

IN DEFENSE OF DEFENSIVE MEASURES:
REAUTHORIZING CYBERSECURITY INFORMA-
TION-SHARING ACTIVITIES THAT UNDERPIN U.S.
NATIONAL CYBER DEFENSE

HEARING
BEFORE THE
SUBCOMMITTEE ON
CYBERSECURITY AND INFRASTRUCTURE
PROTECTION
OF THE

COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES
ONE HUNDRED NINETEENTH CONGRESS

FIRST SESSION

MAY 15, 2025

Serial No. 119-15

Printed for the use of the Committee on Homeland Security



Available via the World Wide Web: <http://www.govinfo.gov>

U.S. GOVERNMENT PUBLISHING OFFICE

61-338 PDF

WASHINGTON : 2025

COMMITTEE ON HOMELAND SECURITY

MARK E. GREEN, MD, Tennessee, *Chairman*

MICHAEL T. MCCAUL, Texas, <i>Vice Chair</i>	BENNIE G. THOMPSON, Mississippi, <i>Ranking Member</i>
CLAY HIGGINS, Louisiana	ERIC SWALWELL, California
MICHAEL GUEST, Mississippi	J. LUIS CORREA, California
CARLOS A. GIMENEZ, Florida	SHRI THANEDAR, Michigan
AUGUST PFLUGER, Texas	SETH MAGAZINER, Rhode Island
ANDREW R. GARBARINO, New York	DANIEL S. GOLDMAN, New York
MARJORIE TAYLOR GREENE, Georgia	DELIA C. RAMIREZ, Illinois
TONY GONZALES, Texas	TIMOTHY M. KENNEDY, New York
MORGAN LUTTRELL, Texas	LAMONICA MCIVER, New Jersey
DALE W. STRONG, Alabama	JULIE JOHNSON, Texas, <i>Vice Ranking Member</i>
JOSH BRECHEEN, Oklahoma	PABLO JOSÉ HERNÁNDEZ, Puerto Rico
ELIJAH CRANE, Arizona	NELLIE POU, New Jersey
ANDREW OGLES, Tennessee	TROY A. CARTER, Louisiana
SHERI BIGGS, South Carolina	ROBERT GARCIA, California
GABE EVANS, Colorado	VACANT
RYAN MACKENZIE, Pennsylvania	
BRAD KNOTT, North Carolina	

ERIC HEIGHBERGER, *Staff Director*
HOPE GOINS, *Minority Staff Director*
SEAN CORCORAN, *Chief Clerk*

SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION

ANDREW R. GARBARINO, New York, *Chairman*

CLAY HIGGINS, Louisiana	ERIC SWALWELL, California, <i>Ranking Member</i>
CARLOS A. GIMENEZ, Florida	SETH MAGAZINER, Rhode Island
MORGAN LUTTRELL, Texas	LAMONICA MCIVER, New Jersey
ANDREW OGLES, Tennessee	VACANT
MARK E. GREEN, MD, Tennessee (<i>ex officio</i>)	BENNIE G. THOMPSON, Mississippi (<i>ex officio</i>)

ALEXANDRA SEYMOUR, *Subcommittee Staff Director*
MOIRA BERGIN, *Minority Subcommittee Staff Director*

CONTENTS

	Page
STATEMENTS	
The Honorable Andrew R. Garbarino, a Representative in Congress From the State of New York, and Chairman, Subcommittee on Cybersecurity and Infrastructure Protection:	
Oral Statement	1
Prepared Statement	2
The Honorable Eric Swalwell, a Representative in Congress From the State of California, and Ranking Member, Subcommittee on Cybersecurity and Infrastructure Protection:	
Oral Statement	3
Prepared Statement	4
The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Ranking Member, Committee on Homeland Security:	
Prepared Statement	6
WITNESSES	
Mr. John Miller, Senior Vice President of Policy for Trust, Data, and Technology, General Counsel, Information Technology Industry Council:	
Oral Statement	7
Prepared Statement	9
Ms. Diane Rinaldo, Private Citizen:	
Oral Statement	17
Prepared Statement	19
Mr. Karl Schimmeck, Executive Vice President and Chief Information Security Officer, Northern Trust:	
Oral Statement	21
Prepared Statement	22
Mr. Katherine Kuehn, Member and CISO-in-Residence, National Technology Security Coalition:	
Oral Statement	26
Prepared Statement	28
FOR THE RECORD	
The Honorable Andrew R. Garbarino, a Representative in Congress From the State of New York, and Chairman, Subcommittee on Cybersecurity and Infrastructure Protection:	
Letter From Business Roundtable	37
Statement of the Protecting America's Cyber Networks Coalition	38
Letter From the Alliance for Automotive Innovation	40
Joint Statement of Intrado Life & Safety, the National Association of State 9–1–1 Administrators, and NENA—The 9–1–1 Association	41
Joint Letter From Multiple Associations	42
Statement of the Operational Technology Cybersecurity Coalition (OTCC) ...	43
Statement of the National Retail Federation	44
Letter From the Software & Information Industry Association (SIIA)	47
APPENDIX	
Questions From Chairman Andrew R. Garbarino for John Miller	57

IV

	Page
Questions From Chairman Andrew R. Garbarino for Diane Rinaldo	59
Questions From Chairman Andrew R. Garbarino for Karl Schimmeck	60
Questions From Chairman Andrew R. Garbarino for Katherine Kuehn	61

**IN DEFENSE OF DEFENSIVE MEASURES:
REAUTHORIZING CYBERSECURITY INFOR-
MATION-SHARING ACTIVITIES THAT
UNDERPIN U.S. NATIONAL CYBER DEFENSE**

Thursday, May 15, 2025

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON CYBERSECURITY AND
INFRASTRUCTURE PROTECTION,
Washington, DC.

The subcommittee met, pursuant to notice, at 2:04 p.m., in room 310, Cannon House Office Building, Hon. Andrew R. Garbarino (Chairman of the subcommittee) presiding.

Present: Representatives Garbarino, Gimenez, Luttrell, Ogles, Swalwell, and Magaziner.

Mr. GARBARINO. The Committee on Homeland Security, Subcommittee on Cybersecurity and Infrastructure Protection, will come to order.

Without objection, the Chair may declare the committee in recess at any point.

The purpose of this hearing is to examine the Cybersecurity Information Sharing Act of 2015, or CISA 2015, which is up for reauthorization this year. We will evaluate the voluntary cybersecurity information-sharing framework established by this legislation, assessing how it has influenced the way private entities share information today.

This hearing will highlight the need to continue cybersecurity information sharing given an increasingly complex threat environment, and we'll consider improvements to the legislation.

I now recognize myself for an opening statement.

Information sharing is a critical component of our Nation's defense against global cyber threats. From utility companies in rural areas to major banks on Wall Street, the private sector is on the front lines of the digital battlefield, frequently defending itself from malicious cyber actors.

Securing the United States in cyber space requires a whole-of-society approach, strong partnerships, and close coordination between industry and Government at all levels. Our national resilience against cyber threats is reinforced by sharing threat information and best practices amongst all stakeholders.

Nearly 10 years ago, Congress passed the Cybersecurity Information Sharing Act of 2015, establishing a framework for the vol-

untary exchange of cybersecurity information between private entities and the Federal Government.

By providing liability and privacy protections for information shared in accordance with the statute, CISA 2015 removed longstanding barriers to public-private collaboration in cybersecurity.

Over the past decade, the threat landscape has evolved significantly, with sophisticated nation-state and criminal actors increasingly exploiting cyber space to target infrastructure and individuals.

As these threats continue to rise, CISA 2015 has become more vital than ever. The law has fostered a foundation of trust among cybersecurity stakeholders, making information sharing the default rather than an exception.

A significant volume of critical cyber threat intelligence has been exchanged between industry and Government under this law. For instance, just this year a major organization shared 84 formal reports, reaching thousands of partner organizations. This doesn't include the numerous informal daily exchanges that are also protected by the law.

This September, CISA 2015 is set to expire unless Congress reauthorizes it.

As we've heard from many stakeholders, the liability and privacy protections provided by the law have facilitated better information sharing, helped secure networks, and improved our overall cybersecurity posture.

The Cybersecurity and Infrastructure Security Agency, which this subcommittee oversees, has played a crucial role in fostering these information-sharing partnerships, a mission I look forward to continuing under the new administration.

There are valid concerns that without these protections the private sector would be less willing to share cybersecurity information, either amongst themselves or with the Federal Government. Without these safeguards, we can be certain that our Nation would be more vulnerable to cyber threats.

I strongly support reauthorizing CISA 2015. I've made it a top priority this year. I am encouraged that just yesterday Secretary Noem voiced similar support before the full committee.

This hearing is a crucial step forward in the reauthorization process, and I look forward to incorporating feedback into a reauthorization bill.

I'd like to thank our expert panel for being here. Your insights on how this law has been implemented across industry are invaluable. Some of you have tracked or worked directly on this law since its inception.

I look forward to exploring ways to maintain and potentially improve voluntary cybersecurity information sharing between the public and private sectors.

[The statement of Chairman Garbarino follows:]

STATEMENT OF CHAIRMAN ANDREW R. GARBARINO

MAY 15, 2025

Information sharing serves as a critical component in our Nation's defense against global cyber threats. Ranging from utility companies in rural communities to large

banks on Wall Street, the private sector operates on the front lines of the digital battlefield and is frequently defending itself from malicious cyber actors.

Securing the United States in the cyber domain requires a whole-of-society approach—partnerships and close coordination with industry as well as State, local, Tribal, and territorial governments. Our national resilience against cyber threats is strengthened by sharing threat information and best practices among stakeholders.

Almost 10 years ago, Congress enacted the Cybersecurity Information Sharing Act of 2015—otherwise known as “CISA 2015.” This law created a framework for the voluntary exchange of cybersecurity information between private entities and with the Federal Government.

By granting liability and privacy protections to information shared in accordance with the statute, CISA 2015 removed significant and long-standing barriers to public-private collaboration in cybersecurity.

The threat landscape has evolved significantly in the past 10 years, with an emergence of sophisticated nation-state and criminal actors who use cyber space to exploit infrastructure and individuals. As threats continue to rise, CISA 2015 has become more important than ever before. The law has built a bedrock of trust among cybersecurity stakeholders to make information sharing the default, rather than the decision point.

Indeed, a high volume of critical cyber threat intelligence has been shared between industry and Government under this statute. For example, this year alone, a large organization has shared 84 formal reports that have reached—in some cases—thousands of partner organizations. This does not include the multiple, daily, informal information-sharing engagements that the law also protects.

This September, CISA 2015 will expire unless Congress acts now to reauthorize this key authority. As we have heard from many stakeholders, the liability and privacy protections have enhanced information sharing, helped secure their networks, and improved overall cyber defense posture of the United States. CISA the agency, which this subcommittee oversees, has played a significant role in facilitating information-sharing partnerships—something I look forward to seeing it continue as it refocuses on its core mission.

There are valid concerns that, without this framework and its protections, the private sector would be less willing to share cybersecurity information among itself or with the Federal Government.

We can be certain that our Nation would be more vulnerable to cyber threats if there were significant reductions in cybersecurity intelligence sharing.

I wholeheartedly support the reauthorization of CISA 2015, and have made this bill a top priority this year. This hearing is a vital step forward for the reauthorization process, and I look forward to incorporating feedback from this hearing into a reauthorization bill that I intend to introduce very soon.

I want to thank our expert panel for being here today. You bring valuable insights about how this law has been operationalized across industries. Some of you have even tracked, or directly worked on, this law from initial inception.

I look forward to exploring ways in which we can maintain, and potentially further improve, voluntary cybersecurity information sharing between the public and private sectors.

Mr. GARBARINO. I now recognize the Ranking Member, the gentleman from California, Mr. Swalwell, for his opening statement.

Mr. SWALWELL. Thank you, Chairman.

I was a member of the Intelligence Committee back in 2015 when the CISA 2015 was enacted, and it was apparent to me then, even in the midst of very intense, vigorous debate, that we needed greater public-private cybersecurity collaboration.

So I want to first just thank the witnesses for coming today and sharing their perspective, their members' positions, their industry's concerns, because we want to get this right and we want to build on the success that we have.

So we're hearing about new cybersecurity attacks every day, yet the Federal Government at the time had very little visibility into what was happening on private networks, and the private sector was receiving very little information from the Federal Government on cyber threats.

I would say that is probably still happening today, and the biggest complaint I hear from you all, especially on JCDC, is it's a one-way relationship. I know we want to do more to increase what is shared with you in the private sector.

But I laid out in the 2015 debate that there was at the time almost no cyber sharing between the public sector and the private sector.

CISA 2015 sought to change that, and it has changed that. It's provided the legal framework to facilitate cyber information sharing between the Federal Government and the private sector. It gives companies the confidence that they'll be legally protected if they voluntarily share cyber threat information with the Department of Homeland Security or with their competitors.

It's rare that these days we see such a wide consensus on any topic, but on the issue of reauthorizing CISA 2015 I've received a very clear message from everyone I've talked to: Do not let it lapse.

Stakeholders have consistently stated that CISA 2015 has drastically improved public-private collaboration, helping our cyber defenders better do their job.

Of particular importance to me was that in 2015 we addressed privacy and civil liberty protections and demonstrated that their effectiveness was in ensuring information shared with the Government is protected and always used properly.

As CISA 2015 was developed, I advocated for strong privacy protections, and I'm glad to see those statutory requirements have achieved their outcomes.

We must move quickly to reauthorize CISA 2015 before it expires in September. Maybe we could change the name so it's not so confusing with the other CISA that we're working on. That is one change I think we would all welcome. Yeah, good name change.

While it's reasonable to discuss if there are ways to strengthen the law going forward, we cannot allow such discussions with such an imminent time line to delay reauthorization.

It's also important to remember there are steps that Congress and the administration can take in the interim after reauthorization.

While establishing the legal regime to facilitate cyber information sharing, the maturation of the Cybersecurity and Infrastructure Security Agency—the original CISA—has provided a central hub for public-private cyber collaboration across critical infrastructure sectors.

If CISA lacks the people and forms necessary to receive, analyze, and share cyber threat information, CISA 2015's provisions will be rendered meaningless.

One important step for Congress that I have been working with in this committee is to codify the Joint Cyber Defense Collaborative and better define its mission and structure, and I hope we get a vote on that again this Congress.

The administration should restore the Critical Infrastructure Partnership Advisory Council—also known as CIPAC—or establish a similar new entity that provides a mechanism for critical infrastructure collaboration.

Finally, we must continue to support CISA's efforts to improve Automated Indicator Sharing and implement its Threat Intelligence Enterprise Services Program.

Again, I thank the witnesses for participating in this. I expect I will hear across the board the value of CISA, that there are reforms that we can put in place.

But if it's deciding between not authorizing and trying to find better reforms and risking this lapsing or reauthorizing something clean and then fighting and working together collaboratively ultimately to get reforms in the future, I think that you would choose the latter.

With that, I yield back.

[The statement of Ranking Member Swalwell follows:]

STATEMENT OF RANKING MEMBER ERIC SWALWELL

MAY 15, 2025

As a Member of the Intelligence Committee when the Cybersecurity Information Sharing Act of 2015 (CISA 2015) was enacted, it was very apparent to me then that there was a need for greater public-private cybersecurity collaboration.

We were hearing about new cyber attacks every day, yet the Federal Government had little visibility into what was happening on private networks, and the private sector was receiving little information from the Federal Government on cyber threats. As I explained during the debate leading up to the enactment of CISA 2015, there was, at the time, "virtually zero relationship between private industry and Government" when it came to cybersecurity.

Thanks to CISA 2015, that has changed over the last decade. CISA 2015 has provided the legal framework to facilitate cyber information sharing between the Federal Government and the private sector, as well as between private-sector entities. It gives companies the confidence that they will be legally protected if they voluntarily share cyber threat information with the Department of Homeland Security or with their competitors.

It is rare these days that we see such a wide consensus on any topic, but on the issue of reauthorizing CISA 2015, I have received a very clear message from everyone I have talked to—we cannot let this authority lapse. Stakeholders have consistently stated that CISA 2015 has drastically improved public-private collaboration, helping our cyber defenders better do their job.

Of particular importance to me, CISA 2015's privacy and civil liberties protections have demonstrated their effectiveness in ensuring information shared with the Government is protected and used properly. As CISA 2015 was developed, I advocated for strong privacy protections, and I am glad to see those statutory requirements have achieved their desired outcomes. We must move quickly to reauthorize CISA 2015 before it expires in September.

While it is reasonable to discuss if there are ways to strengthen the law going forward, we cannot allow such discussions to delay reauthorization, which would risk CISA 2015 lapsing and undermine the private sector's confidence in cooperating with the Federal Government.

It is also important to remember that there are steps that Congress and the administration can take to improve cybersecurity information sharing beyond just reauthorizing CISA 2015. While CISA 2015 established the legal regime to facilitate cyber information sharing, the maturation of the Cybersecurity and Infrastructure Security Agency has provided a central hub for public-private cyber collaboration across critical infrastructure sectors. Continued support and resourcing for CISA will be essential to improved information sharing.

If CISA lacks the people and forums necessary to receive, analyze, and share cyber threat information, CISA 2015's provisions will be meaningless. One important step for Congress to take would be to codify the Joint Cyber Defense Collaborative and better define its mission and structure. And the administration should restore the Critical Infrastructure Partnership Advisory Council (CIPAC) or establish a similar, new entity that provides a mechanism for critical infrastructure collaboration.

Additionally, we must continue to support CISA's efforts to improve Automated Indicator Sharing and implement its Threat Intelligence Enterprise Services program. It is critical that CISA has access to the best technologies available to facili-

tate timely and useful cyber threat information sharing, and Congress must ensure CISA has the resources and capacity to modernize its systems and services so that they become more useful to the private sector.

I know there is bipartisan support for these efforts and am eager to work together to get CISA 2015 reauthorized and to continue building out the Federal Government's capacity for information sharing.

I thank the witnesses for participating today and look forward to hearing from them about how CISA 2015 has strengthened our national security and how we can continue to better facilitate public-private information sharing going forward.

Mr. GARBARINO. The gentleman yields back.

Other Members of the committee are reminded that opening statements may be submitted for the record.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

MAY 15, 2025

Ten years ago, Congress enacted legislation that transformed how the Government and private sector collaborate to defend the Nation against cyber threats. The Cybersecurity Information Sharing Act of 2015 reflects a hard-fought compromise that took years and multiple Congresses to accomplish.

Many of the witnesses testifying today worked with Congress over the multi-year authorization effort to ensure the bill included protections for privacy and civil liberties and establish appropriate mechanisms for information sharing. I'd like to thank you for your efforts to get CISA 2015 enacted then and to get it reauthorized now. Today, CISA 2015 serves as the foundational authority for critical public-private collaboration programs—from CISA's Ransomware Task Force and Notification Initiative to the Joint Cyber Defense Collaborative—as well as private-sector information-sharing organizations like information sharing and analysis centers (ISACs).

More broadly, the Cybersecurity Information Sharing Act transformed security culture, creating within the private sector a bias toward sharing information with Government and each other through both formal and informal mechanisms. As a result, Government has been able to work with the private sector to more dynamically respond to a range of cyber threats from our most sophisticated adversaries and cyber criminals.

