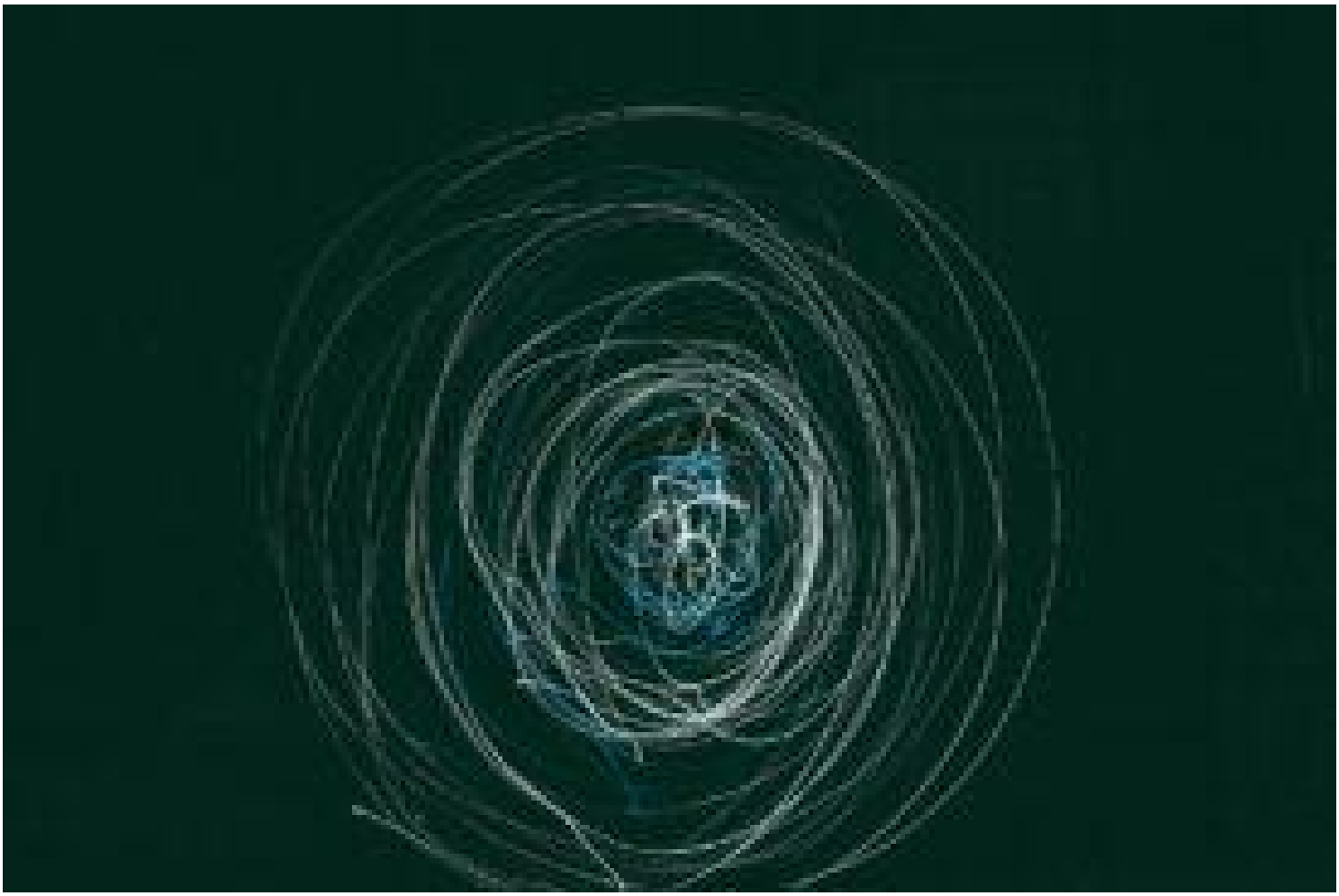
ROPES & GRAY
RopesDataPhiles
Practical Data, Privacy & Cybersecurity Tips from Ropes & Gray

CIPAC Disbandment and CISA 2015 Reauthorization: Recent Developments in the U.S. Cybersecurity Landscape

By Cooper D'Anton on May 2, 2025



Gertrūda Valasevičiūtė, Unsplash

On March 7, 2025, the Department of Homeland Security ("DHS," "the agency") **disbanded** the Critical Infrastructure Partnership Advisory Council ("CIPAC," "the Council"), originally established in 2006 to facilitate communication between the public and private sectors on critical infrastructure issues. CIPAC's termination comes against the backdrop of the **2015 Cybersecurity Information Sharing Act's** ("CISA 2015," "the Act") upcoming expiration on September 30, 2025. CIPAC and CISA 2015 have jointly provided a valuable legal and operational framework for sharing information between the public and private sector in the U.S. for the past decade. Financial services industry stakeholders and members of Congress have **expressed concern** in recent months over increased cyber threats to industry stakeholders should the current public-private information sharing framework deteriorate. These recent developments are poised to significantly impact the financial services industry's cybersecurity landscape – absent steps by Congress and the Administration to provide continuity for the current framework.

