National Council of ISACs FAQ

What is the National Council of ISACs?

The National Council of ISACs (NCI) is a member-based information sharing organization focused on collaboration and coordination between Sector-based Information Sharing and Analysis Centers (ISACs). Formed in 2003, the NCI today is comprised of 25 organizations designated by their sectors as their information sharing and operational arms.

The NCI is a true cross-sector partnership, providing a forum for sharing cyber and physical threats and mitigation strategies among ISACs and with government and private sector partners during both steady-state conditions and incidents requiring cross-sector response. Sharing and coordination is accomplished through daily and weekly calls between ISAC operations centers, daily reports, requests-for-information, monthly meetings, exercises, and other activities as situations require. The NCI also organizes its own drills and exercises and participates in national exercises.

Council members are present on the National Cybersecurity and Communications Integration Center (NCCIC) watch floor, and NCI representatives can embed with National Infrastructure Coordinating Center (NICC) during significant national incidents. The Council and individual members also collaborate with other agencies of the federal government, fusion centers, the State and Local Tribal Territorial Government Coordinating Council, the Regional Consortium Coordinating Council, the Partnership for Critical Infrastructure Security – the Cross-Sector Council, and international partners.

Who can join the NCI?

The NCI welcomes membership from organizations that have been designated by their sector leadership as their official forum for sharing threat information. Critical infrastructure sectors and subsectors that have not yet established a method for sharing across their sectors are encouraged to contact the NCI to discuss how they can collaborate with NCI and participate in its activities.

What is an Information Sharing and Analysis Center (ISAC)?

Sector-specific ISACs are trusted entities established by critical infrastructure owners and operators to foster information sharing and best practices about physical and cyber threats. Typically global, private, non-profit organizations, ISACs work directly within their sectors, communicating critical information far and wide and maintaining sector-wide situational awareness. ISACs are trusted entities that collect, analyze and disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency. Besides sharing threat information with members, ISACs also share information with government and other critical infrastructure ISACs as applicable.

ISACs were created in response to Presidential Decision Directive-63 (PDD-63), signed in 1998, which called for each of the 16 critical infrastructure sectors to voluntarily establish sector-specific organizations to share information about cyber threats and vulnerabilities. After 9/11, the mission of ISACs was expanded to include the sharing of physical threats and vulnerabilities.

What is the difference between an ISAC and ISAO?

ISACs were created in 1998 in response to PDD-63 to advance the security of critical infrastructure/key resources (CIKR) sectors – those sectors deemed vital to the well being of a nation – through the sharing of information within and among the sectors and with government.

Information Sharing and Analysis Organizations (ISAOs), formed in 2013 in response to Executive Order 13691, are information sharing organizations for any sector or community. ISAO's do not need to be part of the 16 critical infrastructure like ISACs. Instead, ISAOs may be organized on the basis of sector, sub-sector, region, or any other affinity, including in response to particular emerging threats or vulnerabilities.

ISACs are the original ISAOs for the critical infrastructure sectors. However, ISACs play a much bigger role in critical infrastructure protection and resilience than just sharing information. ISACs are a vital operational component in the national partnership framework. ISACs work through the National Infrastructure Protection Plan (NIPP-13) and collaborate with sector specific agencies and coordinating councils to perform structured collaboration within an established role in incident response across the CIKR. They are recognized as the designated arms for dissemination of information, manage and set the threat levels, and have strong reach and subject matter expertise within their respective sectors. ISACs are all-hazards and look at both cyber and physical. They provide a sector perspective and allow for anonymization and aggregation of data.

What does an ISAC do?

ISACs help critical infrastructure owners and operators protect their facilities, personnel and customers from cyber and physical security threats and other hazards. ISACs collect, analyze and disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency.

www.nationalisacs.org

Join an ISAC today! Visit our website www.nationalisacs.org for more information

ISACs share information, collaborate, and discuss threat, vulnerability, and risk information about cyber and physical security risks through secure forums. ISACs also provide operational services – such as risk mitigation, incident response, and information sharing – that protect critical infrastructures. Other ISAC services include annual meetings, technical exchanges, workshops, webinars, 24/7 threat warning, incident reporting capabilities, setting the threat level for their sectors, and sharing actionable and relevant information more quickly than government partners.