While I recognize that there is room to improve and modernize the Cybersecurity Information Sharing Act, we cannot allow efforts to rethink the bill to interfere with its timely reauthorization. This critical authority expires in just 44 legislative days. If history is any guide, changes to CISA 2015—however minor—will involve multiple stakeholders and multiple rounds of careful negotiation. I recommend, in the strongest terms, that this committee move a clean, 10-year extension of CISA 2015 as soon as possible to ensure continuity of the collaboration programs that both Government and the private sector rely on.

Doing so will send a strong message to the security community that despite the current upheaval across Government, Congress remains committed to ensuring the Federal Government is a strong security partner. It will also make clear to our adversaries that our political divisions will not distract us from our obligation to defend the critical infrastructure Americans rely on every day from cyber attacks.

I appreciate the Subcommittee Chair and Ranking Member's commitment to reauthorizing the Cybersecurity Information Sharing Act of 2015, and I look forward to working with them to get it across the finish line.

Mr. GARBARINO. I am pleased to have a distinguished panel of witnesses before us today. I ask that our witnesses please rise and raise their right hand.

[Witnesses sworn.]

Mr. GARBARINO. Let the record reflect that the witnesses have answered in the affirmative.

Thank you, and please be seated.

I would now like to formally introduce our witnesses.

Mr. John Miller currently serves as the senior vice president of policy for trust, data, and technology and general counsel for the Information Technology Industry Council.

Mr. Miller is responsible for driving ITI's global strategy and advocacy on cybersecurity, technology, and digital policy issues while also serving as the organization's chief legal officer.

In addition to his work at ITI, his experience includes serving as co-chair of CISA's ICT Supply Chain Risk Management Task Force, 3 terms as chair of the IT Sector Coordinating Council, and co-founder of the Council to Secure the Digital Economy.

Ms. Diane Rinaldo previously served on the House Permanent Select Committee on Intelligence, where she had first-hand experience working on CISA 2015. Ms. Rinaldo also held senior-level roles in the Executive branch, serving as acting administrator of the National Telecommunications and Information Administration and as acting assistant secretary of Commerce for communications and information. She currently serves as the executive director of the Open RAN Policy Coalition.

Mr. Karl Schimmeck currently serves as executive vice president and chief information security officer of Northern Trust. He's also here on behalf of the Securities Industry and Financial Markets Association, or SIFMA, where he previously served as the managing director of cybersecurity, business resiliency, and operational risk.

At Northern Trust, he is responsible for designing and managing the strategy and operations of the bank's information security, cybersecurity, and data protection programs. Additionally, he serves on the board of directors of both the Financial Services Information Sharing and Analysis Center and the Cyber Risk Institute.

Ms. Kate Kuehn serves on the board of directors and is CISO-in-residence at the National Technology Security Coalition, where she brings experience leading and advising cybersecurity, technology, innovative AI strategies, and teams to help shape the industry with better business security and risk decisions.

In addition to her work at the NTSC, Ms. Kuehn serves on the board of directors for HYAS and the Cybermaniacs.

I thank the witnesses for being here today.

I now recognize Mr. Miller for 5 minutes to summarize his opening statement.

STATEMENT OF JOHN MILLER, SENIOR VICE PRESIDENT OF POLICY FOR TRUST, DATA, AND TECHNOLOGY, GENERAL COUNSEL, INFORMATION TECHNOLOGY INDUSTRY COUNCIL

Mr. MILLER. Chairman Garbarino, Ranking Member Swalwell, and distinguished Members of the subcommittee, on behalf of the Information Technology Industry Council, or ITI, thank you for the opportunity to testify today on the critical need for Congress to reauthorize the Cybersecurity Information Sharing Act of 2015, or CISA 15, before it is set to expire in just 4 months.

ITI is a global trade association representing 80 of the world's leading tech companies, and I lead ITI's Trust, Data, and Technology policy team, including our work on cybersecurity, AI, and privacy in the United States and globally.

I've worked on cyber policy issues for nearly 2 decades, and I have extensive experience partnering with DHS, CISA, and other Federal Government stakeholders to improve cyber and critical infrastructure security, including currently serving in the leadership

of the IT Sector Coordinating Council and ICT Supply Chain Risk Management Task Force.

I've had the honor of testifying before this subcommittee previously on the related topic of security incident notification, so I know you appreciate that sharing cyber threat information is vital to improving the Nation's cyber resilience and security by increasing situational awareness across Government and industry and driving more effective operational collaboration to prevent and respond to cyber threats.

The same principles underlying CIRCIA motivated Congress to pass CISA 15, and that law is as fundamental to our collective cybersecurity today as it was back in 2015.

I want to underscore that any lapse in CISA 15 authorities would be an unfortunate step backward, an unforced error that only stands to benefit cyber criminals, including sophisticated nation-state threat actors, such as China, Iran, and Russia.

The axiom that cybersecurity is a team sport is no more self-evident than in the context of information sharing, which dictates that those experiencing or observing an incident, vulnerability, or other indicators that a network or device has been compromised should share that information.

Sharing these indicators of compromise and other threat intelligence helps defenders team up to prevent potential targets from becoming future victims.

The goal of CISA 15 and a central thrust of U.S. cyber policy over the years has been to foster cyber threat info sharing to increase real-time situational awareness of the threat landscape to improve threat prevention, response, and mitigation efforts.

CISA 15 sought to accomplish this goal by incentivizing and making it easier for companies to share threat intelligence, both with the Government and with each other, without fear of lawsuits or liability, including as related to antitrust, information disclosure, or regulatory uses, provided the information shared adhered to privacy and civil liberties guardrails. It also required DHS to establish an automated process for sharing such information at scale.

After nearly 5 years of debate and negotiation, the CISA 15 statute realized these goals. It included precisely-scoped definitions of the information the bill authorized organizations to share and carefully negotiated and calibrated liability and privacy protections that balance the competing and sometimes conflicting concerns of stakeholders, ranging from the intelligence community to privacy advocates.

As a cyber policy expert and lawyer working on this issue at the time, I worked, along with fellow witnesses on this panel and many others, to help Congress strike a winning balance.

While it was a messy and sometimes contentious process, Congress ultimately reached an effective compromise, and we are better off today from a cybersecurity standpoint than we were 10 years ago.

The reality today is that organizations are benefiting more from cyber threat info sharing than they were before CISA 15 became law, and they are sharing and receiving via automated processes, not via spreadsheets.

This is not to say that CISA 15 was perfectly designed or has been perfectly implemented or that it cannot be improved. But with a looming September deadline for CISA 15 reauthorization, we cannot allow the perfect to be the enemy of the good.

Please do not jeopardize the cybersecurity improvements and partnerships that CISA 15 has catalyzed and that many now likely take for granted by letting the law lapse if that is the price of making changes.

That said, the tech sector stands ready to work with Congress to update and improve upon the cyber threat info-sharing ecosystem in the United States at any time.

Three targeted improvements worth considering include, No. 1, both the threat landscape and technology have changed over the past decade. From ransomware and operational technology to the explosion of generative AI, technologies and threats continue to evolve well beyond 2015 and hackers continue to adapt.

One simple rubric Congress could use in considering changes to CISA 15 is to evaluate whether the statute, as written, effectively captures the sharing of information necessary to combat cyber threats in 2025.

No. 2, given the rise of software supply chain attacks, I encourage Congress to examine whether definitions of terms such as cyber threat indicator can be updated to promote the sharing of information useful in preventing or mitigating threats to the ICT supply chain, such as information related to suspect suppliers.

No. 3, Congress could consider including adjacent authorities which also support public-private information sharing and partnership, such as the currently suspended Critical Infrastructure Partnership Advisory Council, or CIPAC, in a future iteration of CISA 15.

While the administration has indicated it plans to reinstate CIPAC authorities in some form, Congress could provide certainty by firmly codifying functionally equivalent authorities in statute.

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

[The prepared statement of Mr. Miller follows:]

PREPARED STATEMENT OF JOHN MILLER

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 80 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 inter-

¹The 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 4 continents. We promote public policies and industry standards that advance companies on and innovation worldwide. Our diverse membership and expert staff provide policy makers the broadest perspective and thought leadership from technology, hardware, software, services, manufacturing, and related industries. Visit <https://www.itic.org/> to learn more.

net 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, health care, 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 United States 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

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 United States "dropping its guard" and would be an unforced error in a dangerous and evolving moment of cyber risk for the United States. 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 United States.

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 indicators 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 con-

strained 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 policy makers in both Congress and the Executive branch that something needed to be done to improve the threat information-sharing ecosystem in the United States. 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 new authorities could be used for “nefarious purpose[s].”⁶ Civil liberties groups feared that information sharing might become a back door 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 dialog 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

²In 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/bills/112/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>.

⁶Hayley 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/gIQA5-ur0IT_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>.

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 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 provisions¹¹ have

⁸Michael 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-sharing>.

¹⁰Id.

¹¹U.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>.

proven effective. DHS¹² and the intelligence communities¹³ 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, wide-spread 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

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

¹²U.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=

¹³Office 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>.

¹⁴National Council of ISACs website, last visited May 12, 2025, <https://www.nationalisacs.org/>. "Formed in 2003, the [National Council of ISACs (NCIO)] 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."

¹⁵Id.

¹⁶Scott 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>.

¹⁷Id.

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 10 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 3 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 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

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

in the volume of STIX data shared among organizations in recent years¹⁹ 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.

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 policy makers 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 au-

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 ITT'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.

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.>

thorities 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 “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. Information Sharing for Effect—Degrading Threat Actor Infrastructure & the JCDC

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.

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 infra-

²² Sec. 102. Definitions. (6) available at <https://www.cisa.gov/sites/default/files/publications/Cybersecurity%20Information%20Sharing%20Act%20of%202015.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%9Dis%20defined%20under,be%20scoped%20more%20broadly%20or>.

structure. 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.

Mr. GARBARINO. Thank you, Mr. Miller.

I now recognize Ms. Rinaldo for 5 minutes to summarize her opening statement.

STATEMENT OF DIANE RINALDO, PRIVATE CITIZEN

Ms. RINALDO. Thank you.

Chairman Garbarino, Ranking Member Swalwell, Members of the committee, thank you for the opportunity to appear before you today.

My name is Diane Rinaldo, and by way of background, I worked on the Cybersecurity Information Sharing Act from its inception to passage into law as a staff member on the House Permanent Select Committee on Intelligence. I am grateful to speak to the urgent need for its reauthorization.

This act 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.

When the original legislation was drafted in 2012, growing concerns about the frequency and sophistication of cyber attacks were already taking shape. In hindsight, those early warnings significantly underestimated the scale and complexity of today's threat landscape.

Over the past decade, threat actors have become more capable and emboldened, outpacing both legislative safeguards and defensive technologies. High-profile attacks, such as Salt Typhoon and

incursions on the U.S. Government, have made it abundantly clear: No sector, private or public, is immune.

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 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 and trade secrets.

This is not random or opportunistic. It's a deliberate strategy to fuel China's economic and military ambitions, with cyber capability 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 Cyber Information Sharing Act laid the foundation for improved collaboration between Government agencies and the private sector by creating a legal framework for voluntary information sharing. It offered liability protections to encourage private-sector companies to share threat indicators and defensive measures with the Federal Government and business to business.

Our thought was simple: See something, say something.

That framework helped normalize and destigmatize cyber threat information sharing across industry.

The Department of Homeland Security's Automated Indicator Sharing program and the role of ISACs is a direct result and outgrowth of this legislation.

This legislation was the product of 4 years of intensive effort, including more than 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 3 major rewrites based on the feedback that we 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, some gaps still remain: limited participation, speed and relevance of information, lack of bidirectional flow, inconsistent standards, and a trust deficit.

Reauthorizing information sharing gives Congress the opportunity to strengthen and scale its original vision. To strengthen national security, Congress should expand and clarify liability protections to encourage broader information sharing.

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's 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.

In closing, I urge the committee to quickly 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 ecosystem our future demands.

Thank you, and I look forward to your questions.
[The prepared statement of Ms. Rinaldo follows:]

PREPARED STATEMENT OF DIANE RINALDO

MAY 15, 2025

Chairman Garbarino, 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 cyber attacks 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 4 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 3 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 health care—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, tool kits, 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.

Mr. GARBARINO. Thank you, Ms. Rinaldo.

I now recognize Mr. Schimmeck for 5 minutes to summarize his opening statement.

STATEMENT OF KARL SCHIMMECK, EXECUTIVE VICE PRESIDENT AND CHIEF INFORMATION SECURITY OFFICER, NORTHERN TRUST

Mr. SCHIMMECK. Chairman Garbarino, Ranking Member Swalwell, and distinguished Members of the committee, thank you for the opportunity to testify today on a matter of critical national importance: the urgent need to reauthorize the Cybersecurity Information Sharing Act of 2015.

My name is Karl Schimmeck. I serve as the chief information security officer at Northern Trust and serve on the board of directors of the Financial Services Information Sharing and Analysis Center, or the FS-ISAC.

I'm here today on behalf of the Securities Industry and Financial Markets Association, or SIFMA, where I sit on the Cybersecurity Committee.

SIFMA is the leading trade association for broker-dealers, investment banks, and asset managers operating in the United States. SIFMA advocates on legislation, regulation, and business policy affecting financial markets.

I've spent much of my career focused on cybersecurity in the financial sector, and I was directly involved in the advocacy that helped shape CISA 2015. That law was a bipartisan achievement, and it remains one of the most important cybersecurity tools that we have and a cornerstone of our Nation's cyber defense strategy.

The threats we face today are not hypothetical. They are real, growing, and increasingly dangerous. Nation-state actors are conducting relentless cyber operations against our critical infrastructure—banking systems, communication networks, energy grids, and Government agencies.

These attacks are not just attempts to steal data. They are designed to disrupt, destabilize, and undermine confidence in our institutions.

Put simply, cyber is now a national security domain, and the private sector is on the front lines.

CISA 2015 provides the legal foundation that enables companies like mine to share threat intelligence quickly and confidently with the Federal Government and with one another. It creates the trust, structure, and legal protections required for real-time collaboration.

Without the protections in the act—protections against civil liability, regulatory action, and antitrust exposure—companies would hesitate. They would share less and they would share more slowly. That hesitation would be a gift to our adversaries.

When CISA passed, there were concerns about protecting the privacy of individuals. After 10 years of activity, there have been no known reports that PII not directly related to a cybersecurity incident has been shared.

The participants in this system have a responsibility to ensure that the only information submitted is directly related to a cybersecurity threat. We take this responsibility seriously, and the unblemished track record demonstrates that commitment.

Let me be clear: If the act lapses, our Nation will be more vulnerable to cyber attacks the very next day. Threat sharing saves time, and in cybersecurity time is everything. It's the difference between stopping an attack at the perimeter or watching it spread

across the system. It's the difference between a minor disruption and a systemic crisis.

We often say that cybersecurity is a team sport, but that's only true if the rules allow us to play together. CISA 2015 makes teamwork possible. Recent events, including SolarWinds and CrowdStrike, clearly evidence the value of rapid information sharing, which helped to minimize the damage of these events.

That's why we are calling on this subcommittee and the full Congress to act swiftly and decisively to reauthorize the act without delay, without changes. We cannot afford a gap in our defenses, not now, not with the threat landscape evolving by the day.

We are not asking for new authorities. We are asking to preserve what already works—a proven framework that enables trust, protects privacy, and makes us all stronger.

The act is not just a legal mechanism, it's a force multiplier. It has created a trusted architecture for cyber collaboration. To let it expire would be to knowingly dismantle the critical defense layer at a precise moment when we need it most.

In closing, I'll leave you with this: Cyber threats don't take breaks and they don't wait for legislative calendars. If we hesitate, we expose ourselves. If we act, we protect the Nation.

Thank you for the opportunity to speak today, and I look forward to any questions.

[The prepared statement of Mr. Schimmeck follows:]

PREPARED STATEMENT OF KARL SCHIMMECK

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 United States 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 1,000 participants from 20

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).

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 essential to the collective protection of the United States 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 10 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 on-going 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 cyber criminals 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 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 on-going threats to financial institutions, Federal and State governments, and the general public cannot be overstated. Nation-state hackers have

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

³Cong. 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.

⁴6 U.S.C. §§ 681a–681b.

⁵Dep'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>.

launched numerous attacks on U.S. critical infrastructure⁶ 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 9 agencies were compromised,⁸ and the Office of the Comptroller of the Currency email breach this year.⁹ Unfortunately, foreign cyber criminals 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.

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.

⁶Dustin 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>.

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

⁸Nat’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>.

⁹Office 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>.

¹⁰Office 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>.

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

¹²6 U.S.C. § 1505.

¹³6 U.S.C. § 1503(e)(1).

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 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., cyber crime, 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 wide-spread 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 2 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 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.

¹⁴Kapko, 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/>.

¹⁵See 6 U.S.C. § 681a.

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.

Mr. GARBARINO. Thank you, Mr. Schimmeck.

I now recognize Ms. Kuehn for 5 minutes to summarize her opening statement.

STATEMENT OF KATHERINE KUEHN, MEMBER AND CISO-IN-RESIDENCE, NATIONAL TECHNOLOGY SECURITY COALITION

Ms. KUEHN. Chairman Garbarino, Ranking Member Swalwell, and Members of the committee, thank you for the opportunity to testify today in support of reauthorizing the Cybersecurity Information Sharing Act of 2015 and the importance of public-private partnerships in protecting our national security.

My name is Katherine Kuehn, and I am a board member of the National Technology Security Coalition and serve as their CISO-in-residence.

Established in 2016, the NTSC is a nonprofit, nonpartisan organization that advocates for the chief information security officers, chief privacy officers, and senior security technology executives.

NTSC's mission is to advance cybersecurity policies that protect critical national infrastructure and foster strong collaboration between the public and private sectors to secure our digital landscape.

As a part of this mission, we have been deeply involved in shaping the national conversation on cybersecurity, including advocacy for the creation of the Cybersecurity Advisory Committee.

The Cybersecurity Information Sharing Act of 2015 has long been a cornerstone of our national cybersecurity strategy. Since its inception, this law has fostered collaboration between industry leaders and Federal agencies, enabling the identification and mitigation of cybersecurity threats.

The legal protections offered by CISA encourage private organizations to share information without fear of repercussions, enhancing the Nation's ability to respond to cyber attacks. It facilitates the exchange of critical cyber information threats between private-sector companies and the Federal Government.

CISA provides incentives for companies to share cybersecurity threat indicators, such as software vulnerabilities and malware, with the Department of Homeland Security, DHS. This collaboration is crucial for preventing data breaches and attacks from cyber criminals and foreign adversaries.

This law has been pivotal in addressing some of the most significant cyber threats over the past decade, including high-profile incidents like the SolarWinds breach and, more recent, the Volt Typhoon and Salt Typhoon campaigns. These attacks underscore the growing sophistication and scale of cyber threats we face today.

As noted by Senators Gary Peters and Mike Rounds, allowing CISA 15 to lapse would significantly weaken our cybersecurity ecosystem and undermine the ability to address these sophisticated threats. Moreover, a lapse would remove essential liability protections and hinder defensive operations across critical sectors.