Overview

Below, we outline CIPAC's operational function and the CISA 2015 legal protections that firms rely on when sharing sensitive information. Next, we provide brief summaries of the impact these changes could have on the private sector cybersecurity landscape in the U.S. and the path forward to maintain an operational and legal framework to encourage public-private collaboration on cybersecurity issues. Lastly, we provide key takeaways to summarize the material presented.

CIPAC

The **Homeland Security Act of 2002** ("the HSA") compelled DHS to create an effective framework for sharing sensitive critical infrastructure information with the private sector. To accomplish its directive, DHS exercised its **advisory committee authority** under the HSA to **establish CIPAC** in 2006. CIPAC can best be understood not as a *council*, as its name suggests, but as a ***process*** with certain legal protections to promote collaboration between members. These members consisted of representatives from government and sector coordinating councils comprising private firms across 16 critical infrastructure sectors. CIPAC facilitated strategic planning and discussion on cybersecurity issues between government coordinating councils, sector coordinating councils, and cross-sector groups up through its most recent charter renewal in **September 2024** and until its termination in March 2025.

CIPAC served an **operational function** for members by providing a common structure for collaboration – rather than individual firms having to engage with each other and individual agencies one-on-one. Crucial to the Council's capacity to encourage open and honest deliberations was its exemption from the Federal Advisory Committee Act ("FACA"), which **mandates public meetings** of federal advisory committees. This exemption allowed industry participants to hold frank discussions through CIPAC meetings without fear of public disclosure.

As one of 16 critical infrastructure sectors, the financial services industry has benefited from CIPAC's structure. For example, the Financial Services Sector Coordinating Council ("FSSCC"), an industry-led nonprofit that provides a voice for the financial services industry on critical infrastructure issues, **recommended** CIPAC's Cybersecurity Profile Development Working Group as a venue for dialogue to discuss questions raised in an interagency advanced notice of proposed rulemaking on enhanced cyber risk management standards. The FSSCC also allows Working Groups under its **charter** to conduct their efforts through CIPAC. The Council's efforts are wide ranging. For instance, CIPAC groups were **involved** in responding to cyber attacks from U.S. adversaries and have also alerted stakeholders of physical threats, like weather disasters, that could harm critical infrastructure like power grids and pipelines. Collaboration through CIPAC was best accomplished not only through the non-public nature of its meetings but also through the accompanying legal protections provided under CISA 2015.

CISA 2015

Enacted in response to the 2015 Office of Personnel Management data breach, CISA 2015 has promoted an increase in public-private information sharing over the past decade. The Act formed the foundation for how firms collaborate with the federal government and each other to share necessary information to protect themselves and their clients from cybersecurity threats. Notably, CISA 2015 works in tandem with other federal cybersecurity laws by providing potentially **incident-preventing information**, as opposed to the post-incident information reporting required under the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA"). CISA 2015's provisions are implemented through the Automated Indicator Sharing Program ("AIS"), which operates a server that allows participants to share cyber threat indicators. The AIS primarily shares indicators provided by government agencies as well as those voluntarily shared by the private sector.

CISA 2015's legal protections empower firms to voluntarily share cyber threat indicators and defensive measures ("cyber threat information") without fear of litigation or enforcement. These provisions further protect firms' legal privileges, control over their information, and their contractual, trade secret, and intellectual property rights when sharing cyber threat information. Key provisions in the Act include the following:

- Monitoring and Defending Information Systems (Sections 104(a)(1)(A)–(C), 104(b)(1)(A)–(C)): Allows a firm to monitor and operate defensive measures on its own information system – or if permitted, another party's information system – for cybersecurity purposes.

- Information Sharing (Section 104(c)(1)): Firms may share cyber threat information with other private entities and with the federal government.

    - Removal of Personal Information (Section 104(d)(2)(A)–(B)): Firms must scrub personal information when sharing cyber threat indicators.

    - Lawful Restrictions on Use (Sections 104(c)(2), 104(d)(3)(A)(ii)(I)): Firms must comply with lawful restrictions that the sharing firm imposes on sharing or using their information.

    - Voluntary Participation (Sections 106(c)(1)(A–B), 108(h)(1)–(2), 108(i)): There is no obligation for a firm to share cyber threat information or warn others based on information received. Additionally, the federal government may not condition its sharing of information with a firm on that firm's reciprocal information sharing.

