Statement of the
National Retail Federation

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

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

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, D.C., 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 one in four 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

NATIONAL RETAIL FEDERATION
1101 New York Avenue, NW, Suite 1200
Washington, DC 20005
www.nrf.com

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% 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 CISA 2015 also applies to threat information related to cybercrime and online 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.

---

[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/bill/119th-congress/senate-bill/1337

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 UK 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 cybercriminal 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 cybercriminals send phishing campaigns.

As a second example, Payroll Pirates is a cybercriminal 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% 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 $20B 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 instances, 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 dialogue 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 four months to ensure that CISA 2015 is reauthorized and extended before the September 2025 expiration date.