The protections under CISA 15 have provided legal certainty for companies that might otherwise hesitate to share critical data threats.

This safe harbor provision has been crucial in fostering a culture of trust and collaboration. Without this legal protection, the flow of vital threat intelligence would slow, hindering both proactive and reactive cyber defense efforts.

Cybersecurity is a team sport, one that requires collaboration between Government and private sector. Information sharing is essential for national security as cyber threats become increasingly sophisticated.

The current global cyber threat environment demands constant information exchange between these sectors to protect the Nation's critical infrastructure.

CISA 15 has been instrumental in supporting this collaboration, particularly through initiatives like the Joint Cyber Defense Collaborative, which unites Federal agencies and leading private-sector companies.

Unfortunately, the recent termination of the Critical Infrastructure Partnership Advisory Council, the disbandment of the Cyber Safety Review Board, and the dismissal of members of the Cybersecurity Advisory Committee have undermined public-private cooperation in cybersecurity. These advisory bodies have played crucial roles in fostering dialog and sharing best practices between Government and industry. Their loss has created a gap that must be addressed.

The importance of public-private partnerships is further emphasized by the fact that critical infrastructure sectors, such as energy, finance, and health care, are predominantly managed by private companies. These industries rely on timely and accurate information to protect themselves against attacks from nation-state actors and cyber criminals.

Information sharing is crucial for defending against complex state-sponsored attacks, such as those originating from Russia, China, and North Korea.

The NTSC was directly involved in creating the Cybersecurity Advisory Committee, which was introduced in 2019 through bipartisan legislation, a bill aimed at establishing an advisory committee composed of highly-skilled cybersecurity professionals responsible for protecting enterprises across all primary business sectors.

The Advisory Committee would serve as a valuable cyber resource, providing unparalleled insight and expertise to the director of the Cybersecurity and Infrastructure Security Agency and Homeland Security.

The NTSC, in collaboration with these Members of Congress and this committee, proposed the idea for the Advisory Committee and played a central role in the establishment.

In conclusion, the reauthorization of CISA 15 is crucial for maintaining the Nation's cybersecurity and strengthening public-private partnerships in cybersecurity. The law has fostered a collaborative environment that enables real-time sharing of cyber intelligence and defends against attacks from sophisticated adversaries.

We urge Congress to prioritize a clean reauthorization of CISA 15 and to ensure that we continue to look at areas we can focus on joint public-private cybersecurity collaboration.

I thank you for your attention to this critical issue, and I look forward to addressing your questions.

[The prepared statement of Ms. Kuehn follows:]

PREPARED STATEMENT OF KATHERINE KUEHN

WEDNESDAY, MAY 15, 2025

The National Technology Security Coalition (NTSC) is a nonprofit, nonpartisan organization that serves as the preeminent advocacy voice for the chief information security officer (CISO) and senior security technology executives. Through dialog, education, and Government relations, we unite both public and private-sector stakeholders around policies that improve national cybersecurity standards and awareness.

Chairman Garbarino, Ranking Member Swalwell, and Members of the committee, thank you for the opportunity to testify today in support of reauthorizing the Cybersecurity Information Sharing Act of 2015 (CISA 2015) and the importance of public-private partnerships in protecting our national security. My name is Katherine Kuehn, and I am a board member of the National Technology Security Coalition (NTSC), serving as the CISO-in-residence.

Established in 2016, the NTSC is a nonprofit, nonpartisan organization that advocates for chief information security officers, chief privacy officers, and senior security technology executives. NTSC's mission is to advance cybersecurity policies that protect critical infrastructure and foster strong collaboration between the public and private sectors to secure our digital landscape. As part of this mission, we have been deeply involved in shaping the national conversation on cybersecurity, including advocacy for the creation of the Cybersecurity Advisory Committee.

The Cybersecurity Information Sharing Act of 2015 has been a cornerstone of our national cybersecurity strategy. Since its inception, this law has fostered collaboration between industry leaders and Federal agencies, enabling the identification and mitigation of cybersecurity threats. The legal protections offered by CISA encourage private organizations to share information without fear of legal repercussions, enhancing the Nation's ability to respond to cyber attacks. It facilitates the exchange of critical cyber threat information between private-sector companies and the Federal Government. Through CISA 2015, companies can share indicators of cyber threats, such as software vulnerabilities, malware, and malicious IP addresses, without fearing liability or legal repercussions. This collaborative approach has been instrumental in enhancing the Federal Government's ability to respond to cyber attacks quickly and effectively.

CISA provides incentives for companies to share cybersecurity threat indicators, such as software vulnerabilities and malware, with the Department of Homeland Security (DHS). This collaboration is crucial for preventing data breaches and attacks from cyber criminals and foreign adversaries. This law has been pivotal in addressing some of the most significant cybersecurity threats over the past decade, including high-profile incidents like the SolarWinds breach and the more recent Volt Typhoon and Salt Typhoon campaigns. These attacks underscore the growing sophistication and scale of cyber threats we face today. As noted by Senators Gary Peters and Mike Rounds, allowing CISA 2015 to lapse would "significantly weaken our cybersecurity ecosystem" and undermine the ability to address these sophisticated threats.

Moreover, a lapse would remove essential liability protections and hinder defensive operations across critical sectors. The protections under CISA 2015 have provided legal certainty for companies that might otherwise hesitate to share critical threat data. This "safe harbor" provision has been crucial in fostering a culture of trust and collaboration. Without this legal protection, the flow of vital threat intelligence would slow, hindering both proactive and reactive cyber defense efforts.

Cybersecurity is a team effort—one that requires collaboration between the Government and the private sector. Information sharing is essential for national security as cyber threats become increasingly sophisticated. The current global cyber threat environment demands constant information exchange between these sectors to protect the Nation's critical infrastructure. CISA 2015 has been instrumental in supporting this collaboration, particularly through initiatives like the Joint Cyber Defense Collaborative, which unites Federal agencies and leading private-sector cybersecurity firms.

Unfortunately, the recent termination of the Critical Infrastructure Partnership Advisory Council, the disbandment of the Cyber Safety Review Board, and the dismissal of members of the Cybersecurity Advisory Committee have undermined public-private cooperation in cybersecurity. These advisory bodies played a crucial role in fostering dialog and sharing best practices between the Government and industry. Their loss has created a gap in collaboration that must be addressed.

The importance of these public-private partnerships is further emphasized by the fact that critical infrastructure sectors—such as energy, finance, and health care—are predominantly managed by private companies. These industries rely on timely and accurate information to protect themselves against attacks from nation-state actors and cyber criminals. Information sharing is crucial for defending against complex, state-sponsored cyber attacks, such as those originating from Russia, China, and North Korea.

The NTSC was directly involved in creating the Cybersecurity Advisory Committee, which was introduced in 2019 through bipartisan legislation. In the 116th Congress, Representatives John Katko, Dan Newhouse, Brian Fitzpatrick, and Dan Lipinski introduced H.R. 1975, the Cybersecurity Advisory Committee Act of 2019, a bill aimed at establishing an advisory committee composed of highly-skilled cybersecurity professionals responsible for protecting enterprises across all primary business sectors. The advisory committee would serve as a valuable cyber resource, providing unparalleled insight and expertise to the director of the Cybersecurity and Infrastructure Security Agency and the Secretary of Homeland Security. The NTSC, in collaboration with these Members of Congress and this committee, proposed the idea for the advisory committee and played a central role in its establishment.

The advisory committee was established to provide expert guidance on cybersecurity policy and offer actionable recommendations to enhance the Nation's defenses. Its work has been invaluable in shaping cybersecurity policy and ensuring the Government remains in close contact with industry leaders. Reinstating this advisory body is essential for ensuring that our cybersecurity policies continue to evolve in response to new threats.

Given the urgency of the current cyber threat landscape, Congress must proceed with a clean reauthorization of CISA 2015. While there will be opportunities to adjust the law in the future, now is not the time for complicated negotiations that could delay reauthorization. A clean reauthorization would preserve the practical framework that facilitates public-private collaboration and provides legal protections for information sharing.

In conclusion, the reauthorization of CISA 2015 is crucial for maintaining the Nation's security and strengthening public-private partnerships in cybersecurity. The law has fostered a collaborative environment that enables the real-time sharing of cyber threat intelligence, helping to defend against attacks from sophisticated adversaries.

We urge Congress to prioritize a clean reauthorization of CISA 2015 to ensure the continued effectiveness of these public-private partnerships and the legal protections they provide. Furthermore, we urge Congress and the administration to reinstate advisory bodies, such as CIPAC, CSRB, and CSAC, to strengthen public-private cybersecurity collaborations.

Thank you for your attention to this critical issue. I look forward to addressing any questions you may have.

Mr. GARBARINO. Thank you, Ms. Kuehn.

Members will be recognized by order of seniority for their 5 minutes of questioning. I want to remind everyone to please keep their questioning to 5 minutes. Sometimes we go over. It's OK. An additional round of questioning may be called after all Members have been recognized.

I now recognize the gentleman from Florida, Mr. Gimenez, for 5 minutes of questioning.

Mr. GIMENEZ. Thank you, Mr. Chairman.

I understand the importance of reauthorizing that bill, but what is the state of the cyber threat today compared to what it was 10 years ago?

Mr. Miller.

Mr. MILLER. Thank you for the question, Congressman.

I think by any account, the state of the cyber threat today is that there are far more threats. We have a different technology environment, including threats such as ransomware, which we weren't really talking about 10 years ago, threats to operational technology, and artificial intelligence, which is clearly on everyone's minds. Artificial intelligence can be used both as a sword and a shield, as it were.

Also, I think it's fair to say that we have much more—even more sophisticated nation-state threat actors, the usual suspects, of course, China, Russia, North Korea, Iran.

So, I mean, I think when we look at it and we look at the cyber threat ecosystem in particular, there are a lot more threats. But the good news is, in large part because of CISA 15, we're able to share much more information at scale to keep pace with the various different changes in technology today than we were 10 years ago. That's why I think you hear unanimity on this panel that we need to—

Mr. GIMENEZ. There are a number of cybersecurity companies that are contracted by different companies, et cetera, right? So do you find that they share information freely or do they try to keep their stuff proprietary and try to shield themselves from competition?

Mr. MILLER. Well, I mean, I don't know that I can talk about individual companies' business practices. But I will say, generally speaking, that when we think about Automated Indicator Sharing in particular we have—yes, there are some very large, excellent cyber threat companies who are sharing information with their customers at scale. They're plugged into the AIS system.

Mr. GIMENEZ. But that's not—I'm not talking about their customers. I'm talking about sharing it throughout the Nation. In other words, not just their customers. I'm talking about sharing information with other entities that may not be using the same company for cybersecurity.

How is that? Is there still a barrier there? Are there barriers there? Or are they freely sharing information across different companies and different platforms?

Mr. MILLER. I think when we look at the Information Sharing and Analysis Centers, the ISACs—and I can most speak to the IT-ISAC, but there are ISACs for all 16 critical infrastructure sectors—there are thousands of companies participating in those ISACs and sharing information, including the cybersecurity companies.

I mean, as far as I know, there are not barriers to sharing there. Actually, the fact that we are able to share at scale amongst all these different entities is certainly a very good thing, because the cyber companies do participate in those sorts of sharing activities.

There are others, other groups, like the Cyber Threat Alliance for instance, there are various other information and sharing and analysis organizations out there, and there's a lot of sharing going on, much, much more sharing than there was pre-CISA 15.

Mr. GIMENEZ. Thank you.

You talked about artificial intelligence, that it could be a sword or it could be a shield. Who's winning?

Mr. MILLER. I mean, I'd certainly like to think that the good guys are winning. Right now, it's probably——

Mr. GIMENEZ. That's a matter of perspective. When we're trying to hack into somebody else, we're the good guys. So that's a sword.

So who's winning, the sword or the shield? Who is keeping pace with who? Is the shield keeping pace with the sword?

Mr. MILLER. I think it's hard to generalize, but, I mean, I think that the way in which artificial intelligence technology is being used by defenders is proving quite effective today. But we really can't let our guard down, because, again, the good guys are innovating and so are the bad guys. So we really need to keep pace.

Mr. GIMENEZ. Do you think that it would be a wise move for Congress, for the Government, to invest in artificial intelligence as a shield? Because we're never going to match our adversaries in terms of the manpower that they pour into this effort. The only way that we can match that is through automation.

Do you agree with that, Mr. Schimmeck?

Mr. SCHIMMECK. Similar to private-sector companies, the U.S. Government should be investing in artificial intelligence, improving its capabilities. We rely on the U.S. Government and its capabilities, both offensive and defensive in nature, to support us and protect us. So the more effective you can be, the better protected we're going to be in the end.

Mr. GIMENEZ. Thank you so much.

I yield back.

Mr. GARBARINO. The gentleman yields back.

I always love when you ask questions. I never know where you're going to go.

[Laughter.]

Mr. GIMENEZ. I don't either until I get here.

Mr. GARBARINO. I love it.

I now recognize the gentleman from Rhode Island, Mr. Magaziner, for 5 minutes of questions.

Mr. MAGAZINER. Thank you, Chairman.

The Cybersecurity and Infrastructure Security Agency, CISA, leads our Nation in securing businesses' critical infrastructure and the Government from cyber criminals, hackers, and adversarial countries.

When U.S. businesses are attacked, CISA provides vital response and recovery. When there's an emerging cyber threat or a breach, CISA warns private industry about the threat and also provides training and education to the private sector, critical information operators, educational partners, and the general public.

The absolutely vital work done at CISA makes our country safer from the growing threats on cyber space, in cyber space. I am glad that there is bipartisan interest in reauthorizing the Cyber Information Sharing Act of 2015 so that this work can continue.

In part, though, the continued success of CISA and the hopefully growing success of CISA depends not just on this legislation being reauthorized but in making sure that CISA is adequately resourced. We need to ensure that the Trump and Musk administration doesn't cut CISA to the extent that they have announced they intend to do so. We should be investing in this space, not cutting back, because our adversaries are not cutting back.

If we're going to believe that the administration takes cybersecurity seriously, then we're going to need to see from them a reversal in their plan to cut nearly half a billion dollars from CISA's budget, which is what was proposed in the administration's fiscal 2026 budget. If the administration took cybersecurity seriously, they would be investing in CISA, not cutting it.

So we need to talk about that. Then we need to talk about the alternative. How do we build CISA up to continue to be successful going forward in the context of an ever-more complex and hostile threat environment targeting the United States?

So I'll start with Ms. Kuehn.

So in April it was reported that the administration, the Trump administration, plans to cut over a thousand jobs at CISA, which is expected to impact a myriad of programs across the agency.

Can you discuss what the impact of those kinds of work force cuts would be and whether they are a good idea or not?

Ms. KUEHN. So I think when you talk about the threats—if we talk about the threats that we're facing right now—you were asking about adversaries earlier.

One of the critical roles that CISA is playing right now is that we really have, with the advent of AI, and specifically generative and agentic AI, 3 types of threats right now. We have malicious, which we all understand, nation-state adversaries and criminals.

We also have malfunction and mistake. So if we think about what happened this summer with CrowdStrike from a software incident perspective, and then also with AI when all of a sudden an LM decides to go poorly.

So CISA is playing a critical role, No. 1, the public partnership groups that I discussed before, like JCDC and the Advisory Council, of helping share information between the companies that are on the front lines in the private sector developing technologies and the Government when things happen from a threat perspective.

The other thing that's really critical is we talk a lot about the private sector, but the reality is, is that a huge amount of our critical national infrastructure sits within medium and small businesses, and they rely on CISA for things like the small company guidances that came out in the last few years with cyber.

Mr. MAGAZINER. Yes. I think that's such an important point. I mean, one of the things that I think the general member of the public doesn't fully appreciate unless they're deep in this stuff is that when our adversaries, particularly the state actors, China, Iran, North Korea, others, are trying to hack into U.S. systems, it's not just the big Government agencies like the Pentagon or the big companies like Northern Trust, but small and medium-sized businesses, and also all of these local utilities and local governments all across the country.

We hear about these cases in Classified settings, but there are also plenty of cases that have been publicly reported of local water systems, local airports, et cetera.

So, again, just getting back to the issue of resources and work force, CISA has, I mean, thousands and thousands of customers that it needs to interface with, small businesses, small localities.

So, again, how important is it that we maintain a strong work force at CISA in that light?

Ms. KUEHN. So I'll give an example. You talk about the small businesses and the importance of CISA.

Not long ago I was on a plane chatting with a woman next to me. She was on her way to Florida because she was meeting her husband and her grandkids, and her husband was retiring from his job.

What did he do? Well, he was a concrete distributor in Dallas. She explained to me that they were selling the company.

The company was going out of business, basically, because, she literally went, "There was one of those ransomware attack things. He borrowed my phone and did something for business on my phone, and we had a ransomware thing. And something, there was a gang in Turkiye"—and this is her explaining this to me—"who charged us \$6 million. And it was just too hard to clean up. We don't have the ability of understanding the cybersecurity. And so we just gave up and we're closing the business and he's going to retire."

That's the issue we're facing here, is that while we can represent large organizations that can spend millions and millions and millions on cybersecurity, there are exponentially more organizations out there—critical national infrastructure, small banks, grocery stores, you name it—that don't have the ability and need organizations like the program CISA provides in order to ensure that we have mature cybersecurity.

Mr. MAGAZINER. Thank you.

Mr. GARBARINO. The gentleman yields back.

I now recognize the gentleman from Tennessee, Mr. Ogles, for 5 minutes of questions.

Mr. OGLES. Thank you, Mr. Chairman.

Thank you to the witnesses.

I think, by and large, we all agree that CISA should be reauthorized. So then the question becomes: How do we make it better? I know there have been some calls, let's do a clean re-auth and just get it out the door quickly.

But as we look at the landscape as we go forward, obviously in battlefield terms, as warfare has changed, I would argue that one of those battlefields is in the cyber realm.

So, Mr. Miller, I know you've had some suggestions in particular, some of the definitions as it pertains to CISA. Any thoughts on how we can improve as we go into reauthorization to make it better, stronger, more robust?

Mr. MILLER. Thank you for that question, Congressman.

Yes, I did include some recommendations in my statement. I mean, I do think, in general, the approach that we should be taking if we're looking at changes is to just ask a pretty simple question: Hey, what's changed in the past 10 years from a threat standpoint, from a technology standpoint?

Are the very technical definitions that we have of cyber threat indicator and defensive measures in the bill, do they really account for all the different types of attacks that companies are experiencing today? Are we sharing the types of threat information that we need to counteract those threats?

I think one example of a relatively novel type of attack that's grown to prominence—I mean, someone mentioned SolarWinds earlier—supply chain attacks, software supply chain attacks.

Right now, if a company knows that there is a suspect supplier in its supply chain, it doesn't get the type of liability protections that CISA provides to share that sort of information.

So if you were thinking about making surgical, precise edits or changes to the bill, again, I would not open it up entirely, but you could look at things like the definition of cyber threat indicator, which has, I don't know, 7 or 8 subparts, and you could perhaps add something like derogatory information about a supplier in your supply chain or something like that.

That's just an example. But, I mean, that's like the general type of approach I would take rather than making wholesale changes to update the law.