Why is belonging to an ISAC important?

Being a member of an ISAC can extend the scope and capabilities of your organization's security and risk management activities and help bolster threat and risk awareness, preparedness capabilities and help connect you to organizations and insights that may not be readily available to individual organizations, particularly smaller organizations with limited staff. Our adversaries – extremists of all stripes, cyber criminals, nation states and others – share their tactics, techniques, and procedures to outsmart and out-maneuver us individually. Together, as we share information and cyber threat intelligence across the community, we decrease attackers' chances of success.

Was there a law that required ISACs to form?

No, there was no law that required ISACs to form. The concept of ISACs was introduced and promulgated pursuant to PDD-63, signed May 22, 1998, after which the federal government asked each critical infrastructure sector to voluntarily establish sector-specific organizations to share information about threats and vulnerabilities. Many industry sectors took up the cause. Some ISACs formed as early as 1999, and most have been in existence for at least ten years.

The Cyber Information Sharing Act (CISA) passed in 2015 does provide liability protection for critical infrastructure sharing when information is properly shared through an ISAC or other information sharing organization.

How are ISACs structured?

ISACs are trusted entities established by critical infrastructure owners and operators to foster information sharing and best practices about physical and cyber threats and mitigation. Typically global, private, nonprofit organizations, ISACs reach deep into their sectors, communicating critical information far and wide and maintaining sector-wide situational awareness.

What response capabilities do ISACs have?

Each ISAC has its own model to meet the unique needs of its members. Generally, all ISACs facilitate the sharing of sensitive threat, attack and vulnerability information among its members, provide regular threat analysis and reporting, and serve as a forum for members to collaborate and coordinate during incidents. ISACs have a track record of responding to and sharing actionable and relevant information more quickly than government partners.

Who can join an ISAC?

Each ISAC has specific requirements and membership eligibility for their sector. Details about the different ISACs can be found on the NCI website: www.nationalisacs.org.

What are the benefits of an ISAC?

Joining your sector's ISAC is one of the best ways organizations can protect themselves and their employees against cyber and physical threats and vulnerabilities while taking an active stance in safeguarding our nation's critical infrastructure. ISACs provide trusted sector specific forums for active information sharing and collaborative analysis around cyber and physical threats, vulnerabilities, and incidents. ISACs bring together analysts from companies of all sizes to share information on how to identify and defend against active attacks. In this way, companies with more robust capabilities assist each other and those with less robust programs.

The ability to have a single point of outreach to each critical infrastructure community is an important tool for national cyber incident response. ISACs can quickly and effectively share information from government to their members and can provide an important source of company-neutral analysis as to how a threat or incident affects their particular sector. ISACs may also provide members with tools to mitigate risks and enhance resiliency.

How much does it cost to join an ISAC?

Since each ISAC is independently operated and governed, the cost to join an ISAC varies by ISAC. ISAC dues are used to provide and produce products and services to support its members.

How does my organization become a member of my sector's ISAC?

Organizations can apply to their industry specific ISAC. To find a list of the different ISACS, visit: www.nationalisacs.org.

How do member organizations benefit from sharing with each other?

Members can share on a real-time basis and then take that information, intelligence, and analysis and use it in their environments to prevent, protect against, mitigate, respond to, and recover from the cyber, physical, health, and natural threats and hazards that pose the greatest risk.

How do ISACs work with the government?

Information may be shared from ISACs with government partners and organizations but only with the submitting organization's explicit approval, under the agreed to Traffic Light Protocol designation and with or without member attribution, as desired by the member.

ISACs work through the National Infrastructure Protection Plan (NIPP-13) and collaborate with sector specific agencies and coordinating councils to perform structured collaboration within an established role in incident response across the critical infrastructure sectors.

Join an ISAC today! Visit our website www.nationalisacs.org for more information