISA 15 contributed to the sustained growth of additional platforms and automated information sharing standards. Specifically, the Open Threat Exchange (OTX), a crowd-sourced cybersecurity platform initiated by AlienVault (now AT&T Cybersecurity), has seen substantial growth. According to the latest reports, OTX boasts over 180,000 participants across 140 countries, sharing more than 19 million potential threats daily. CISA 15 provided a key impetus to help push the adoption of standardized formats for the automated sharing of such cyber threat information. Specifically, section 105(c)(1) of CISA 15 required DHS to develop a “capability and process” to share threat indicators in an automated manner, catalyzing the uptake of the Structured Threat Information Expression (STIX) and the Trusted Automated Exchange of Intelligence Information (TAXII). Studies have shown a steady increase in the volume of STIX data shared among organizations in recent years[19] which suggests the continued utilization and need for automated information sharing.

Evolving Threats and the Technology Landscape

Private sector cyber defenders, including those from critical infrastructure entities, are regularly targeted by threat actors. Since the enactment of the CISA 15, the threat landscape has continued to evolve alongside significant technology innovation.

For example, AI has become a ubiquitous feature of IT applications, offerings, and services transforming various aspects of cybersecurity. AI is being used to enhance threat detection and response capabilities, but it is also being leveraged by malicious actors to conduct more sophisticated attacks. Experts note that with the advent of advanced AI models, we face novel risks like adversarial AI manipulation (tricking algorithms through malicious inputs), data poisoning (corrupting the training data of AI systems), and prompt injection exploits – challenges that our current cybersecurity approaches were not designed to handle.[20] While such AI-specific attacks are still emerging, their potential impact is serious and highlights how our defensive strategies (and the laws governing them) may need to adapt to keep pace with technological change.

---

[19]Jin et al., Sharing cyber threat intelligence: Does it really help? Network and Distributed System Security (NDSS) Symposium, January 2024, available at https://www.ndss-symposium.org/ndss-paper/sharing-cyber-threat-intelligence-does-it-really-help/.

[20] ITI’s AI Security Policy Principles, dated October 2024, available at https://www.itic.org/documents/artificial-intelligence/ITI_AI-Security-Principles_102124_FINAL.pdf#:~:text=However%2C%20threats%20unique%20to%20AI,systems%20has%20been%20steadily%20increasing.

Additionally, the convergence of Information Technology (IT) and Operational Technology (OT) systems has introduced new complexities and vulnerabilities. This integration aims to improve operational efficiency but also expands the attack surface, making it crucial to manage a broader landscape of cybersecurity risks effectively.

New categories of attacks have emerged since Congress passed CISA 15 as malicious actors continuously seek new attack vectors. Ransomware attacks have become increasingly prevalent, causing significant disruptions and financial losses. These attacks are striking ever more critical targets – governments, hospital systems, pipelines – with increasingly dire consequences.[21] Software supply chain attacks such as SolarWinds have also gained prominence, targeting vulnerabilities in third-party software components to compromise entire systems.

While we have a better understanding of these new threats and patterns thanks to a combination of pre- and post-incident information sharing enabled by CISA 15. Defenders depend on threat indicator sharing to strengthen their defenses and protect their customers' data. Information sharing alone cannot be the solution, but it is undoubtedly a critical component of our collective response to the evolving threat landscape, and it is fair to ask whether CISA 15 adequately accounts for the sharing of threat information related to all of these technological advances.

Recommendations

Given the importance of CISA 15 authorities to our national cyber defense, Congress' first and most important job this year is the reauthorization of the existing law before it lapses in September. Given recent cybersecurity incidents, notably the Salt Typhoon campaign against U.S. telecommunications companies, Congress should examine how to improve our nation's digital defenses. The technology sector looks forward to partnering with policymakers to improve all areas of our cybersecurity posture, including improvements to CISA 15. The improvements cannot come at the expense of the existing cyber activities that rely on CISA 15 authorities. Any lapse to CISA 15's liability protections could have real and immediate negative consequences that put all American organizations at greater risk.

There are ways in which Congress could improve the information sharing ecosystem spurred by CISA 15. These include updating the scope of covered cyber threat indicators to match the modern threat environment, exploring ways to support offensive cyber capabilities, and considering the intersection of CISA 15 authorities with other laws and authorities. I will cover each of these recommendations below.

1. Modernize Terms to Match Threats and Technology

Given the ever improving and evolving nature of technology and of hacker behaviors and capabilities, Congress should consider updating the scope of CISA 15 to align with modern threats, indicators, and defensive measures. Specifically, Congress should consider whether and how to refine the definition of

[21]Threat Evaluation Working Group, Supplier, Products, and Services Threat Evaluation, Information and Communications Technology Supply Chain Risk Management Task Force, July 2021, available at https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force-threat-scenarios-report-v3.pdf#:~:text=The%20impacts%20of%20ransomware%20attacks,Another%20recently.

"cyber threat indicator,"[22] to ensure that CISA 15 is operative and applicable to cover the current landscape of threats, vulnerabilities, and malicious activities. Additional indicators may be appropriate to include, especially those related to supply chain exploits and risk information,[23] ransomware, or fraud. Similarly, AI-related threats may be worth considering such as those related to training data anomalies, evasion logs, prompt ejections or malicious prompt patterns.