Mr. OGLES. Well, kind-of going back to Mr. Gimenez's point, I think one of the things we need to look at is better information sharing, broadening the scope of who might be included. But then, with that, you probably need, to your point, the liability protections to protect someone as they're sharing information that otherwise might be.

So what about the JCDC? What role might they play as we go forward?

Mr. MILLER. Yes. I mean, as others have testified to, the JCDC is a very valuable newer partnership that CISA has led, obviously.

It's really focused on operational collaboration as opposed to simply sharing information, and that's really what this is all about.

I will say, it is my understanding that you really could not have JCDC still without the liability protections that exist in CISA 15, though.

I mean, there are MOUs that companies that participate in JCDC sign, but that really deals more with information dissemination and adhering to pretty strict traffic light protocols. It doesn't have anything to do with the fundamental liability protections and authorizations that CISA provides for sharing the threat information in the first place, which at the end of the day is what underpins JCDC.

Mr. OGLES. Ms. Rinaldo, you touched on China in rather stark terms. Do you just want to give us a quick brief of are we adequately protecting ourselves with CISA and the reauthorization in terms of China and obviously their bad actions?

Ms. RINALDO. Absolutely. When we were doing our fact-finding mission as we were drafting the legislation, one thing that was very abundantly clear is that more than 90 percent of our networks are held by the private sector. So what can we do as a Government to help protect the private sector?

So the idea of information sharing and the importance of Government to business. I think, to your question to John, how do we improve the transport of information from the Government to business? I would say that was one part that's lacking today. Not necessarily need—you don't need a Congressional change to make that happen, just oversight. How could we stay on top of the agencies to make sure that they are pushing out information?

Then I would also say security clearances is a big issue. You may have people that can get a clearance, go into a room, hear the information, but do you have the engineers that can actually act on it? So that's an important aspect as well.

Mr. OGLES. Mr. Chairman, I know I'm out of time. But I would just say to all the witnesses, if you have any suggestions or recommendations that might be specific as to how we make it better, now would be the time to provide that input. So if you would like to send that to my office or, of course, to anyone on the committee, the Chairman, happy to take a look at that, incorporate it, because, obviously, again, as we look to the future, as we look to the future of warfare, this is one of those battlefronts. We need to be ready. We need to be proactive. We need to be ahead of the AI curve.

Mr. Chairman, I yield back. Thank you for your graciousness.

Mr. GARBARINO. The gentleman yields back.

I second that thought. So that's great.

I now recognize the Ranking Member, the gentleman from California, Mr. Swalwell, for 5 minutes of questions.

Mr. SWALWELL. Thank you.

To follow what Ms. Rinaldo was saying about JCDC, Ms. Kuehn, can you discuss how JCDC facilitates information sharing? To Ms. Rinaldo's point, how important is it for CISA 2015 to be effective that we have a mechanism like JCDC that facilitates cross-sector information sharing?

Ms. KUEHN. I think how JCDC disseminates today and the critical importance of it and, to your point, that it's a relatively new program, one of the things about it is it allows for rapid distribution when threat happens between industry and Government so that we have, in essence, a real-time channel of things that are going on.

From an industry perspective it's really important that we even broaden the scope of it to work closer with the ISACs and to think about how we can distribute not just to the top level of industry but actually pull it down.

From a JCDC perspective, I think it's one of the best things we've seen come out of CISA so far, and it's still evolving.

But that ability to have information sharing without repercussion I think is one of the areas that we really need to focus on. So that's why looking at the, in essence, reauthorization of this act is so important, because we're just at the beginning of where JCDC could go.

As we start to think about—we mentioned China, but if we think about the Chinese threats that have come in from Volt Typhoon, Salt Typhoon, Flax Typhoon, Nylon Typhoon—there's a lot of typhoons right now—we're going to see, in essence, cross-pollination of those critical vulnerabilities' exploits, and JCDC is going to be incredibly important to ensure we disseminate rapidly through that.

Mr. SWALWELL. To Ms. Rinaldo's point about security clearances, it's a frustration I share as well. My district is high tech and biotech, two nuclear labs. Often I hear what Ms. Rinaldo is saying, which is, yes, the CEO is cleared, but he's not the engineer. He doesn't understand. No. 1, his time is limited, or her time is limited; and, No. 2, he or she doesn't have the skill set to receive and

understand the threat. But the problem on the Government side is they're not really willing to clear that many individuals.

I just welcome your feedback on if you're seeing that. Because if you remember like 2 years ago, it was a 19-year-old who was caught leaking Ukraine war plans, and it was a military service member. You're like, wait, we have a 19-year-old like basically the war plans for Ukraine, but we have like 20-year professionals who we could give 1-day passes or more information to better protect critical infrastructure and we're cautious about that?

So it just seems like we've got the priorities crosswise. But I'd welcome feedback from you, Ms. Kuehn, on that.

Ms. KUEHN. It's interesting. I've been in cybersecurity for over 25 years, and some of the first attacks or hacks I dealt with were nation-state-level attacks going around the financial services network. You can imagine, I was 23 years old walking rooms with Scotland Yard and looking at data center break-ins. Then some of the first financial services attacks.

I have never held a security clearance in the United States and I've been a risk executive of 2 Fortune 25 companies.

The reality is that we do need to reexamine how we look at clearance. But we also have to think about the fact that cybersecurity is to some degree—and we talked about it—a team sport. I've known 15-year-olds who have had inventions become state secrets and housed in the NSA, and I've known 90-year-olds who still sit on boards and talk about cybersecurity.

The reality of today's risk is that cyber risk is now business risk. It's a question of how we look at protecting all the different areas. Companies look at risk from a financial, operational, resilience perspective, everything.

So from a clearance perspective, it's getting the right individuals in an organization cleared to ensure they understand, but also to make it more of a common language so we understand the impact risk has on our organizations.

Mr. SWALWELL. Just as Mr. Ogles said, I welcome ideas, feedback. I am a little hesitant to want to amend this at all at this point, at this late hour, risking that opening this up would not see it reauthorized.

But I do agree with Mr. Ogles that we need your feedback. Just because we reauthorize it, if we do it in a clean way, that doesn't mean we can't down the road, even right after reauthorization, have hearings and mark-ups to make it even better.

But avoiding a lapse is my priority, and it sounds like, Ms. Kuehn, you agree.

Ms. KUEHN. That would actually be my recommendation. I think that a reauthorization cleanly and then look at how we optimize and look at things down the road for a couple reasons.

We're at the beginning of AI. We're still trying to figure out some things regarding different types of attacks. Like I said, we have malicious, mistake, and malfunction. I think there's a way we can strengthen public-private on the back of it. But I would recommend a clean authorization.

Mr. SWALWELL. Thank you. I yield back.

Mr. GARBARINO. The gentleman yields back.

I now recognize myself for 5 minutes of questions.

I just want to say, since the beginning of Congress we have been approached by countless stakeholders about the need to reauthorize CISA 2015. In fact, we have 8 statements that we will be submitting for the record, one of which has 52 organizations as signatories.

So I would like to, without objection, add these to the record.

So done. OK, wonderful. So ordered.

That's great. I can do this by myself. Wonderful.

[The information follows:]

LETTER FROM BUSINESS ROUNDTABLE

May 15, 2025.

The Honorable MARK GREEN,
Chairman, Committee on Homeland Security, U.S. House of Representatives, Washington, DC 20515.

The Honorable BENNIE THOMPSON,
Ranking Member, Committee on Homeland Security, U.S. House of Representatives, Washington, DC 20515.

The Honorable ANDREW GARBARINO,
Chairman, Subcommittee on Cybersecurity and Infrastructure Protection, Committee on Homeland Security, U.S. House of Representatives, Washington, DC 20515.

The Honorable ERIC SWALWELL,
Ranking Member, Subcommittee on Cybersecurity and Infrastructure Protection, Committee on Homeland Security, U.S. House of Representatives, Washington, DC 20515.

DEAR CHAIRMAN GREEN, RANKING MEMBER THOMPSON, SUBCOMMITTEE CHAIRMAN GARBARINO, AND SUBCOMMITTEE RANKING MEMBER SWALWELL: Business Roundtable urges the Committee on Homeland Security to swiftly consider legislation to reauthorize the Cybersecurity Information Sharing Act of 2015 to ensure there is no disruption in the critical information-sharing activities on which the public and private sectors depend to defend against escalating cyber threats. A lapse in the Cybersecurity Information Sharing Act of 2015 authorities would hamstring both Federal and private-sector preparedness for and response to cyber threats. It would signal to malicious threat actors that, after September 30, 2025, the United States' cybersecurity posture will weaken, potentially encouraging future attacks on our critical infrastructure.

Since enactment, the Cybersecurity Information Sharing Act of 2015 has played a crucial role in facilitating information sharing on cybersecurity threats in the United States. By providing liability protections and exemptions from Federal anti-trust law, Freedom of Information Act disclosure, and State disclosure laws, the law incentivizes voluntary sharing of cyber threat indicators and defensive measures. This law ultimately simplifies the process for sharing information, reducing regulatory burden and accelerating the response to cybersecurity incidents within and across sectors. The collective defense of private-sector networks is more important than ever as the cyber threat landscape grows increasingly perilous.

As the Federal Government and private sector have worked to collaboratively improve cybersecurity, the Cybersecurity Information Sharing Act of 2015's framework has served as the foundation. For example, the law underpins not only Cybersecurity and Infrastructure Security Agency's (CISA) Joint Cyber Defense Collaborative but also serves to drive greater information sharing between the various critical infrastructure sectors through Information Sharing and Analysis Centers. Moreover, the Cyber Incident Reporting for Critical Infrastructure Act explicitly builds on Cybersecurity Information Sharing Act of 2015 by directing CISA to use consistent procedures for incident reporting.

Thank you for holding today's hearing entitled "In Defense of Defensive Measures: Reauthorizing Cybersecurity Information Sharing Activities that Underpin U.S. National Cyber Defense." Business Roundtable appreciates the Committee on Homeland Security's commitment to strengthening the Nation's cybersecurity defenses. Reauthorization of the Cybersecurity Information Sharing Act of 2015 is critical for the public and private sectors to defend against escalating cyber threats. We look forward to continued collaboration with you and your staff to ensure this essential authority is renewed.

AMY SHUART,
Vice President, Technology & Innovation, Business Roundtable.

STATEMENT OF THE PROTECTING AMERICA'S CYBER NETWORKS COALITION

MAY 13, 2025

TO THE MEMBERS OF THE U.S. CONGRESS: The Protecting America's Cyber Networks Coalition (the Coalition) urges Congress to reauthorize the Cybersecurity Information Sharing Act of 2015 (CISA 2015) before it expires on September 30, 2025.

Reauthorizing CISA 2015 is a top policy priority for the Coalition, a partnership of leading business associations representing nearly every sector of the U.S. economy. If CISA 2015 lapses, the United States will encounter a more complex and dangerous security environment. A variety of foreign cyber criminals are targeting our advanced commercial capabilities, critical infrastructure, and economic well-being through various tactics, such as phishing and ransomware.¹ Malicious hackers target both large national corporations and local branches, offices, and warehouses. Their attacks impact individual businesses, people, and their surrounding communities.

Sharing information about cyber threats and incidents complicates attackers' operations because defenders learn what to monitor and prioritize. Consequently, attackers are forced to invest more in new tools or target different victims. CISA 2015 helps defenders improve their security measures while raising costs for attackers.

Congress passed CISA 2015 with bipartisan support from both parties and the administration.² This important cybersecurity law enables private entities to increase their protection of data, devices, and computer systems while promoting the sharing of cyber threat information with industry and Government partners within a secure policy and legal framework. CISA 2015 also provides protections for businesses related to public disclosure, regulatory issues, and antitrust matters to promote the timely exchange of information between public and private entities. Industry and Government have a strong record of safeguarding privacy and civil liberties under this legislation.³

CISA 2015 is a cornerstone of American cybersecurity. It enhances businesses' ability to respond swiftly to today's cyber threats, including tackling cybersecurity issues and addressing them at scale. Lawmakers must send the CISA 2015 reauthorization legislation to the president to continue ensuring that businesses have legal certainty and protection against frivolous lawsuits when voluntarily sharing and receiving threat indicators and taking steps to mitigate cyber attacks.

Since the implementation of CISA 2015, collaboration in cybersecurity has improved significantly in several ways, including encouraging the development and/or the expansion of information sharing and analysis centers, or ISACs, across multiple sectors. These centers serve as hubs for sharing cybersecurity information within specific industries, thereby boosting sector-specific threat detection and response capabilities.

Cyber incidents underscore the need for legislation that helps businesses augment their understanding of cybersecurity threats and strengthen their protection and response capabilities in collaboration with Government entities.⁴ It is encouraging that leading members of the House and Senate Homeland Security and Intelligence committees advocated for the renewal of CISA 2015.⁵

The Coalition is dedicated to collaborating with the Trump administration and lawmakers to swiftly reauthorize CISA, thus enhancing national security and bol-

¹ *Annual Threat Assessment of the U.S. Intelligence Community*, Office of the Director of National Intelligence, March 18, 2025. <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf>.

² Consolidated Appropriations Act, 2016 (Pub. L. 114–113), December 18, 2015 (see division N, title I). <https://www.congress.gov/114/statute/STATUTE-129/STATUTE-129-Pg2242.pdf>.

³ "Recent Inspector General reviews have not found that [personally identifiable information] has been shared in violation of the act." Congressional Research Service, *The Cybersecurity Information Sharing Act of 2015: Expiring Provisions*, April 8, 2025. <https://www.congress.gov/crs-product/IF12959>.

⁴ *Cybersecurity: Selected Cyberattacks, 2012–2024*, Congressional Research Service, January 8, 2025. <https://www.congress.gov/crs-product/R46974>.

⁵ "A major cybersecurity law is expiring soon—and advocates are prepping to push Congress for renewal," *CyberScoop*, February 26, 2025. <https://cyberscoop.com/cybersecurity-information-sharing-law-expiring-congress-renewal>.

stering the resilience and protection of the U.S. business community.⁶ Congressional action is urgently needed.

Sincerely,

ACT/THE APP ASSOCIATION
 AIRLINES FOR AMERICA (A4A)
 ALLIANCE FOR AUTOMOTIVE INNOVATION
 ALLIANCE FOR CHEMICAL DISTRIBUTION (ACD)
 AMERICAN CHEMISTRY COUNCIL (ACC)
 AMERICAN COUNCIL OF LIFE INSURERS (ACLI)
 AMERICAN FUEL & PETROCHEMICAL MANUFACTURERS (AFPM)
 AMERICAN GAMING ASSOCIATION
 AMERICAN GAS ASSOCIATION (AGA)
 AMERICAN INSTITUTE OF CPAS
 AMERICAN PETROLEUM INSTITUTE (API)
 AMERICAN PROPERTY CASUALTY INSURANCE ASSOCIATION (APCIA)
 AMERICAN PUBLIC POWER ASSOCIATION (APPA)
 AMERICAN SHORT LINE AND REGIONAL RAILROAD ASSOCIATION (ASLRRA)
 AMERICAN WATER WORKS ASSOCIATION (AWWA)
 ASIS INTERNATIONAL
 ASSOCIATION OF AMERICAN RAILROADS (AAR)
 ASSOCIATION OF METROPOLITAN WATER AGENCIES (AMWA)
 BUSINESS SOFTWARE ALLIANCE (BSA)
 COLLEGE OF HEALTHCARE INFORMATION MANAGEMENT EXECUTIVES (CHIME)
 CONNECTED HEALTH INITIATIVE (CHI)
 CTIA
 CYBERACUVIEW
 THE CYBERSECURITY COALITION
 EDISON ELECTRIC INSTITUTE (EEI)
 ELECTRIC POWER SUPPLY ASSOCIATION (EPSA)
 THE FERTILIZER INSTITUTE (TFI)
 THE FINANCIAL SERVICES INFORMATION-SHARING AND ANALYSIS
 CENTER (FS-ISAC)
 THE GRIDWISE ALLIANCE
 HEALTHCARE INFORMATION AND MANAGEMENT SYSTEMS SOCIETY (HIMSS)
 HEALTHCARE LEADERSHIP COUNCIL (HLC)
 HEALTH-ISAC
 INTERNET SECURITY ALLIANCE (ISA)
 INTERSTATE NATURAL GAS ASSOCIATION OF AMERICA (INGAA)
 LARGE PUBLIC POWER COUNCIL (LPPC)
 NATIONAL ASSOCIATION OF WATER COMPANIES (NAWC)
 NATIONAL DEFENSE INDUSTRIAL ASSOCIATION (NDIA)
 NATIONAL ELECTRICAL MANUFACTURERS ASSOCIATION (NEMA)
 NATIONAL PROPANE GAS ASSOCIATION (NPGA)
 NATIONAL RETAIL FEDERATION (NRF)
 NCTA—THE INTERNET & TELEVISION ASSOCIATION
 NTCA—THE RURAL BROADBAND ASSOCIATION
 OPEN RAN POLICY COALITION
 PLUMBING MANUFACTURERS INTERNATIONAL (PMI)
 REINSURANCE ASSOCIATION OF AMERICA (RAA)
 SECURITY INDUSTRY ASSOCIATION (SIA)
 THE SOFTWARE & INFORMATION INDUSTRY ASSOCIATION (SIIA)
 THE SULPHUR INSTITUTE
 TIC COUNCIL
 U.S. CHAMBER OF COMMERCE
 USTELECOM—THE BROADBAND ASSOCIATION
 UTILITIES TECHNOLOGY COUNCIL (UTC).

⁶In April 2025, Secretary of Homeland Security Kristi Noem called for CISA 2015 to be reauthorized. “Homeland Security Secretary Noem urges partnerships to guide future of CISA, backs secure by design” *Inside Cybersecurity*, April 29, 2025. <https://insidecybersecurity.com/daily-news/homeland-security-secretary-noem-urges-partnerships-guide-future-cisa-backs-secure-design>.

LETTER FROM THE ALLIANCE FOR AUTOMOTIVE INNOVATION

May 15, 2025.

The Honorable ANDREW GARBARINO,
*Chairman, Subcommittee on Cybersecurity and Infrastructure Protection, Committee
 on Homeland Security, U.S. House of Representatives, 2344 Rayburn House Of-
 fice Building, Washington, DC 20515.*

The Honorable ERIC SWALWELL,
*Ranking Member, Subcommittee on Cybersecurity and Infrastructure Protection,
 Committee on Homeland Security, U.S. House of Representatives, 174 Cannon
 House Office Building, Washington, DC 20515.*

DEAR CHAIRMAN GARBARINO AND RANKING MEMBER SWALWELL: The Alliance for Automotive Innovation (“Auto Innovators”) appreciates the opportunity to share its support for the reauthorization of the Cybersecurity Information Sharing Act of 2015 (“CISA 2015”). The U.S. automotive industry strongly urges Congress to prevent the September 30, 2025, expiration of this critical law, which is integral to the cybersecurity posture of the automotive ecosystem. We respectfully submit this letter for the hearing record.