- Liability Protection for Monitoring (Section 106(a)): Protects firms against litigation for monitoring an information system for cybersecurity purposes.

- Liability Protection for Sharing Cyber Threat Indicators (Section 106(b)): Protects firms against litigation for sharing cyber threat information, if done in accordance with CISA's requirements, including scrubbing personal information and using DHS's process when sharing with the federal government.

- Liability Protection for Antitrust (Section 104(e)(1)–(2)): Protects firms against antitrust litigation for sharing cyber threat information and assisting each other to prevent, investigate, or mitigate cybersecurity threats.

- Protection from Regulation and Enforcement (Section 105(d)(5)(D)(i–ii)): Prevents the federal government from using cyber threat information provided by firms for regulation or enforcement, except to develop or implement new cybersecurity regulations.

- No Waiver of Privilege or Protection (Section 105(d)(1)): Providing cyber threat information to the federal government does not waive any legal privileges or protections, including trade secret protection.

- Preserving Contracts (Section 108(g)): The Act does not amend current or future contracts or abrogate trade secret or intellectual property rights.

- Freedom of Information Act ("FOIA") Exemption (Section 105(d)(3)): Information shared is exempt from FOIA or any state or local provisions requiring disclosure of information or records.

Impact on Private Sector

As **industry advocates** publicly recognize, CIPAC's termination could frustrate open dialogue between members – the precise **complaint** DHS's principal advisory committees expressed when initially contemplating CIPAC's FACA exemption. Similarly, without a non-public forum, firms may face challenges to understanding their legal obligations and protections when sharing cyber threat information. And without a collaborative platform, firms may experience operational disruptions while seeking alternative ways to coordinate their cybersecurity efforts. This could result in delays in threat detection and response. Throttling communication between the public and private sectors could leave firms increasingly vulnerable to cyber threats that they may have otherwise avoided, had they been armed with cross-sector cyber threat information.

Even if DHS replaces CIPAC with a comparable alternative, the expiration of CISA 2015's legal protections will have a chilling effect on cyber threat information sharing, making companies **reluctant** to contribute to the joint public-private cyber defense. A lapse in the legal framework provided in the Act could exacerbate the growing cyber threats firms already face.

Cyber threats impose considerable costs on firms. The average global cost of a data breach to an organization is $4.88 million, according to the **2024 IBM Cost of a Data Breach Report**. The average cost in the U.S. is $9.36 million. Firms incur data breach costs in the form of notifications to clients, regulators, and third parties, regulatory fines and legal expenditures, and lost business

resulting from operational disruptions and reputational damage. For instance, cyber threats in the **asset management industry** have greatly increased as funds rely more and more on technology. These threats surface across distribution channels, data and intellectual property, front-, middle-, and back-office operations, settlement and finance systems, and increasing use of automation.

Moving Forward

The extent of the impact of CIPAC's termination may depend on whether DHS establishes a new advisory committee with a similar function to take its place. The current administration could fill CIPAC's role with a new, rebranded committee. In fact, during a keynote speech at the recent RSAC Conference, DHS Secretary Kristi Noem stated that she plans to **reinstate CIPAC**. Further, CISA held a meeting on March 14 where "they said their plan is get the same authorities through some other name," according to a **press** source. In addition, there are signs that part of CIPAC's work continues. A press outlet **reported** that a regularly scheduled cross-sector coordination call between industry groups representing different critical infrastructure sectors occurred as recently as the day after CIPAC's termination. An industry source told the outlet that the regularly scheduled call is set to continue uninterrupted – despite being a byproduct of CIPAC.

The legal protections in CISA 2015 enjoy bipartisan support in Congress but face several **obstacles** to reauthorization. While Senators Gary Peters (D-MI) and Mike Rounds (R-SD) recently **introduced** a bipartisan reauthorization bill, the legislative timeline to pass the bill is tight in light of competing priorities. Lawmakers may take the opportunity to advocate for updates to the current law, such as by **expanding existing definitions** in the Act to clarify the type of information shared or to account for recent technological developments. **Lawmakers** may also use the need for reauthorization to extract controversial policy concessions on both related and unrelated issues, potentially creating a logjam in negotiations.

Key Takeaways Firms in critical infrastructure sectors are facing a dynamic legal landscape when sharing cyber threat information with each other and the federal government. CIPAC's termination and CISA 2015's upcoming expiration threaten the operational and legal framework that allowed firms to collaborate on cybersecurity issues for the past decade. However, the Administration may choose to replace CIPAC with a new, similar process to facilitate public-private collaboration. And the CISA 2015 legal protections firms rely on when providing sensitive information to their competitors and regulators enjoy bipartisan support in Congress for reauthorization.

RopesDataPhiles