NationalCouncilofISACs

JANUARY 2016

INFORMATION SHARING AND ANALYSIS CENTERS (ISACS) AND THEIR ROLE IN CRITICAL INFRASTRUCTURE PROTECTION

About ISACs

- Leverage the expertise and experience of existing private/public sector critical infrastructure protection organizations to improve the resilience of the nation.
- Maximize the operational foundation of the ISACs that share information between the government and private sector critical infrastructures, as well as share information among sectors.
- Support the needs of all critical infrastructures to provide trusted and secure actionable information sharing and sector specific analytical capabilities while respecting the individuality of each sector.

Why ISACs?

- 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 nonprofit organizations, ISACs have unique capabilities to provide comprehensive sector analysis and have extensive reach within their sector.
- ISACs communicate threat information across sectors and with the government to create situational awareness.
- ISACs analyze and address all aspects of security and other hazards related to critical cyber and physical infrastructures and cross-sector interdependencies.
- ISACs have demonstrated success in providing operational services – such as risk mitigation, incident response, and information sharing – that protect critical infrastructures.
- In addition to information sharing, ISAC services include annual meetings, technical exchanges, workshops, webinars, and other learning opportunities.

- ISACs have a track record of responding to and sharing actionable and relevant information more quickly than government partners.

- ISACs empower business resiliency through security planning, disaster response, and execution. Most ISACs have 24/7 threat warning and incident reporting capabilities, and may also set the threat level for their sectors.

- Additional ISAC services include annual meetings, analyst focused technical exchanges, workshops, webinars, and other learning opportunities.

Accomplishments

- In addition to supporting their individual sectors, ISACs address physical and cyber threats, incidents, and vulnerabilities on a cross-sector basis through:
    - National Council of ISACs (NCI)
    - Partnership for Critical Infrastructure Security (PCIS) – the Cross-Sector Council
    - National Cybersecurity and Communications Integration Center (NCCIC) of the U.S. Department of Homeland Security
    - National Infrastructure Coordinating Center (NICC) of the U.S. Department of Homeland Security
    - Cyber Intelligence Group of the U.S. Treasury Department
    - Individual agreements designed to foster information sharing

- ISACs play a key role in coordinating sector wide responses to incidents and disasters, and may collaborate with the State and Local Tribal Territorial Government Coordinating Council (SLTTGCC), the Regional Consortium Coordinating Council (RCCC), and international partners.

- ISAC operational staff have the capability to embed at the NICC to help establish, obtain and share ground truth information about the cross-sector impact of physical events.

- Convened by the NCI, ISACs meet daily and weekly to exchange cross-sector information on the latest physical and cyber threats, vulnerabilities, and incidents.

- Many ISACs have implemented automated threat information sharing capabilities using OASIS CTI (STIX/TAXII) based technologies to facilitate the sharing of cyber threat indicators in near-real time.

- When financial institutions suffered distributed denial of service (DDoS) attacks backed by a foreign government in 2012 and 2013, ISACs shared mitigation strategies between sectors and with the government. This information proved to be extremely beneficial during the third and fourth waves of attacks.

- Recognizing that trusted relationships between the private sector and intelligence and law enforcement communities are critical, ISACs have fostered partnerships with the FBI, Director of National Intelligence, SSAs and state and local fusion centers.

- Several ISACs have collaborated with each other and with federal agencies on joint advisories, white papers, and reports.

- The NCI conducts exercises and recently completed Phase 2 of the Operational Collaboration Forum Series (OCF) to enhance cross-sector information sharing and operational coordination during and after incidents of national significance. Through tabletop exercise and workshops, the ISACs examined gaps, identified opportunities, and established working groups to develop solutions.

- ISACs participate in DHS and FEMA exercises, such as National Level Exercises, the Cyber Storm series, and CyberGuard. Some also organize and participate in their own exercises (e.g., the financial services sector's Cyber Attack against Payment Processes exercises and the electricity sector's GridEx series).

Background

The concept of Information Sharing and Analysis Centers (ISACs) was introduced and promulgated pursuant to Presidential Decision Directive-63 (PDD-63), signed May 22, 1998. PDD-63 recognized the potential for the infrastructures of the United States to be attacked either through physical or cyber means with the intent to affect the military or economic power of the country. The federal government asked each critical infrastructure sector in PDD-63 to establish sector-specific organizations to share information about threats and vulnerabilities. Some ISACs formed as early as 1999, and most have been in existence for at least ten years. ISACs continue to mature and new ISACs continue to form.

National Council of ISACs

- Sector-based ISACs collaborate and coordinate via the National Council of ISACs (NCI). Formed in 2003, the NCI today comprises twenty ISACs. Its objective is to establish and maintain an operational framework in order to maximize information flow across the private sector infrastructures and with government.

- In recent years, the NCI has expanded its mission to exchange critical information with other sectors that do not have their own ISACs. All sector-based ISACs and sectors without their own ISACs are invited to participate.

For further information, please contact nationalcouncilofisacs@natlisacs.org

Please visit the National Council of ISACs public website at www.isaccouncil.org