Auto Innovators represents the full automotive industry, including the manufacturers producing most vehicles sold today in the U.S., major equipment suppliers, battery manufacturers, semiconductor makers, technology companies, and autonomous vehicle developers. The automotive industry is America’s largest manufacturing sector and underpins our nation’s industrial base. The sector employs ten million Americans in all fifty States and drives \$1.2 trillion into the economy each year—nearly 5 percent of GDP.

Nimbleness and agility in response to a dynamic cybersecurity threat environment—particularly as the modern vehicle fleet becomes more automated, connected, and electrified—remains a top priority for the U.S. automotive industry. Automotive companies rely upon the exchange of cybersecurity threat intelligence, defensive measures, and shared experiences across industry sectors to counter cybersecurity threats and the ever-evolving tactics and capabilities of malicious threat actors. Congress enacted CISA 2015 to enable such cooperation and collaboration with broad bipartisan support.

Key provisions of CISA 2015 include:

- Clear authorization for information sharing of cybersecurity threat indicators, defensive measures, cybersecurity incidents, and significant cybersecurity concerns;
- Exemptions that safeguard shared intelligence and security information from disclosure under the Freedom of Information Act and State open records laws;
- Assurances that threat indicator and defensive measure sharing in accordance with the law do not waive applicable privileges or other protections provided by law, including trade secret protection;
- Designation of threat indicators and defensive measures shared by a private-sector entity with Federal entities as their commercial, financial, and proprietary information; and
- Protections against claims of antitrust violations or civil liability for entities when sharing information in accordance with the provisions of the law.

The Automotive Information Sharing and Analysis Center (“Auto-ISAC”) launched the same year as CISA 2015’s enactment. Established to serve as the trusted cybersecurity community for automotive companies, the Auto-ISAC facilitates the sharing of cybersecurity threat intelligence and insights gained from public and private-sector sources. CISA 2015 fostered confidence among the initial Auto-ISAC members that their unified, community approach to cybersecurity risk mitigation was lawful. In the intervening decade, Auto-ISAC membership has grown over 500 percent, including original equipment manufacturers, suppliers, autonomous vehicle developers, and technology companies, highlighting the value that participants see in this trusted framework. In addition to the exchange of invaluable information, other key initiatives of the Auto-ISAC include table-top exercises, cybersecurity training, development of best practice guides and informational reports on important cybersecurity topics, and the creation of a common threat taxonomy related to automotive cybersecurity governance.

The Auto-ISAC’s initiatives, proactive engagement efforts, threat and incident analyses, and dissemination of cybersecurity awareness and preparedness information depend on the statutory provisions of CISA 2015. These various cybersecurity risk mitigation efforts would not be possible without the authorizations and protections provided by the law.

As a result, Auto Innovators strongly supports Congress’ reauthorization of CISA 2015. Such action is necessary to sustain the U.S. automotive industry’s efforts that

counter the unrelenting dangers posed by malicious threat actors. These efforts are crucial to ensuring the safe operations and resilience of the nation's largest manufacturing sector, and a predictable and durable policy environment related to cybersecurity information sharing is critical to these efforts. Auto Innovators looks forward to partnering with Congress on the reauthorization of CISA 2015, and we are grateful to the subcommittee for holding this hearing on such an important topic.

Sincerely,

JENNICA SIMS,
Director, Federal Affairs.

JOINT STATEMENT OF INTRADO LIFE & SAFETY, THE NATIONAL ASSOCIATION OF
STATE 9-1-1 ADMINISTRATORS, AND NENA—THE 9-1-1 ASSOCIATION

MAY 15, 2025

Intrado Life & Safety, the National Association of State 9-1-1 Administrators, and NENA—The 9-1-1 Association thank you and the Members of the House Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection for holding this critical hearing, titled, "In Defense of Defensive Measures: Reauthorizing Cybersecurity Information Sharing Activities that Underpin U.S. National Cyber Defense."

Two hundred forty million calls are made to 9-1-1 every year. Together, as public safety advocates and industry leaders we proudly represent those who serve others in times of crisis. The networks that support our 9-1-1 infrastructure are the backbone of our national and public safety systems.

But these networks are also under constant threat. Bad actors seeking to cause harm are attempting to infiltrate America's public safety networks on a daily basis. To combat these attempts, we must use every private and public sector tool at our disposal.

That is why we have come together to voice our support for the reauthorization of the Cybersecurity Information Sharing Act, which sunsets on September 30, 2025. This legislation was enacted 10 years ago with the bipartisan vision of incentivizing and protecting information sharing between industry and Government to reduce cybersecurity threats to our Nation. It is working.

As current members of information sharing and analysis centers, we can speak to the invaluable impact the bill has had as we work to defend our network and protect 9-1-1 professionals, first responders, and the communities they serve. Information sharing in these forums provides us with key insights, data, and analysis that allows for quick, decisive action necessary to deploy our cyber defenses.

Nation-state actors and cyber criminals target critical 9-1-1 infrastructure daily. If CISA's authority is not extended, we fear we will lose our ability to be one step ahead of those who attack our critical infrastructure and seek to harm our national security. In short, the United States will encounter a more complex and dangerous security environment.

When we share information about cyber threats and incidents, we learn what to monitor and prioritize. This makes attack operations more difficult and requires bad actors to acquire new tools or target different victims, which raises their cost and gives us time to act.

Information sharing is a cornerstone of cybersecurity best practice, and the public-private sharing that this legislation has encouraged is central to protecting our national security and defending our homeland.

We are grateful to you and the subcommittee for holding this important hearing on the future of this legislation. We are hopeful it will lead to reauthorizing this legislation and needed support our Nation's continued efforts to defend our 9-1-1 systems.

JOINT LETTER FROM MULTIPLE ASSOCIATIONS

April 28, 2025.

The Honorable RAND PAUL,
Chairman, Homeland Security & Governmental Affairs Committee, 295 Russell Senate Office Building, Washington, DC 20510.

The Honorable GARY PETERS,
Ranking Member, Homeland Security & Governmental Affairs Committee, 724 Hart Senate Office Building, Washington, DC 20510.

DEAR CHAIRMAN PAUL AND RANKING MEMBER PETERS: The undersigned trade associations (collectively, “the associations”) urge Congress to extend, for at least 10 years, the Cybersecurity Information Sharing Act (CISA 2015), which is scheduled to expire at the end of September 2025.

Originally enacted in 2015 with broad bipartisan support, CISA 2015 established the voluntary information network to enable “public and private-sector entities to share cyber threat information, removing legal barriers and the threat of unnecessary litigation.”¹ The law remains foundational to strengthening our collective defense against cybersecurity threats, facilitating trust in the public-private partnership, and serving as the backbone of essential programs across the Federal Government—programs that have measurably improved the security posture of critical infrastructure in the United States and strengthened the Federal Governments’ security awareness.

Of paramount importance, the law’s antitrust exemption and liability protections enables private-sector sharing of sensitive cyber information. Our Nation’s critical infrastructure operators depend on threat indicator sharing from one another and from the Federal Government to strengthen their overall defenses. A lapse in CISA 2015 authorities will curb this sharing, which is fundamental for enhancing overall awareness of national security threats.

CISA 2015 continues to improve the capacity and speed of information sharing between the private sector and the Federal Government, while most critically providing necessary protections for privacy and confidentiality. Illustrative of this success is the joint effort of the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI) to identify the People’s Republic of China (PRC) cyber actor, Volt Typhoon, in United States energy systems. This collaboration, fostered by CISA 2015, contributed to one of the most comprehensive, actionable, declassified cyber information sharing reporting in our Nation’s history and continues to lead to further discoveries of this advanced persistent threat actor in other critical infrastructure sectors.

Extending CISA 2015 is also pivotal for supporting the effectiveness of Federal programs, like CyberSentry² and “Section 9”³ support, that mutually benefit the Federal Government as well as the infrastructure operator. In addition, CISA 2015 plays an essential role in the functions of CISA’s Joint Cyber Defense Collaborative (JCDC), which reduces cyber risk by unifying the cyber defense capabilities and actions of Government and industry partners, including the associations’ members. Furthermore, these statutory provisions are so undeniably indispensable that they are incorporated by reference in other significant cyber laws, including the Cyber Incident Reporting for Critical Infrastructure Act.⁴ Within the legal framework of the industry’s Cyber Mutual Assistance (CMA) Program, CISA 2015 provides CMA Program participants additional protections when sharing certain sensitive cybersecurity information with one another. These additional protections strengthen the program and enhance security for the industry by encouraging and protecting greater sharing of cybersecurity information between private entities.

For these reasons, an expiration of these protections risks leaving our infrastructure more vulnerable to cyber incidents that could impact operational integrity and resilience. The associations and the companies we represent thank you for your

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

² Participating entities share threat information with CISA in real time for analysis and further dissemination to critical infrastructure operators across the Nation. CyberSentry also provides valuable insights into the nature and scope of potential cyber attacks, and facilitates proactive mitigation as well as swift and effective incident response planning.

³ See Executive Order—Improving Critical Infrastructure Cybersecurity § 9 (February 12, 2013). <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.

⁴ See 6 U.S.C. § 681e.

leadership on this issue and stand ready to engage with Congress to ensure CISA 2015 remains prioritized in reinforcing our national and energy security goals.

Sincerely,

*American Fuel & Petrochemical Manufacturers Association
American Gas Association
American Petroleum Institute
American Public Gas Association
Edison Electric Institute
GPA Midstream
InterState Natural Gas Association of America
Liquid Energy Pipeline Association.*

CC: The Honorable Mark Green, Chairman, House Homeland Security Committee; The Honorable Bennie Thompson, Ranking Member, House Homeland Security Committee; The Honorable Tom Cotton, Chairman, Senate Select Committee on Intelligence; The Honorable Mark Warner, Ranking Member, Senate Select Committee on Intelligence; The Honorable Rick Crawford, Chairman, House Permanent Select Committee on Intelligence; The Honorable Jim Himes, Ranking Member, House Permanent Select Committee on Intelligence.

STATEMENT OF THE OPERATIONAL TECHNOLOGY CYBERSECURITY COALITION (OTCC)

MAY 15, 2025

The Operational Technology Cybersecurity Coalition, a dedicated group of cybersecurity vendors committed to safeguarding our Nation's critical infrastructure, writes to urge the reauthorization of the Cybersecurity Information Sharing Act of 2015 (CISA 2015).

Since its enactment following the Office of Personnel (OPM) data breach, CISA 2015 has provided a vital framework for voluntary public-private cyber threat information sharing, thereby strengthening our collective national cyber defenses. On November 12, 2024, your full House Committee on Homeland Security released a cyber threat snapshot that detailed a 30 percent increase in cyber attacks targeting critical infrastructure since 2023. The report also cited the Cybersecurity and Information Security Agency's findings that ransomware reports across all sectors increased over 70 percent from 2022 to 2023. The escalating sophistication of cyber threats, underscored by recent attacks on critical infrastructure including Volt Typhoon and Salt Typhoon, and on Federal agencies in incidents like SolarWinds, Storm 0558, and MOVEit, highlight the persistent and critical need for this legislation.

CISA 2015 has successfully facilitated collaboration by providing legal protections, including antitrust exemptions, necessary for companies to confidently share threat indicators and defensive measures with both governmental partners and other private entities. This collaborative environment has demonstrably improved the speed and capacity with which our Nation can respond to large-scale cyber incidents such as the Log4j JNDI attack and the CrowdStrike/Microsoft incident of 2024. In 2022, the latest year for which there is published data, 413,834 cyber threat indicators were shared with the Cybersecurity and Information Security Agency. For operational technology assets of critical infrastructure, this speed is essential to effectively mitigate cyber attacks, which is the core mission of our Coalition.

We firmly believe that a lapse in the CISA 2015 framework would inevitably and immediately reduce the crucial flow of information, leaving the United States—civilian, military, commercial, et al—more vulnerable to the malicious activities of nation-state actors and cyber criminals. These established communication channels are essential for maintaining situational awareness and enabling rapid, effective responses to security incidents which are crucial to protecting operational technology. Furthermore, the provisions of CISA 2015 are foundational to other significant cyber laws, including the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), making its reauthorization essential for the stability of our broader cybersecurity legislative landscape.

The Operational Technology Cybersecurity Coalition champions an open, vendor-neutral approach to cybersecurity, a principle that is bolstered by voluntary information-sharing frameworks like the one established by CISA 2015. Echoing our formal communication sent to Congress on March 21, 2025, we reiterate the urgent call for the extension of the Cybersecurity Information Sharing Act of 2015. Preserving this framework is paramount to maintaining and enhancing the crucial information-sharing capabilities that protect our Nation's critical infrastructure and ensure our national security against ever-evolving cyber threats.

We thank the subcommittee for your leadership on this important matter and remain committed to working alongside you.

STATEMENT OF THE NATIONAL RETAIL FEDERATION

MAY 15, 2025

The National Retail Federation (“NRF”) submits this statement to the committee for its hearing entitled “In Defense of Defensive Measures: Reauthorizing Cybersecurity Information Sharing Activities that Underpin U.S. National Cyber Defense” and in support of the extension and reauthorization of the Cybersecurity Information Sharing Act of 2015 (“CISA 2015”). The framework established by CISA 2015, including its liability protections, has facilitated increased collaboration and information sharing both within the retail sector and between related stakeholders and partners over the past decade. It is critical that Congress reauthorizes the law before September 30, 2025.

NRF passionately advocates for the people, brands, policies, and ideas that help retail succeed. From its headquarters in Washington, DC, NRF empowers the industry that powers the economy. Retail is the Nation’s largest private-sector employer, contributing \$3.9 trillion to annual GDP and supporting 1 in 4 U.S. jobs—52 million working Americans. For over a century, NRF has been a voice for every retailer and every retail job, educating, inspiring and communicating the powerful impact retail has on local communities and global economies.

For more than a decade, NRF has worked to increase collaboration among retailers on cybersecurity. In 2014, NRF established its IT Security Council, a forum for retail Chief Information Security Officers (CISOs) and other senior members of their teams to engage with each other; share best practices; and participate in workshops, benchmarking surveys, and sector-specific cyber exercises.¹ In early 2023, NRF established a formal partnership with the Retail and Hospitality Information Sharing and Analysis Center (“RH-ISAC”) and today works closely with them to increase sector-wide cybersecurity engagement.² NRF has also worked to build ties with key Governmental partners on cybersecurity issues, including the Federal Bureau of Investigation (FBI), U.S. Secret Service, National Institute for Standards and Technology (NIST), and the Cybersecurity and Infrastructure Security Agency (CISA).

Over the past decade, we have seen a gradual increase in the willingness of retailers to share cyber threat indicators that they have uncovered and collected, both via the RH-ISAC and directly with Government and industry partners. While the number of retailers that shared their own cyber threats indicators in the years immediately after CISA 2015 was limited, this engagement has increased over time, such that the RH-ISAC reported that 60 percent of its 300+ member companies had contributed cyber intelligence within the ISAC in 2024, including over 51,000 indicators of compromise and nearly 2,000 responses to requests for information.³

Several factors explain this increase in information sharing over the past decade. Many large and medium-sized retailers have significantly increased the size and capability of their cybersecurity teams, which has strengthened efforts to detect and share information on threats. Retail legal teams have also gradually become more comfortable with allowing their cyber teams to share threat information, in large part due to the liability protections provided by CISA 2015. In the years immediately after CISA 2015 was enacted, NRF regularly heard from retail CISOs that their legal teams were reluctant to allow cyber threat information sharing. But over time, this reluctance has waned, and more teams are able to proactively share cyber threat information. We are concerned that this progress will stall or reverse if CISA 2015 lapses later this year.

Given the urgency of this reauthorization, NRF’s priority request is for a clean extension of CISA 2015, consistent the language in Senate legislation introduced last month by Senators Gary Peters (D-MI) and Mike Rounds (R-SD).⁴ If there are opportunities to further amend the law as part of reauthorization, or in subsequent legislation, we would also support modest changes to the definitions of “cybersecurity threat,” “cyber threat indicator” and “defensive measure” that would clarify that

¹ NRF IT Security Council webpage. <https://nrf.com/membership/committees-and-councils/it-security-council>.

² NRF press release, January 9, 2023. <https://nrf.com/media-center/press-releases/retail-hospitality-isac-and-national-retail-federation-partner-enhance>.

³ RH-ISAC, 2024 Year in Review Report. https://rhisac.org/wp-content/uploads/2024_RH-ISACYearinReview.pdf.

⁴ S. 1337, Cybersecurity Information Sharing Extension Act. <https://www.congress.gov/bills/119th-congress/senate-bill/1337>.

CISA 2015 also applies to threat information related to cyber crime and on-line fraud, given the significant growth in threats in these domains over the past several years and the convergence of cyber and fraud threat actor tactics.

In support of the extension and reauthorization of CISA 2015, cybersecurity leaders at NRF and RH-ISAC member companies have provided examples of how cybersecurity information sharing has helped them prevent, disrupt, or respond to relevant cyber threats. The following quotes are relevant excerpts from these comments, anonymizing the company names by their general retail category:

CISO of National Grocery Chain

“We’ve found great success in information sharing both across industry and with our Government partners. We engage regularly with our Secret Service partners regarding intelligence we’ve gathered targeting retail skimming rings in several large markets across the industry. This work has DIRECTLY resulted in convictions of criminals attempting to place skimmers across various retailers in markets across the country.

“We were warned by an ISAC partner that a prolific threat group was spinning up a campaign against us. This advanced warning gave us time to prepare for the incoming attack.

“Recently, we were able to leverage the ISAC to anonymously share information regarding a potential breach of a third-party service provider. Our sharing allowed other ISAC members to make better decisions at a time when public information was scarce and fear, uncertainty, and doubt were circulating everywhere.”

CISO of National Sporting Goods Chain

“Within the first month of starting my new CISO role at a new company, I saw a post on the Retail & Hospitality ISAC portal from a cyber threat intel analyst that provided indicators of compromise (IOC) that contained over 600 known email addresses associated with the Democratic People’s Republic of Korea (DPRK, aka North Korea) threat actor known as FAMOUS CHOLLIMA. This group impersonates U.S.-based tech workers applying for remote jobs, and when hired, will syphon the salaries to the DPRK government, steal sensitive data, and cause harm (e.g., ransomware) when discovered or when they have achieved their objectives.

“I forwarded the link to my Security Operations Center (SOC) Manager, who also leads our Cyber Threat Intelligence (CTI) function, and asked if they had seen these IOCs yet, and if not, to please add them to our tooling for detection, blocking, and alerting. The following day we had 3 hits where the threat actor had applied for multiple jobs with the company, and one had already completed their interviews and was about to receive an offer. We were able to immediately stop the hiring process, which prevented an unknown but likely significant event, and we now have a process that continues to update these IOCs to prevent future risks with this and similar threats.”

CISO of Footwear Company

“RH-ISAC has been essential in helping protect our organization from modern cyber threats. There is no other place we get the quality of intelligence at the pace we need to action on it before adversaries take advantage of us. The recent major outages in the U.K. commercial sector attributed to Scattered Spider highlight what happens when threat actors use the same tactics against organizations that aren’t sharing intelligence. Using intelligence from RH-ISAC partners, we have been able to detect and prevent these exact types of attacks and keep our business running and customer data secure.

“Having access to verified community intelligence has allowed us to prevent malware infections, identify critical vulnerabilities, mitigate supply chain attacks, and respond to incidents more quickly than we otherwise would have been able to. This intelligence is a vital part of our information security practice.”

