Congressional Research Service
Informing the legislative debate since 1914

INSIGHT

ANCHOR-CI: A New Public-Private Partnership Framework for Critical Infrastructure Stakeholders

November 25, 2026

On July 1, 2026, the Department of Homeland Security (DHS) announced a new framework for public-private coordination and information sharing within the national critical infrastructure security and resilience enterprise. The Alliance of National Councils for Homeland Operational Resilience—Critical Infrastructure (ANCHOR-CI) replaces the previous framework that the Trump Administration terminated on March 7, 2025, which was known as the Critical Infrastructure Partnership Advisory Council (CIPAC). This Insight discusses ANCHOR-CI; how it differs from its predecessor, CIPAC; and selected congressional considerations regarding information sharing under the new framework.

Although much of the nation's critical infrastructure (e.g., cell-phone communications, some electric grid systems, and hospitals) is privately owned, the public may be put at risk if these systems fail. Federal critical infrastructure risk management policies have fostered voluntary collaboration (as opposed to regulatory mandates) between the public and private sectors through incentives, information sharing, and voluntary investments in security. First introduced in 2006, CIPAC facilitated establishment of numerous advisory councils as forums for discussions of sensitive infrastructure security and resilience information affecting 16 officially recognized critical infrastructure sectors.

Dissolution of CIPAC and Establishment of ANCHOR-CI

DHS terminated CIPAC in accordance with Executive Order 14217 of February 19, 2025, "Commencing the Reduction of the Federal Bureaucracy," which directed the dissolution of "unnecessary" government entities. DHS officials indicated that they planned to introduce a successor framework that would include a wider circle of stakeholders than CIPAC and place more responsibility for infrastructure security and resilience at the state level. According to the Cybersecurity and Infrastructure Security Agency (CISA), the DHS agency that administers infrastructure protection programs, the new framework was developed over many months in consultation with experts and other stakeholders.

Introduced on July 1, 2026, the ANCHOR-CI charter provides four types of coordination councils, two of which are new:

Congressional Research Service
https://crsreports.congress.gov
IN12758

- **Critical Infrastructure Sector Councils.** These are organized on a sector basis and existed previously under CIPAC. Interagency government councils, known as Government Coordinating Councils (GCCs), are chaired by a designated Sector Risk Management Agency—federal agencies with expertise and established relationships in a given sector. The private sector counterparts to GCCs are known as Sector Coordinating Councils (SCCs).
- **Cross-Sector Councils.** These councils "address current and emerging threats, interdependencies, or other issues impacting multiple critical infrastructure sectors or industries." This category also existed previously under CIPAC.
- **Critical Infrastructure Industry Councils.** Newly established under ANCHOR-CI, these councils are intended to serve industries with operations across multiple sectors facing industry-specific "specialized risks" and "shared challenges."
- **Regional Coordinating Councils.** Newly established under ANCHOR-CI, the CISA Director may establish councils on a regional basis to "ensure access and representation by State, Local, Tribal, and Territorial government and critical infrastructure entities in rural areas."

Reorganization of Coordinating Bodies and New CISA Authorities

Existing coordination bodies originally chartered under the CIPAC charter and newly created ones will be required to organize (or reorganize) under the ANCHOR-CI framework to be recognized. The ANCHOR-CI framework provides CISA with greater control over composition of coordinating bodies organized under its auspices. The CISA Director has approval authority to nominate members for coordination councils or may appoint members directly. Both public and private sector council members serve at the Director's pleasure and may be dismissed for any reason. Also, the Director has wide discretion to appoint additional public or private sector entities and individuals to ANCHOR-CI councils "as appropriate to best meet the needs of the federal government."

Some observers believe these authorities and the creation of industry and regional councils may allow CISA to broaden the reach of infrastructure security and resilience councils, and introduce fresh perspectives, experience, and urgency to their activities. Others have voiced concerns that the new framework grants CISA too much control over private sector councils that previously had a large degree of autonomy and may diminish the role of mature sector-based security and resilience programs in favor of unproven state and local capabilities in infrastructure risk management and resilience.

Potential Changes to Information Sharing

The underlying policy premise of the coordinating bodies established under CIPAC was that mitigating disincentives for information sharing and increasing trust between the public and private sectors would lead to greater industry willingness to invest in system-level resilience. CIPAC provided exemption from open-meeting and disclosure requirements of the Federal Advisory Committee Act (FACA; P.L. 92-463) to encourage candid discussion of sensitive issues and sharing of infrastructure security information needed to provide stakeholders with timely and accurate risk information. Therefore, dissolution of CIPAC prompted concerns in some quarters that trusted relationships and information-sharing functions between the public and private sectors would atrophy.

ANCHOR-CI reestablishes legal exemptions from FACA requirements previously made by the Secretary of Homeland Security under 6 U.S.C. §451(a). Some stakeholders note that ANCHOR-CI does not include the other exemptions that were customarily recognized under the CIPAC framework for sharing sensitive infrastructure information in a multilateral format. These included information protection

measures, antitrust protections, liability protections, and protections from public disclosure. Other private sector stakeholders expressed concerns that the reduced protections under the new framework may disincentivize participation, according to media reports. According to CISA, the new framework places greater responsibility for antitrust and liability compliance on private sector participants.

Under federal law, FACA-exempt advisory councils established by the Secretary of Homeland Security must disband after two years unless extended by the Secretary. As of this writing, no councils have been chartered under the ANCHOR-CI framework. Therefore, there is some uncertainty as to how certain charter provisions will be implemented and what other protections might apply to private sector participants in ANCHOR-CI information-sharing activities. Depending on implementation and uptake from the private sector, ANCHOR-CI may change the composition of the broader critical infrastructure community by changing incentives for participation and criteria for inclusion and by redefining the scope of federal responsibility for infrastructure security and resilience.

Congress may monitor the adoption of the ANCHOR-CI framework within the critical infrastructure enterprise to ascertain, for example, the extent to which the new format has elicited participation from private sector partners. Congress may solicit testimony from stakeholders on potential improvements with the shift to ANCHOR-CI from CIPAC, such as more representative inclusion in coordination activities, as well as potential drawbacks, such as greater perceived risk for information sharing and how this might affect private sector participation. Congress may consider legislation to expand and clarify legal protection and exemptions for private sector participants in ANCHOR-CI activities. Congress may also consider whether provision of additional resources for infrastructure security and resilience programs at the state and local level is necessary if ANCHOR-CI implementation ultimately places greater responsibility on states and localities for these functions.

Author Information

Brian E. Humphreys
Analyst in Science and Technology Policy

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.