For example, CISA 15 defines a *"cybersecurity threat"* primarily as an action "on or through an information system" that may harm the security or data of that information system.[24] This framing made sense at the time but might not explicitly encompass threats that exploit machine-learning models in the cloud, corrupt software components before they ever reach a victim's network, or target IoT and OT devices that fall outside the classic notion of an IT system. Updating the terminology of CISA 15 to encompass AI-driven exploits, ransomware operations, software supply chain compromises, and OT attacks, among other attack vectors, will remove doubt and friction in our information-sharing efforts.

2. <u>Information Sharing for Effect – Degrading Threat Actor Infrastructure & the JCDC</u>

It is important to underscore the limits of sharing information about cybersecurity vulnerabilities, threat actor behaviors, and other intelligence. If policy makers are concerned about how best to structure the federal cybersecurity enterprise to degrade hackers' ability to conduct attacks, I recommend evaluating the current functions of the Joint Cyber Defense Collaborative (JCDC).

The best version, and stated intent, of the JCDC is to serve as a forum for real-time, joint cyber defense operational planning and response. A public-private collaborative approach is essential to countering advanced persistent threat (APT) actors which are backed by nation-state resources, access to talent, and technical capabilities. The work of the JCDC builds upon and evolves CISA 15, though the program remains only a few years old and could benefit from Congressional direction and oversight.

Combatting sophisticated APT level groups will require a different strategy than promoting basic cyber hygiene policies which, if effectively implemented, can combat the vast majority of cyber criminals but not the most sophisticated threat actors. A deeper public-private collaboration is needed to leverage the authorities and capabilities of a multitude of federal agencies from Homeland Security and Law Enforcement in concert with the private sector companies – including tech, telecom, and cybersecurity firms – who have visibility into the targets APTs are looking to compromise.

---

[22] Sec. 102. Definitions. (6) available at https://www.cisa.gov/sites/default/files/publications/Cybersecurity%2520Information%2520Sharing%2520Act%2520of%25202015.pdf.

[23]CISA website, last visited May 13, 2025, available at https://www.cisa.gov/resources-tools/groups/ict-supply-chain-risk-management-task-force.

[24] Megan Brown, Jacqueline Brow, and Sydney White, CSIA 15 Reauthorization – Are Changes on the Horizon? Wiley Connect Blog, posted March 3, 2025, available at https://www.wileyconnect.com/CISA-2015-Reauthorization-Are-Changes-on-the-Horizon#:~:text=%E2%80%9CCybersecurity%20threat%E2%80%9D%20is%20defined%20under,be%20scoped%20more%20broadly%20or.

ITI appreciates Committee members' interest in JCDC legislation and provided feedback to the Committee on Ranking Member Swalwell's legislative proposal last Congress. At a high-level, additional governance structures and processes at the JCDC are important to make participants co-equal partners in the center's activities. A well-defined strategy for the JCDC, transparency through a charter for the JCDC, and regular reporting requirements would all benefit the JCDC's mission of evolving information sharing into a collaborative planning body.

3. Protect Related Information Sharing Partnerships and Forums for Collaboration

The currently suspended Critical Infrastructure Partnership Advisory Council (CIPAC) provided a protected forum and set of umbrella authorities enabling private sector and federal agencies to exchange threat intelligence, craft cybersecurity policies, and discuss and make recommendations to address risks to critical infrastructure. CIPAC created trust among numerous public-private partnerships by providing a protected channel controlling how shared information could be used and disseminated, exempt from the Federal Advisory Committee Act's requirements.

Examples of partnerships impacted by the suspension of CIPAC include the Sector Coordinating Councils (SCCs), the Enduring Security Framework (ESF) and the Information and Communications Technology Supply Chain Risk Management (ICT SCRM) Task Force. The SCCs are independent, self-governed bodies composed of private sector entities that own, operate and secure the nation's critical infrastructure. The SCCs leveraged CIPAC to provide advice and guidance to collectively address the most pressing security challenges facing our country. ESF is a cross-sector working group that operates under the auspices of CIPAC to address threats and risks to the security and stability of U.S. National Security Systems and critical infrastructure by bringing together the public and private sectors to work on intelligence-driven cyber challenges. The ICT SCRM Task Force is a public-private partnership established by DHS in 2018 in concert with the IT and Communications SCCs as another cross-sector CIPAC-chartered working group whose work is becoming increasingly critical as adversaries scale efforts to disrupt the supply chains underpinning the digital economy. While Secretary Noem has publicly announced plans to reinstate CIPAC authorities in some form, Congress could provide greater certainty by firmly codifying functionally equivalent authorities in statute.

Conclusion

The legal framework established by CISA 15 is a critical foundation for the effective functioning of cyber threat information sharing between the public and private sector, for federal, state and local governments and among industry sectors. Any lapse in these authorities will likely disrupt critical information sharing activities nationwide, significantly weaken our cybersecurity defenses, and provide malicious actors with new opportunities to exploit vulnerabilities. It is imperative that Congress prioritize the reauthorization of CISA 15 ahead of its sunset date in September. We strongly recommend a clean extension to ensure continuity, with any improvements to the important protections in existing law to be addressed in future legislation.

Thank you for the opportunity to testify today. I look forward to your questions.