IT Leader at Book Retailer

“Our company uses the CISA portal to monitor cybersecurity and strengthen our threat awareness and incident response education—both of which are critical to our cybersecurity program. These capabilities help safeguard our systems, protect customer data and reduce operational risk. CISA 2015 was established to enable secure information sharing between the Government and private sector, helping organizations like ours stay ahead of emerging threats and coordinate timely responses. Eliminating this framework would reduce visibility into nationwide cyber risks and weaken our ability to respond quickly, increasing the likelihood of financial loss, service disruptions, and reputational damage.”

CISO of National General Merchandise Retailer

“We have numerous examples of successful cyber information sharing within retail to address and defend against threats.

“As one example, Atlas Lion is a cyber criminal group targeting retail, hospitality, and gift card organizations that has been active since at least 2021. They manipulate victims into providing log-in information through SMS phishing and phishing, and once inside a network, they quickly identify and exploit gift card systems to facilitate gift card fraud and theft. As part of their Threat Intelligence processes, one of the larger retail cybersecurity teams identified phishing and credential harvesting infrastructure proactively and notified companies of likely phishing attempts before they happened. Together with other mature retail cyber programs, they shared infrastructure tracking for this threat actor with the RH-ISAC, enabling other retailers to proactively defend their infrastructure before the cyber criminals send phishing campaigns.

“As a second example, Payroll Pirates is a cyber criminal group that uses phishing and fake log-in sites to steal victims’ log-in information for human resources and payroll systems. This group sends phishing emails and sets up malicious advertisements on search engines. Once a victim enters their credentials, Payroll Pirates uses that information to redirect salaries and payroll to bank accounts controlled by the cybercriminal group. One of the mature retail cybersecurity programs proactively monitored this group’s infrastructure and alerted multiple RH-ISAC organizations of infrastructure targeting these companies, helping them and their employees defend against fraud.”

CISO of Fashion Retailer

“As a member of the RH-ISAC, I can confidently state that our participation has been transformative for our security posture. Prior to joining the RH-ISAC in 2019, our company experienced a credit card breach. Based on the intelligence sharing and collaborative security resources we’ve accessed through RH-ISAC membership since then, I am 100 percent certain that had we been members beforehand, we would have prevented that breach entirely.

“Our membership has enabled us to advance our security program much more rapidly and in a targeted way compared to attempting to build our defenses independently. The threat intelligence and best practices shared through the RH-ISAC have directly contributed to protecting our customers’ data and our business operations.”

CISO of Footwear Manufacturer and Retailer

“Information sharing fosters a culture of trust and collaboration within the cybersecurity community—specifically sharing of Indicators of Compromise and having that level of information to help reduce impact of known attacks. There isn’t a need to ‘suffer’ as individual companies but rather pooling resources and knowledge, we can develop stronger defenses.”

CISO of a Regional Grocery Chain

“Due to the sharing provisions of CISA 2015, our organization—a retail grocery chain—has been well prepared to prevent, detect, and respond to threats that would otherwise be unknown to us. One such example is recent activity from North Korean nation-state threat actors targeting retailers in fake remote work schemes. Intelligence like this comes from a complex blend of Classified, unclassified, and private sources. CISA 2015 removes the friction of collecting and compiling these sources for CISA and facilitates their ability to distribute a threat intelligence product that is easily digestible and rapidly actionable by us. Our organization, and many others like us, lack the resources to achieve this outcome on our own. We urge you to reauthorize CISA 2015 to maintain this essential public-private cybersecurity partnership.”

CISO of Consumer Goods Product Manufacturer

“In previous roles in the Defense and Aerospace sectors, I experienced first-hand the value of threat intelligence sharing between companies that were essentially competitors and the direct impact on national defense. In my current role, and with a much smaller cybersecurity team, we rely heavily on the intelligence and peer sharing within the ISAC to protect the company and maintain operations. It is almost impossible for companies smaller than \$20 billion to effectively self-fund and manage their own threat intelligence teams/process/reporting.”

Cyber Leader for Truck Stop Company

“Information sharing between private companies, Government agencies, and law enforcement has been critical in furthering our cybersecurity posture. In several in-

stances, information provided to law enforcement, under the security of the Cybersecurity Information Sharing Act of 2015, has been fruitful in thwarting fraud, breaches, and other potentially harmful events.”

* * * * *

NRF is available to provide additional context on these comments with the committee upon request, including opportunities for direct dialog between retail cybersecurity leaders and committee Members and/or committee staff.

Thank you for focusing on this important issue. We encourage you to continue to work over the next 4 months to ensure that CISA 2015 is reauthorized and extended before the September 2025 expiration date.

LETTER FROM THE SOFTWARE & INFORMATION INDUSTRY ASSOCIATION (SIIA)

May 15, 2025.

The Honorable ANDREW GARBARINO,
Chair, Subcommittee on Cybersecurity and Infrastructure Protection, U.S. House of Representatives, Committee on Homeland Security, H2-176 Ford House Office Building, Washington, DC 20515-6480.

The Honorable ERIC SWALWELL,
Ranking Member, Subcommittee on Cybersecurity and Infrastructure Protection, U.S. House of Representatives, Committee on Homeland Security, H2-176 Ford House Office Building, Washington, DC 20515-6480.

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

DEAR CHAIR GARBARINO AND RANKING MEMBER SWALWELL: On behalf of the Software & Information Industry Association (SIIA), I write to urge the subcommittee to consider reauthorization of the Cybersecurity Information Sharing Act of 2015 (CISA 2015) during its May 15 hearing, “In Defense of Defensive Measures: Reauthorizing Cybersecurity Information Sharing Activities that Underpin U.S. National Cyber Defense.” We would appreciate your including our views in the record of the hearing.

SIIA is the principal trade association for those in the business of information, including its aggregation, dissemination, and productive use. Our members include roughly 380 companies reflecting the broad and diverse landscape of digital content providers and users in academic publishing, education technology, and financial information, along with creators of software and platforms used worldwide, and companies specializing in data analytics and information services.

SIIA supports reauthorizing CISA 2015, which is scheduled to expire on September 30, 2025.¹ Cybersecurity is a critical legislative priority, and one essential to the safety and security of a functioning democracy and a robust private sector. Information sharing between the Government and the private sector—as well as among private-sector entities—helps to harmonize meaningful cybersecurity safeguards with appropriate business compliance, and smooth implementation of joint cybersecurity efforts.

CISA 2015’s protections for private-sector cyber defenders, including its antitrust exemption, has led to increased public-private collaboration and cyber threat information sharing, and has also improved information sharing within the private sector. This foundation has enabled American businesses to address and respond to cybersecurity threats and has raised the level of cyber resilience in critical infrastructure sectors and beyond. By improving cybersecurity resilience, CISA 2015 has also helped to advance consumer privacy and mitigate the impact of breaches. This has also benefited consumer privacy interests, since information sharing among private-sector entities, especially around threat indicators, has been foundational for responsibly stewarding customer data in the face of these threats.

Permitting CISA 2015 to lapse would be detrimental to the United States’ cybersecurity posture at a time when cybersecurity risks are intensifying in intensity and scope. Recent incidents, including the Salt Typhoon attack and the BeyondTrust incident, underscore the importance of strengthening domestic cooperative efforts to counter these threats.

Reauthorizing CISA 2015 is an essential first step, but more should be done. We also encourage the subcommittee to examine ways to further incentivize information

¹The bipartisan Cybersecurity Information Sharing Extension Act, introduced in the Senate at S. 1337, provides for a clean extension. No such legislation has been introduced in the House this session.

sharing with the public sector, which has lagged private-to-private sharing in recent years.² This may include expanding CISA 2015's definitions of "cyber threat indicators," "defensive measures," "cybersecurity purpose," and "cybersecurity threat" to expand liability protections and further encourage sharing in a wider variety of contexts. Congress may also wish to consider extending liability protections to direct sharing with agencies beyond DHS and its automated indicator sharing system.

Although undoubtedly helpful to enforcers, CISA 2015's exception permitting Government use of shared information to inform regulation and enforcement may have unintentionally chilled public-private sharing. Last, greater information sharing from the Government to the private sector—especially in the context of incidents targeting critical infrastructure—would be a boon to private-sector cyber defenders. Congress can address this by providing statutory guidance and direction to the Cybersecurity and Infrastructure Security Agency.

Thank you for considering our views and for the subcommittee's attention to this important matter. SIIA looks forward to continuing to engage with the subcommittee as its work continues.

Sincerely,

PAUL N. LEKAS,
Senior Vice President, Global Public Policy Software & Information Industry
Association (SIIA).

Mr. GARBARINO. I know you all have said re-auth has to happen, so I'm not even going to start with that question. Everybody is saying that it has to happen. It sounds like clean re-auth, everybody thinks, is the best way to do it just to make sure it's done.

What would happen if this did not get reauthorized? You can all jump in. I want to hear from everybody. I feel like we need to get on the record why it's so important this has to be reauthorized. What would happen if it wasn't reauthorized?

Want to start, Mr. Miller?

Mr. MILLER. Yes. Thank you for the question, Chairman.

I mean, I think if it was not reauthorized there would be an immediate chilling effect, at least for some organizations on their willingness and ability to share, because those express authorizations in the bill and those attendant liability protections would go away.

I mean, this is not to say that information sharing itself would completely stop. Information sharing did occur before CISA 15, but a lot more of it is occurring after CISA 15.

In particular, automated sharing at scale, again, as I understand it as a lawyer, not as a cybersecurity operator, didn't really exist in nearly the same way that it does today, and the bill should be credited for that.

I personally think it's an open question given what exactly the fate of, for instance, the Automated Indicator Sharing program at CISA would be if the bill went away, because their authorization to run it would go away. It doesn't mean they would necessarily stop doing it. We don't have Homeland authorizations every year, as you know. But it would put things into question.

So I think this would undermine a lot of certainty across industry and Government and, thus, undermine the certainty that we have with the trusted sharing partnerships that have been built since CISA 15.

Mr. GARBARINO. Ms. Rinaldo.

²See, e.g., Megan L. Brown, et al., "CISA 2015 Reauthorization—Are Changes on the Horizon?" *Wiley Connect* (Mar. 3, 2025), <https://www.wileyconnect.com/CISA-2015-Reauthorization-Are-Changes-on-the-Horizon>; see also Sean Lyngaas, "Private Sector Isn't Sharing Data with DHS's Threat Portal," *CyberScoop* (Jun. 28, 2018), <https://cyberscoop.com/dhs-ais-cisa-isnt-used-jim-langevin/>.

Ms. RINALDO. You are taking the decision from the CISO to the general counsel's office, and that is going to slow everything.

Mr. GARBARINO. Us attorneys are the worst.

[Laughter.]

Ms. RINALDO. I wasn't going to say that.

Mr. GARBARINO. I can say it. It's OK.

Mr. Schimmeck.

Mr. SCHIMMECK. Yes. Reiterate that. Basically, firms would immediately hesitate. There would be uncertainty in what would be shared. Things would slow down.

The other thing is, you would very much be locking out the small and medium-sized businesses and companies and vendors. This would be a big-firm-only play, because we would be the only ones willing to try it, willing to evaluate it.

Then you'd also, I think, you'd start to see what we saw previously, which is every firm building bilateral gratis with the U.S. Government instead of going through this framework.

Mr. GARBARINO. It's a very key point. Thank you for making that.

Ms. Kuehn.

Ms. KUEHN. Just to reaffirm everything that everyone else has said. But you're right, there was information sharing before 2015. We did have it. But it was picking up the phone and kind-of chatting behind closed doors.

That's going to hinder from both a proactive and a reactive cyber defense strategy if we don't have those safe harbors. To my fellow committee Member's point, it puts it in the hands of the lawyers.

The reality is, is that with AI coming in, with what we're seeing with the rapid spread of threats, we don't have time for it to go to the lawyers at this point. We have to be able to share information quickly.

Mr. GARBARINO. The slower we are, the more exposed we are.

Ms. KUEHN. Hundred percent.

Mr. GARBARINO. That information sharing is very important.

Mr. Schimmeck, I want to ask you both—you worked at—you worked with SIFMA for a while. I wanted to know if you could specifically share some information or some anecdotal information about how your companies or other companies you've worked with have shared information under this law.

Mr. SCHIMMECK. Sure. So what we'll use this for typically is we will provide the information via AIS. So we have that path of sharing information with DHS when we need to. We also use other mechanisms, phone calls, email.

DHS provides multiple ways for us to submit information. So it provides maximum flexibility for firms to go do that. But then it also enables us to go peer-to-peer.

There is probably not a day that goes by that I'm not talking to a peer CISO out there on some issue that's going on, either emerging or on an active threat that we're dealing with.

This just provides us that flexibility to make sure that anything we're sharing we're protected, we're doing it under the best intentions. So it really allows us to, as we say in financial services, this is a noncompetitive topic for us.

We want to make sure that the entire system is protected, because if there's an attack against one bank, it calls into question the entire system. Financial services, more than anything else, is built on trust.

Mr. GARBARINO. I appreciate that. My time has expired.

We're going to start a second round of questioning, and I'm now going to recognize for a second round of questioning the gentleman from Florida, Mr. Gimenez, 5 minutes.

Mr. GIMENEZ. I'm trying to figure out where I'm going to go.

Mr. SWALWELL. Uh-oh. Watch out.

Mr. GIMENEZ. I'm not so sure I share the Ranking Member's problems with a 19-year-old. In "Ender's Game" the guy was like 12 years old, and he defeated an entire alien race. So maybe the Ukrainians are onto something. So there, that's where I was going.

So my question is, and anybody can answer this, are we as a country spending enough?

Because I do believe that at the end the solution is not going to be—yes, we need a number of people—but with artificial intelligence I can see the day that you're going to be both on the offense and defensive side.

You will have literally millions of attacks per minute being launched and counter-launched and defended against. Then the systems learning from each other and probing and defending, probing, probing, and then basically, almost at the speed of light.

No, we can't have—there's no way we can ever fund that many people.

So are we investing enough as a country in artificial intelligence in order to protect us from what we know is going to be the threat, which is really artificial intelligence-launched cyber attacks on our country and our infrastructure and everything? Are we investing enough in artificial intelligence that will counter that?

Ms. KUEHN. I think, first of all, from the investment question, my other role is I'm head of global advocacy for—cyber advocacy for a privately-held company. From an AI perspective, we've invested over a half-billion dollars and a billion in labs just to look at all the different technologies that are coming in right now, both from a proactive and reactive AI perspective.

What I would say is, I think that we do need to invest more, but I think one of the critical areas is in public-private partnership, is getting closer with the organizations like NVIDIA and others that are on the front lines of creating AI, and also then the companies that are defending AI, which many of them are early stage organizations.

So the more we can strengthen the public-private partnership from Government and industry to approach how we look at AI, how we look at, like I said, malicious, malfunction, mistake going in the future, it's going to have benefit across all areas of industry.

Mr. GIMENEZ. Are we unified in an approach, or is everybody just doing their own thing as individual companies? Is CISA doing its own thing? Is DOD doing its own thing? Is Oracle doing its own thing? Or would it be beneficial to maybe have some other different kind of legislation that kind-of starts to focus it all? Because it's a mutual defense system that we really have to build here, not

just, gee, OK, DOD is protected, but, gee, it's too bad that our critical infrastructure wasn't.

So are we there? Where are we with that? Is everybody just developing their own, or do we have some kind of a strategy to kind of focus in on that to develop—instead of the golden shield, this will be the cyber shield, which is it's going to be artificial intelligence. That's the way it's going to be. Where are we on that?

Ms. RINALDO. So I would say that different agencies are focusing on it for their specific needs. There is not one holistic approach to it but more of a buckshot, if you will. I think there is more of a holistic approach to how we manage AI moving forward, but I think there's a lot of exciting applications.

In my day job I run a telecom trade association, and we're really focusing on 6G and how AI is going to shape sensing communications moving forward, so you're able to detect anomalies in a network, whether it be security, whether it be weather-related. You could tell a certain portion of the network is down. That's all going to be done by AI.

So there are a lot of great aspects of it, and I think it's really important for the different agencies to kind-of focus and really hone in on their particular function.

Mr. GIMENEZ. Do you think our adversaries are somewhat scattered like we are, or do you think they're more focused on their goals?

Ms. RINALDO. I think China remains an existential threat to us on these issues.

Mr. GIMENEZ. Are they focused, or do they have a scattershot kind of approach to their development of AI?

Ms. RINALDO. So what we've seen, and from my work at the House Intel Committee on Huawei, is that China is especially focused on certain individual companies as opposed to we support sectors. So they will want to see one individual company succeed globally while we push a sector. So in that instance, they are honed in.

Mr. GIMENEZ. Should we match that?

Ms. RINALDO. No.

Mr. GIMENEZ. No? OK.

My time is up. I wish I could go further, but I'm done. Thank you.

Ms. RINALDO. True innovation happens when you have multiple different companies competing.

Mr. GARBARINO. The gentleman yields back.

With the consent of the Ranking Member, I now recognize the gentleman from Tennessee, Mr. Ogles, for 5 minutes.

Mr. OGLES. Thank you again, Mr. Chairman.

I also sit on the Financial Services Committee, and, Mr. Schimmeck, I'd love to hear from you as one of the things that concerns me is the sophistication of AI and how we're seeing that play out in the financial sector and just the risks that are involved there.

So, what are the next phases? Does this go far enough? Again, if we're going to come back and do a clean-up or revision of this at some later date, what needs to be included?

Mr. SCHIMMECK. Yes. So AI, obviously, it's an area of investment for financial services both on the business side but also on the security side as well.

Very much still early days in regards to how we're going to embed that within our operations, but pretty much every firm has got a strategy around this and are making significant investments, to Mr. Gimenez's point.

In regards to how this is going to affect CISA, I think we're not really sure how this is going to play out and how we're going to want to share information, whether it's going to be in agentic AI within a financial services firm sharing with another agentic AI within DHS or within another agency. So I think that's something we'll have to work at.

I think it goes to maybe some of the improvements we can have on the AIS systems. The AIS system was probably designed 10 years ago. It's operational. It accomplishes the mission. But it's definitely something that could be modernized both with AI or even other opportunities to just improve the level of detail and to just make it more consumable for us as both a submitter and a consumer of that information.

Mr. OGLES. Ms. Kuehn, you mentioned the typhoon attacks. As a former county executive one of the things that concerns me across our landscape isn't the larger companies. Obviously, they're a target and there's risk associated with it, but it's that critical infrastructure in rural Tennessee that supports hundreds of thousands if not millions of people across this network.

What's the end game there? How do we help these smaller communities that, quite frankly—so I'll give you an example. In metro Nashville or Memphis or even the suburb, Williamson County, which is a very affluent county, they have the resources to have an IT department.

If you go a little further south, east, or west, the IT guy is probably also the H.R. guy, and they're not equipped to defend a county—the water system, the electrical grid—from these types of attacks. So what do we do going forward?

Ms. KUEHN. I think part of it is, again, and I sound like a broken record, it's public-private partnership.

So the 2 attacks you just mentioned, so I'll use Salt and Flax, both of them are exploiting critical vulnerability exploits that were back from, like, 2018, 2021 on known, basically antiquated network and technology gear.

So it's, again, educating smaller and mid-sized businesses. To your point, I saw a statistic recently that 80 percent of critical national infrastructure is sitting in small and medium business.

So working with those organizations to create modernization plans, working with organizations that have the CVEs to help with creating, in essence, modernization, technology upgrade, helping small to medium businesses and critical national infrastructure organizations upgrade to technology that is not vulnerable anymore and putting action plans together to do so.

The typhoons are—they're not going to care whether you're a large or a small organization. They're going to care about the disruption that it causes to critical national infrastructure. So it's going to take a shoulder-to-shoulder proactive measure between

public and private to ensure that we don't have disruptive behavior from them.

Mr. OGLES. Not that I want to be one of the Members of Congress that authorizes Skynet, but it's almost like we need a cyber shield that better equips our private and public partners in this space. But, again, proceed with caution.

I yield back.

Mr. GARBARINO. The gentleman yields back.

I now recognize the Ranking Member, Mr. Swalwell from California, for a second 5 minutes of questions.

Mr. SWALWELL. Great. Thank you, Chair.

Ms. Kuehn, how has the loss of CIPAC impacted information sharing?

Ms. KUEHN. I think when you look at the loss of CIPAC there's kind-of 2 things, whether you're talking about CIPAC or any of the councils, so from the advisory council perspective and then the safety review board. The work that it does is the education that we need.

So from a CIPAC perspective, having that collaboration of experts both from public and private and being able to look and give advice on things like we've talked about, the typhoons, about agentic AI, about even quants that are going on, where should we be pointing our arrows. That's incredibly important for us to rely on.

If we talk about the safety board getting the revisions and understanding what happened on critical attacks, like the work that was being done on Salt Typhoon, there was the Microsoft vulnerabilities, there were others, it's a question of those type of information sharing allows us to go a step further than JCDC and really disseminate critical information about where we want to focus our attentions from public and private and then also how we better protect ourselves.

Mr. SWALWELL. Are you aware as to whether DHS has provided a time line for when a CIPAC replacement will be established or a process for how the private sector can provide feedback?

Ms. KUEHN. I am not aware at this point.

Mr. SWALWELL. How would you structure a new CIPAC?

Ms. KUEHN. From a CIPAC perspective I think that you have to look at—there's practitioners and operators in cybersecurity and in AI. As we think about it, we need a blend of Government, former Government, the practitioner side, like the CISOs and the risk executives sitting here today, and then also operators, who are the business risk side, from boards and CEOs and understanding the cyber perspective from the business side.

Because we're seeing we're in the middle of a digital revolution. Cyber touches every area. Traditional technology, everything we do has technology in it, and there's a cyber component.

So as we look at the new CIPAC, we have to take into consideration that we're no longer just looking from an adversarial perspective, it's a business, operational, resiliency perspective, and we need to adjust accordingly.

Mr. SWALWELL. Great. Yield back.

Mr. GARBARINO. The gentleman yields back.

I now recognize myself for my second 5 minutes of questions.

When the original CISA 2015 law was negotiated significant privacy concerns were raised. As far as I'm aware, these concerns did not come to fruition.

Ms. Rinaldo, you were there. Will you please walk us through the initial debates and how they were resolved dealing with privacy?

Ms. RINALDO. Absolutely.

So during the 4 years we had 3 different bills that were introduced, and from the first bill, which was a couple of pages, to the one that was signed into law, which was much, much bigger, we took a lot of the feedback from privacy groups and industry—John was instrumental in a lot of this work that we did—and we made changes.

The information has to be anonymized. We want to make sure that what is actually being shared is the zeros and ones of it.

I know that the inspector general has done a report recently and has determined that no privacy issues have arisen in the past 10 years. So the language and all the protections that we put in have been working.

Mr. GARBARINO. That's great, because I'll tell you, other than the name, privacy concerns, it might be the biggest obstacle to getting this reauthorized. So the fact that you have—that report has zero reports of privacy breaches is great.

Mr. Miller, you were also instrumental, as we all just heard Ms. Rinaldo say. Have you heard of any privacy-related concerns over the last 10 years the law has been in effect?

Mr. MILLER. No, and I think that's pretty compelling evidence that the bill itself and the structure and the protections that were put in place to protect privacy and civil liberties worked.

If I could add one other protection that I think was very important to what Diane said. Actually having DHS serve as the central hub, what we kind-of called the civilian interface at the time, was very important.

If you think about what else was going on during this time, there was a lot of suspicion about sharing, and in particular about surveillance agencies, in light of the Snowden disclosures, for instance.

So I think that the protections that Diane mentioned, requiring the stripping out of PII, was very important. But also sharing through DHS and then having DHS share across the Federal Government was a good innovation, I think, of the time as well.

Mr. GARBARINO. Mr. Schimmeck, anything to add there regarding privacy?

Mr. SCHIMMECK. Just the only thing I would add to it is, No. 1, as I made in my statement, we have not had anything realized in regards to any disclosures.

Also, from a financial services industry standpoint, we take privacy extremely seriously. It's something that's core to how our business operates.

So having those protections in there and really to focus on it in the act, in the bill, was really important.

Mr. GARBARINO. Ms. Kuehn.

Ms. KUEHN. I would agree. I think that they've summed it up. There really have not been any, to my knowledge, concerns from a privacy perspective. I think that that's one of the reasons that a clean authorization of it from a renewal standpoint is just crit-

ical. We can change what we need to change later, but what's working right now from a fundamental perspective is working.

Mr. GARBARINO. That was my follow-up question. You said clean re-auth, which means you would all agree that there is no need to change the language when it comes to privacy, correct?

Ms. KUEHN. Yes.

Mr. SCHIMMECK. Yes.

Mr. MILLER. Yes.

Mr. GARBARINO. They all said yes, for the record.

Thank you very much for that.

I do want to get to one more, because we're talking about information sharing with the Government, private to Government.

But can you all talk about some reflections on how this legislation changed information sharing amongst private-to-private entities and how it fostered that information sharing? Feel free to jump in, whoever wants.

Mr. MILLER. I mean, I'll jump in.

Talking to, for instance, the executive director of the IT-ISAC recently, it does seem like—and talking about some of the types of things that CISA 15 really has allowed the private sector to do, I mean, I think there are criticisms of whether the private-Government sharing can be better. I mean, we've heard some of those already today.

But the private-private, private-to-private sharing, is a really critical and maybe sometimes overlooked aspect of what CISA 15 really enabled.

Again, if you look at the ISACs, again, some of the ISACs have less than a hundred people, some of them have thousands of companies involved, you look at the National Council of ISACs, the State and local, Tribal, and territorial ISAC, all of these ISACs are—allow—it's kind-of a concept of the few protecting the many.

They're very important in particular for those small and medium-sized businesses who can perhaps participate through ISACs because they don't have million-dollar budgets to spend on cybersecurity.

So I think there's really been a pretty dramatic increase in private-to-private sharing that has been enabled because of CISA 15.

Mr. GARBARINO. Wonderful.

All right. Well, I'm now out of time.

I really want to thank you all for being here. I think you can tell by the fact that we all stayed for our second round and we have such a big crowd in the back that this is a very important hearing and people understand its importance.

Again, I said it was wonderful that the Secretary mentioned it yesterday, that she wants to see reauthorization. That's the second time I've heard her publicly say that, which is great.

So I want to thank you all for your valuable testimony and for the Members for their questions.

Members of the committee may have some additional questions for you all, and we would ask you to respond to these in writing.

Pursuant to committee rule VII(E), the hearing record will be held open for 7 days.

Without objection, the committee stands adjourned.

[Whereupon, at 3:22 p.m., the subcommittee was adjourned.]

APPENDIX

QUESTIONS FROM CHAIRMAN ANDREW R. GARBARINO FOR JOHN MILLER

Question 1. Do barriers still exist to cybersecurity information sharing, such as private-sector companies' reluctance to share with law enforcement or quality concerns regarding redundant cyber threat indicators and defensive measures? What actions have been taken, if any, to overcome these barriers?

Answer. While certain barriers to information sharing may persist, CISA 15 removed or lowered the vast majority of barriers to information sharing by providing clear liability protections to companies for voluntarily sharing or receiving cyber threat indicators (CTIs) or defensive measures (DMs), for authorized monitoring activities, by exempting these sharing activities from disclosure under FOIA and from antitrust laws, and providing limited protections against regulatory use. A lapse of CISA 15 would immediately reintroduce those barriers.

It is important to note that while the intention behind CISA 15 was to incentivize voluntary sharing by removing these above-listed barriers, some private-sector entities have remained reluctant to share with DHS/CISA or other Government agencies due to lingering concerns over regulatory exposure, or other issues such as reputational risk or uncertainty around the onward use or dissemination of shared data.

Additionally, I believe it would be prudent to review and update the list of cyber threat indicators (CTIs) in CISA 2015, not for redundancy but for completeness. Adversaries are constantly developing new tactics, techniques, and procedures to advance their nefarious objectives. Defenders need to have the ability to share updated CTIs on the entire dynamic threat landscape. The CTI definition is framed to encompass much of the threat landscape without risking redundancy. Accordingly, any update to the list of CTIs should focus on adding additional CTIs to reflect developments in the threat landscape. For example, CTIs related to supply chain attacks or AI-enabled TTPs may be appropriate to include. Notably, DHS/CISA has already worked to improve the technical utility of shared data and to facilitate anonymization and contextual enrichment of threat indicators to enhance their value. Evolving the list of CTIs alongside continued stakeholder engagement, transparency, and advancements in automated sharing standards may help to mitigate persistent concerns.

Question 2. What can the Cybersecurity and Infrastructure Security Agency (CISA) do to increase participation in the Automated Indicator Sharing (AIS) program?

Answer. One way for DHS/CISA to increase participation in AIS would be to better emphasize the value proposition behind bi-directional information sharing, particularly from Government to industry. Currently, much information sharing happens industry-to-industry, industry-to-Government, or Government-to-Government. Increasing Government-to-industry sharing of information could incentivize more private-sector entities to participate in AIS. Additionally, DHS/CISA can also broaden industry engagement by continuing efforts to improve the relevance, accuracy, and timeliness of shared indicators and provide metrics demonstrating operational impact and actionable intelligence to further improve the value proposition for reluctant companies. Moreover, enhancing integration with threat intelligence platforms used by private-sector entities and expanding training and onboarding support for small and mid-sized enterprises can make participation more accessible.

While incentivizing greater participation is a worthwhile goal, it is also worth noting that the raw numbers of entities participating in AIS do not tell the whole story. Many companies including SMBs participate indirectly in and gain the benefits of the AIS program by virtue of their participation in the various sector ISACs representing critical infrastructure as well as other Information Sharing and Analysis Organizations (ISAOs).

Question 3. Do you believe that the Cybersecurity Information Sharing Act of 2015 (CISA 2015), if reauthorized, should still exclude protections from sharing with the Department of Defense (DoD), including the National Security Agency (NSA)? Why or why not?

Answer. The original decision to limit certain liability protections for sharing directly with the Department of Defense and NSA reflected a conscious effort to preserve public trust by emphasizing civilian-led cybersecurity collaboration. Removing those protections would resurface the same privacy concerns from a decade ago that took years to resolve. The intentional decision to establish DHS/CISA as a civilian intermediary was intended to mitigate these concerns, and based on available evidence—including no documented privacy incidents or instances of information leakage that I am aware of—the current structure establishing DHS/CISA as the central information sharing hub for the Federal Government has proven a success. There is no compelling reason to reassign these intermediary responsibilities to law enforcement or national security entities, and any effort to do so would raise the same privacy concerns from a decade ago. Resurfacing those concerns now would jeopardize the timely reauthorization of CISA 15.

Question 4. How important is the antitrust exemption in CISA 2015? Please explain and provide any examples that would help illustrate your point.

Answer. The antitrust exemption in CISA 2015 is essential to fostering collaborative defense across sectors. It reassures companies that sharing cyber threat indicators and defensive measures with competitors in good faith will not expose them to antitrust liability. For example, in the financial and energy sectors, where competitors often face similar threats, the exemption has enabled proactive collaboration through the information sharing Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs). Without it, firms may hesitate to engage in joint threat analysis or response coordination. This legal assurance has enabled trusted sharing ecosystems that enhance collective resilience.

Question 5. How does CISA 2015 allow for small and rural critical infrastructure sector organizations to effectively share cyber threat information with Government entities?

Answer. CISA 2015 facilitates participation by small and rural critical infrastructure organizations primarily through sectoral or (multi-)regional Information Sharing and Analysis Centers (ISACs). These intermediaries allow smaller entities to receive relevant threat information and share indicators through a trusted network. Moreover, DHS/CISA's support for automated tools and templates, as well as its outreach to under-resourced entities, helps reduce technical and operational barriers to participation. Liability protections further assure these organizations that sharing information will not result in undue risk.

Question 6. Do liability protections under the existing statute sufficiently address threat actors' new and emerging tactics, techniques, and procedures (TTPs)? If they do not, please provide some recommendations to ensure the law upholds its relevancy as the threat landscape evolves.

Answer. The existing liability protections have proven effective in encouraging information sharing across a range of threats. However, as TTPs evolve, including those involving AI-enabled exploits, supply chain compromises, and manipulation of operational technology systems, there may be ambiguity about whether certain cyber threat indicators or defensive measures are covered. To maintain the law's relevance, Congress should consider modernizing the definitions within the statute to explicitly account for emerging threats, including indicators related to ransomware campaigns, AI anomalies, and software component tampering. Clarifying these elements would reduce hesitation and further incentivize more robust sharing.

Question 7. What changes, if any, can Congress make to CISA 2015 to ensure there are no delays or roadblocks to information sharing, especially when dealing with a campaign from an advanced persistent threat (APT) actor?

Answer. It is imperative that Congress reauthorize the existing law before it lapses in September. Improvements should not come at the expense of the existing cyber information sharing activities that rely on CISA 2015 authorities. Any lapse to CISA 2015's liability protections could have real and immediate negative consequences that put all American organizations at greater risk.

That said, Congress can take several actions to minimize delays in high-stakes scenarios involving APT actors. First, cross-checking, and updating as necessary, the definitions of covered threat indicators and defensive measures to make certain they sufficiently capture advanced and emerging attack vectors related to APTs would reduce ambiguity and make sure actionable information necessary to counter them is shared. Second, reinforcing the role of the Joint Cyber Defense Collaborative (JCDC) as a central hub for coordinated operational planning can streamline real-time shar-

ing and response. Finally, codifying governance mechanisms like charter requirements, stakeholder roles, and reporting standards would strengthen trust and agility. Ensuring that liability protections clearly extend to fast-moving collaborative, operational responses is vital to enabling timely and decisive action during APT campaigns.

QUESTIONS FROM CHAIRMAN ANDREW R. GARBARINO FOR DIANE RINALDO

Question 1. Do barriers still exist to cybersecurity information sharing, such as private-sector companies' reluctance to share with law enforcement or quality concerns regarding redundant cyber threat indicators and defensive measures? What actions have been taken, if any, to overcome these barriers?

Answer. Yes, barriers absolutely remain. Many companies still hesitate to share because they're uncertain about liability protections or they simply lack the resources to participate. Others worry about whether the information they share will be useful, or if they'll get meaningful intelligence back (is the juice worth the squeeze scenario). We've certainly made progress: DHS's Automated Indicator Sharing program, the growth of ISACs, and more streamlined declassification of intelligence have all helped. But the flow is still too often one-way, and the quality and timeliness of information aren't always what industry needs in the middle of an attack. What's required now is to strengthen reciprocity, provide clearer safe harbors, and make participation easier for small and mid-sized companies.

Question 2. What can the Cybersecurity and Infrastructure Security Agency (CISA) do to increase participation in the Automated Indicator Sharing (AIS) program?

Answer. CISA needs to make participation valuable in real time. When a company shares an indicator, they should get timely, actionable intelligence back but within hours. The data also needs to be delivered in formats that companies can use immediately in their security tools. Reducing noise, providing context, and integrating with the platforms companies already rely on would go a long way. Finally, CISA can make participation more attractive by offering incentives such as priority access to threat briefings or incident support for organizations that actively contribute.

Question 3. Is there any ambiguity in CISA 2015's definitions, such as for cyber threat indicators or defensive measures, that Congress should revisit? If so, please explain.

Answer. Yes, there are ambiguities. The term "cyber threat indicator" was written before today's realities like AI-driven attacks, identity-based threats, and large-scale abuse of cloud services. The definition should be broadened to clearly include behavioral analytics, AI detection artifacts, and identity signals like multifactor bypasses. Similarly, "defensive measures" should reflect the automated blocking and orchestration tools that are commonplace today. Clarifying these terms would remove uncertainty and give companies more confidence that their actions fall under the law's protections.

Question 4. Do you believe that CISA 2015, if reauthorized, should still exclude protections from sharing with the Department of Defense (DoD), including the National Security Agency (NSA)? Why or why not?

Answer. There needs to be a more balanced approach. The original exclusion was meant to build trust and avoid concerns about surveillance. The last 10 years have proven that the U.S. Government is able to adhere to the strict minimization standards and protect personally identifiable information (PII). The threat has certainly advanced beyond what we envisioned 10 years ago. When an advanced persistent threat is in play especially from a nation-state actor, it makes sense for DoD or NSA to be part of the picture. My view is that Congress should allow carefully-scoped sharing with these agencies, with guardrails: CISA should remain the front door, minimization and transparency should apply, and use of the data must be limited strictly to cybersecurity defense. That way, we preserve trust while ensuring we can act at the speed of the threat.

Question 5. Do liability protections under the existing statute sufficiently address threat actors' new and emerging tactics, techniques, and procedures (TTPs)? If they do not, please provide some recommendations to ensure the law upholds its relevancy as the threat landscape evolves.

Answer. Protections need to be enhanced to encourage greater participation. The statute was written before AI, before the explosion of ransomware-as-a-service, before the identity and supply chain attacks we see now. Companies need assurance that if they act in good faith, whether by sharing new types of indicators, deploying automated defensive measures, or collaborating internationally, they are protected. Congress should expand liability protections to explicitly cover these evolving tactics

and tools. A good rule of thumb is: if a company follows best practices, uses recognized sharing standards, and acts to defend its network, they should be protected.

Question 6. How does CISA 2015 allow for small and rural critical infrastructure sector organizations to effectively share cyber threat information with Government entities?

Answer. In theory, the law applies equally to everyone. In practice, smaller organizations often don't have the staff, budget, or legal support to participate. Some benefit through ISACs, fusion centers, or State-based programs, but it's patchy. To make this law truly work for them, Congress should consider subsidizing membership in ISACs, and simplified legal frameworks so smaller players can participate without fear or cost barriers.

Question 7. What changes, if any, can Congress make to CISA 2015 to ensure there are no delays or roadblocks to information sharing, especially when dealing with a campaign from an advanced persistent threat (APT) actor?

Answer. Speed is everything in an advanced persistent threat scenario. Congress can help by requiring reciprocity: when companies provide indicators, CISA must push back sanitized, actionable intelligence quickly. Clear statutory time lines would help. Congress should also support "default to declassify" processes so that critical information isn't held up unnecessarily by classification. And we should empower joint operations cells with the relevant agencies such as CISA, FBI, DoD, NSA so the Government can act as one team and provide a single, timely stream of information to the private sector.

QUESTIONS FROM CHAIRMAN ANDREW R. GARBARINO FOR KARL SCHIMMECK

Question 1. Do barriers still exist to cybersecurity information sharing, such as private-sector companies' reluctance to share with law enforcement or quality concerns regarding redundant cyber threat indicators and defensive measures? What actions have been taken, if any, to overcome these barriers?

Answer. Large financial institutions do not have significant barriers to cybersecurity information sharing but there may be reluctance among smaller companies that are not aware of the protections that are provided under CISA 2015. Although there has been outreach to such firms at various points a more concerted effort to raise awareness about the necessity of information sharing and the protections provided would be helpful. The financial services industry views the Federal Government (including CISA and Federal financial regulators) and law enforcement as valuable partners in defending against cybersecurity threats, but having information shared from companies of all sizes will further improve that value of the information shared. CISA 2015 provides significant protections against regulatory and antitrust enforcement actions and antitrust which are critical.

Over the past few years U.S. Treasury has removed many barriers around sending Classified threat indicators (e.g., IOCs) to the private sector. Treasury now declassifies threat indicators more quickly to provide the sector with leading indicators they can use to prevent cyber attacks. And during crises, the public/private sector incident management mechanisms have improved to allow rapid sharing of ground truth during attacks in progress.

Question 2. What can the Cybersecurity and Infrastructure Security Agency (CISA) do to increase participation in the Automated Indicator Sharing (AIS) program?

Answer. CISA should make an affirmative effort to educate companies about the benefits of sharing through the AIS program. The program should also demonstrate its own value by using current technology as well as providing timely and accurate threat information shared in the system.

CISA should explore alternative approaches to its automated threat intelligence and information-sharing capabilities, including implementing a long-term vision for information sharing, building on existing capabilities, and aligning with reporting programs at other Government agencies including financial regulators.

Question 3. How important is the antitrust exemption in CISA 2015? Please explain and provide any examples that would help illustrate your point.

Answer. The antitrust exemption is critical to information sharing between private entities as well as with the Government as that information is also shared indirectly with private companies. Antitrust compliance is time-consuming and costly. The exemption limits the necessity of lengthy internal or external reviews of information to be shared for antitrust compliance thus decreasing response times for sharing critical information with the Government or with other private entities. For example, if a private company has information about a cyber threat stemming from its use of a vendor, that company may share that information with the Government or other private entities who may also use that vendor including what services the

company receives from the vendor which may be related to the cyber threat without risk of that behavior being deemed anti-competitive under U.S. law.

Question 4. Is there any ambiguity in CISA 2015's definitions, such as for cyber threat indicators or defensive measures, that Congress should revisit?

Answer. The definitions are generally well-understood and do not require additional changes to meet the needs of the financial services industry. For the most part, these definitions have been harmonized across the public and private sector to provide for better communication during cyber events. As a result, changing these definitions may cause additional challenges since they are already generally accepted.

Question 5. What changes, if any, can Congress make to CISA 2015 to ensure there are no delays or roadblocks to information sharing, especially when dealing with a campaign from an advanced persistent threat (APT) actor?

Answer. CISA 2015 already contains the necessary framework for information cyber threat information sharing between public and private entities. The Department of Homeland Security should have the necessary financial resources and technology necessary to both share information and provide detailed instructions on defensive strategies wherever possible.

Question 6. Do you believe that CISA 2015, if reauthorized, should still exclude protections from sharing with the Department of Defense (DoD), including the National Security Agency (NSA)? Why or why not?

Answer. CISA 2015 if reauthorized should include the broadest protections possible for sharing with any Federal Government entity which may play a part in the protection of our critical infrastructure. There should be the same protections regardless of which agency the entity shares cyber threat information with.

Question 7. The existing statute states that the Federal Government must share "timely" information. Do you believe that the Federal Government is succeeding in this role, and does this extend to both Classified and unclassified information?

Answer. Response times for information sharing from the Federal Government to the private sector are critical for the system to work. Stale information is not valuable in defending against an impending cyber threat, so it is important that this information be shared as soon as possible while still ensuring the necessary privacy and other confidential information is not shared if it's not necessary to the prevention efforts.

QUESTIONS FROM CHAIRMAN ANDREW R. GARBARINO FOR KATHERINE KUEHN

Question 1. Do barriers still exist to cybersecurity information sharing, such as private-sector companies' reluctance to share with law enforcement or quality concerns regarding redundant cyber threat indicators and defensive measures? What actions have been taken, if any, to overcome these barriers?

Yes, barriers to cybersecurity information sharing persist, despite years of focus on public-private partnerships, and the private sector remains hesitant to share cyber threat information with the Federal Government. In addition, there are concerns that CISA doesn't protect its sensitive equities. According to information originating from the Cybersecurity and Infrastructure Security Agency (CISA), concerns have been raised regarding accuracy and timeliness. For example, Yara rules shared on threats have frequently contained inaccurate or poorly-crafted alerts.

Major barriers include:

- *Lack of Trust.*—Organizations may be reluctant to share information due to concerns about data misuse or leaks, especially when sharing with competitors or Government entities. Building trust through transparent policies and fostering a collaborative culture is crucial.
- *Legal and Regulatory Challenges.*—Different jurisdictions have varied data-sharing laws, and regulations like GDPR can pose challenges for cross-border sharing. Navigating these legal frameworks and ensuring compliance can be complex, potentially hindering collaboration. Concerns about potential liability if shared information is inaccurate or misleading can also deter organizations from sharing.
- *Organizational Barriers.*—Issues such as resource constraints, a lack of technical expertise, and internal silos within organizations can impede effective information sharing.
- *Technical Challenges.*—Difficulties in integrating systems and establishing a common language for sharing can hinder automated information exchange. The amount of data can also overwhelm resources, making it difficult to deliver information to the right place at the right time.

- *Concerns about Disclosure.*—Companies worry about revealing sensitive company information, potential non-compliance with regulations, customer privacy violations, and reputational damage from sharing details of cyber attacks.

Actions taken to overcome these barriers:

Efforts have been made to address these concerns, including updating the Automated Indicator Sharing (AIS) platform and launching programs such as the Joint Cyber Defense Collaborative (JCDC). However, these steps have not meaningfully changed the landscape. The private sector still overwhelmingly relies on peer-to-peer exchanges, commercial threat intelligence providers, and industry-specific Information Sharing and Analysis Centers (ISACs), all of which are connected to the foundation laid by CISA 2015, which provides the liability protections and other legal assurances necessary for these programs to exist. Even with these assurances, trust issues and inefficiencies continue to dominate the information-sharing environment and will persist without the safeguards established in CISA 2015. A clean renewal is necessary to continue the programs that are working, and as we look toward the future, additional actions could include:

- Additional Legislation and Policy
- More Collaborative Government/Industry Initiatives
- Incorporation of Technological Advancements
- Focus on Trust and Communication.

Following the clean renewal of the Cybersecurity Information Sharing Act of 2015 (CISA 2015), we can examine other ways of sharing information that should be considered for dissemination and building more trust between public-private partnerships. One suggestion would be to continue the Office of the National Cyber Director (ONCD) roundtable efforts or expand JCDC or AIS, which would enable coordinated cross-functional cyber information dissemination points that could act in a central and controlled way with the ability to engage with Industry in a functional and approved manner.

A potential framework for this type of partnership could be replicated by either the ONCD or the JCDC/AIS, which could be derived from the incomplete one currently found on the U.S. Cyber Command website. <https://www.cybercom.mil/Partnerships-and-Outreach/Private-Sector-Partnerships/>

PRIVATE-SECTOR PARTNERSHIPS THE MISSION

The mission of our unclassified private-sector partnership program and forum, otherwise known as UNDER ADVISEMENT, is to engage with industry partners, agilely sharing critical information that enables both U.S. Cyber Command missions and private-sector partner priorities.

Who We Are

UNDER ADVISEMENT is U.S. Cyber Command's front door regarding information sharing to and from private-sector partners. The immediate cyber crises information shared supports U.S. Cyber Command's entire mission set while providing vital information to our partners so they can further protect and defend their networks from adversary threats.

How We Do It

U.S. Cyber Command enters into two-way information-sharing agreements with partners from across all aspects of the public and private sectors. These agreements are designed to enhance and expand trust and dialog between our partners and CYBERCOM. Once an agreement is in place, members of the UNDER ADVISEMENT program work with our partners to facilitate sharing of critical information across multiple agreed outlets.

Question 2. What can the Cybersecurity and Infrastructure Security Agency (CISA) do to increase participation in the Automated Indicator Sharing (AIS) program?

Answer. The Cybersecurity and Infrastructure Security Agency's Automated Indicator Sharing (AIS) program aims to facilitate the real-time sharing of cyber threat information among organizations, thereby enhancing cybersecurity and preventing attacks. However, recent reports from the Department of Homeland Security's Office of Inspector General (OIG) have raised concerns about the program's effectiveness and its usefulness to participants. Post a clean renewal of CISA 2015, a review of the program should be considered as a longer-term goal.

Current Benefits of CISA AIS are:

- *Real-time threat intelligence sharing.*—Participants can share and receive machine-readable cyber threat indicators (CTIs) and defensive measures (DMs) in real time to proactively defend their networks.

- *Collective knowledge.*—Organizations benefit from the collective knowledge of participants, gaining insights into observed threats and vulnerabilities.
- *Liability and privacy protections.*—The Cybersecurity Information Sharing Act of 2015 (CISA 2015) provides certain legal protections to encourage sharing, including liability protection, privacy protections, and exemption from specific disclosure laws.

Challenges and Criticisms:

1. *Declining participation.*—The number of participants actively sharing information through AIS has decreased significantly in recent years.
2. *Insufficient shared indicators.*—The volume of shared CTIs has also declined considerably, raising concerns about the program's ability to facilitate effective real-time threat sharing.
3. *Lack of context.*—Some reports indicate that the quality of shared information is not always sufficient, lacking the contextual details necessary for effective threat mitigation.
4. *Outreach and funding issues.*—The OIG attributed the decline in participation to CISA's inadequate outreach strategy and difficulties in identifying specific program costs and auditing expenditures.

Overall Usefulness:

Despite the reported challenges, the CISA AIS program is a valuable tool for enhancing cybersecurity by promoting information sharing and collective defense. However, the program's current effectiveness is under scrutiny due to the decline in participation and shared threat indicators. CISA has acknowledged the issues and is working to address them, including the development of a new threat intelligence strategy and evaluation of the AIS program's effectiveness. The agency is also exploring alternative information-sharing systems, potential technical enhancements, and feedback from participants to improve the program.

From a technical enhancement perspective, the platform needs more than technical compliance with STIX and TAXII standards. It should offer meaningful metrics, such as scores for timeliness, uniqueness, and detection effectiveness. The system must also reduce integration friction. Many companies already support the necessary formats but do not use AIS due to the additional burden involved.

One recommendation would be for CISA to offer hosted pilots for smaller organizations, provide direct feedback about how shared data is used, and build tools that demonstrate how one company's input protects others. Perhaps most importantly, AIS should be repositioned as a core element of national cyber defense, rather than merely serving as a data repository.

In conclusion, while the CISA AIS program offers potential benefits for cybersecurity, its usefulness may currently be limited by the reported challenges with participation and information sharing. It needs to be revamped if we are to achieve stronger collaboration. Still, the work necessary cannot be fully executed before the expiration of CISA 2015 and should not be considered in a clean renewal strategy.

Question 3. How has the Cybersecurity Information Sharing Act of 2015 (CISA 2015) changed the information-sharing environment among private-sector entities?

Answer. The Cybersecurity Information Sharing Act of 2015 significantly altered private-sector cybersecurity information sharing by creating a legal framework that encourages voluntary sharing of cyber threat indicators and defensive measures with both the Government and other private entities. This framework provides protections and incentives for companies to share information, including antitrust exemptions and immunity from specific disclosure laws.

Protections Include:

- *Legal Protection for Sharing.*—CISA 2015 provides protections from legal liability when organizations voluntarily share cyber threat information with both the Federal Government, through the Department of Homeland Security (DHS), and other entities in the private sector.
- *Antitrust Exemptions.*—The act permits companies to collaborate and share information without the risk of antitrust scrutiny by providing exemptions from antitrust laws.
- *Immunity from Disclosure Laws.*—CISA 2015 shields shared information from specific disclosure laws, such as open Government and Freedom of Information Act requests, to encourage more open sharing.
- *Non-Waiver of Protections.*—Sharing information under the guidance of CISA 2015 does not waive any other applicable protections or privileges.
- *Centralized Sharing.*—CISA 2015 established a centralized mechanism for sharing information with DHS as the primary point of contact through the AIS Initiative.

- *Focus on Cyber Threat Indicators and Defensive Measures.*—CISA 2015 encourages the sharing of cyber threat indicators, such as malicious IP addresses, and defensive measures, including security patches.
- *Ex Parte Communications Waiver.*—The sharing of cyber threat information with the Federal Government, under CISA 2015, is not considered ex parte communication.
- *No Mandate for Sharing.*—While CISA 2015 encourages sharing, it does not require private entities to share information, which is a key point of the act. Sharing is voluntary and helps establish the trust necessary for transparent communications.

CISA 2015 marked a turning point in public-private cybersecurity collaboration. In summary, it provides the critical legal protections outlined, which encourage the private sector to share threat indicators more confidently, primarily through ISACs and coordinated efforts with CISA. By addressing liability, privacy, and antitrust concerns, the act helps shift cybersecurity from a siloed effort to a more collective defense model.

The act also promotes the use of standardized data formats, which improved technical compatibility and laid the groundwork for broader sharing across sectors. Over time, even this has led to stronger partnerships and faster threat awareness. While there have been challenges and developments that must be addressed, a clean renewal of CISA 2015 is the most effective way to maintain information sharing and the partnership in the future.

Question 4. Is there any ambiguity in CISA 2015's definitions, such as for cyber threat indicators or defensive measures? If so, please explain.

Answer. Yes, there are acknowledged ambiguities in the definitions within the Cybersecurity Information Sharing Act of 2015 (CISA 2015), particularly regarding its scope and application. These ambiguities, however, can be addressed in subsequent modifications to CISA 2015 after a clean renewal of the current act, modernization of the current public/private sharing organizations, and a potential revamp of CISA. The main examples of ambiguities are:

- *Substantial Cyber Incidents.*—While CISA's approach to covered cyber incidents is limited to "substantial" incidents, the definition of "substantial" has been interpreted broadly, leading to ambiguities regarding which incidents fall under the reporting requirements.
- *Third-Party Incidents.*—The definition of "third-party" incidents, encompassing incidents involving vendors and suppliers of covered entities, has been read broadly.
- *Cybersecurity Threat.*—While the act defines "cybersecurity threat" as an action on or through an information system that may result in an unauthorized effort to impact its security or data adversely, it also includes exemptions for activities that are solely violations of consumer agreements and authorized activities that incidentally cause adverse effects.
- *Definition of "Cyber Threat Indicator."*—Since CISA 2015, the recommendation has been made to expand the definition of "cyber threat indicator" to address emerging threats such as AI-related issues and supply chain vulnerabilities.

These ambiguities can raise operational questions in addition to concerns around legal risk, and impact how entities implement and comply with CISA 2015, particularly concerning information sharing and incident reporting. Companies often worry about crossing legal lines, especially when using sinkholing, beaconing, or deception techniques. The statute prohibits anything that causes "damage," but it does not clearly outline what counts as damage in a cyber context. Even the phrase "timely removal of personal information" lacks a specific time frame, which leads to differing interpretations and inconsistent application.

These ambiguities create risk for legal teams and discourage organizations from sharing data that may otherwise be valuable and have led to discussions surrounding the CISA 2015 reauthorization, suggesting a need to address these ambiguities, possibly by amending definitions or expanding liability protections to encourage greater sharing of information now. This can, though, be accomplished post a clean renewal of CISA 2015 and would still enable the desired outcome of on-going efforts to refine the law and address potential issues related to its interpretation and effectiveness as new technologies. One short-term solution suggestion would be for CISA to continue to release more guidance to help clarify aspects of the law and assist non-Federal entities in sharing cyber threat information.

Question 5. How important is the antitrust exemption in CISA 2015? Please explain and provide any examples that would help illustrate your point.

Answer. The antitrust exemption in CISA 2015 is considered crucial for promoting cybersecurity information sharing, particularly within the private sector. It encourages collaboration, facilitates broader information sharing, enhances collective de-

fense, and minimizes legal risks for companies. In essence, the antitrust exemption, alongside other legal protections provided by CISA 2015, plays a crucial role in enabling and encouraging the voluntary sharing of cyber threat information, which is considered vital for defending against modern cyber threats and strengthening national cybersecurity.

While the antitrust exemption is critically important, it is underutilized. In a few high-profile incidents, such as the response to Log4Shell, the exemption enabled competitors to coordinate quickly and share detection signatures. But these examples remain rare and could be examined post a clean renewal of CISA 2015 as an area for improvement. Legal departments often remain cautious because the statutory language is narrow and unfamiliar. Without more clarity or precedent, many companies still avoid open collaboration.

To make the exemption more effective, the Government, via either the ONCD or CISA, should publicize success stories and clarify boundaries. Clear guidance about what is and is not permitted would go a long way toward increasing confidence and use of this vital provision. Trying to address this improvement now, however, may jeopardize the renewal of the act, and is not recommended; it may, however, be an area for consideration in the future.

Question 6. The existing statute states that the Federal Government must share “timely” information. Do you believe that the Federal Government is succeeding in this role, and does this extend to both Classified and unclassified information? Please explain.

Answer. Consistency is critical, and while there has been improvement in the release of public joint advisories across CISA, NSA, and FBI, there has been little consistency. Without CISA 2015, there is a significant concern about “timely” sharing that needs to be addressed. The perception is that it often falls to the private sector to provide anchor points for further industry examination from the information provided by the Federal Government. If we were to lose the protections of information sharing that CISA 2015 provides, there would be significant concerns about how these critical anchor points would be disseminated.

In addition, as we highlighted, without a revamp of the AIS program, which could not be accomplished before the CISA 2015 renewal deadline, the current AIS feeds continue to deliver data with variable delays. The quality of that information is inconsistent, as noted with the incorrect Yara rules in many reports.

In cybersecurity, time matters. In discussions with the broader private-sector community, the primary concern is that our critical national infrastructure is increasingly becoming a target for non-state aggressors. Only through enhanced information sharing, such as that established in CISA 2015, will we be able to ensure its longevity. A clean renewal of CISA 2015 is one of the key ways we can start to take the steps necessary to enhance and improve a “timely” response from the Federal Government on cybersecurity, build more trust with the private sector, and address the rapidly-changing threat landscape.

In addition, from a “timely” information-sharing perspective, the goal of the Federal Government should be to shorten distribution cycles and modernize its communication methods, like the AIS program, to facilitate stronger and more accurate reporting of critical cybersecurity incidents, whether Malicious, Malfunction, or Mistake-driven that may impact the private sector. The sharing facilitated by CISA 2015 is crucial to achieving this goal.

