About NCI ISACs

Information Sharing and Analysis Centers – ISACs – help critical infrastructure owners and operators protect their facilities, personnel and customers from cyber and physical security threats and other hazards. ISACs reach deep into their sectors, communicating critical information far and wide and maintaining sector-wide situational awareness. ISACs collect, analyze and disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency.

- **Automotive ISAC**
- **Aviation ISAC**
- **Communications ISAC**
- **Defense Industrial Base ISAC**
- **Downstream Natural Gas ISAC**
- **Elections Infrastructure ISAC**
- **Electricity ISAC**
- **Emergency Management & Response ISAC**
- **Financial Services ISAC**
- **Health ISAC**
- **Healthcare Ready**
- **Information Technology ISAC**
- **Maritime ISAC**
- **Multi-State ISAC**
- **National Defense ISAC**
- **Oil & Gas ISAC**
- **Real Estate ISAC**
- **Research & Education Network ISAC**
- **Retail & Hospitality ISAC**
- **Surface Transportation, Public Transportation and Over-The-Road Bus ISACs**
- **Water ISAC**

Because critical infrastructure sectors are interdependent, the National Council of ISACs (NCI) has a vital role in facilitating cross-sector coordination among the ISACs, particularly during security incidents and natural disasters. NCI provides a forum for sharing threat and response information and serves as a gateway to the ISACs for federal agencies and other partners. NCI also organizes its own drills and exercises and participates in national exercises. During significant national incidents, NCI is on the National Infrastructure Coordinating Center (NICC) watch floor. NCI members are also present on the National Cybersecurity and Communications Integration Center (NCCIC) watch floor.

AUTOMOTIVE ISAC

www.automotiveisac.com

The Automotive Information Sharing and Analysis Center (Auto-ISAC) is a non-profit information sharing organization that provides a trusted environment and platform for automotive manufacturers and suppliers to collaborate on cybersecurity. Founded by a global group of automakers in 2015, the Auto-ISAC is the central hub for industry-wide sharing of cyber threats, vulnerabilities, and best practices related to the connected vehicle. We embrace a working together model, engaging across the community with automotive strategic partners, trade associations, researchers and universities, and government. Membership is open to light and heavy-duty automotive manufacturers, suppliers, carriers, and fleet operators.

AVIATION ISAC

www.a-isac.com

The Aviation ISAC provides an aviation-focused information sharing and analysis function to help protect global aviation businesses, operations and services. Our vision is a safe, secure, efficient, and resilient global air transportation system. The A-ISAC analyzes and shares timely, relevant and actionable cyber security information as it pertains to threats, vulnerabilities, and incidents. Also, the A-ISAC enables its members to share threats in real time, understand how to tactically combat threats and implement mitigation strategies, enhance collective sector knowledge and implement best practices. A non-profit organization, A-ISAC membership is open to trusted private sector global aviation companies.

Copyright© NCI 2019

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

COMMUNICATIONS ISAC

www.dhs.gov/national-coordinating-center-communications

The Communications ISAC is the operational arm of the communications sector. Also known as the DHS National Coordinating Center, the ISAC's goal is to avert or mitigate impacts upon telecommunications infrastructure so that communication networks remain operational. As a clearinghouse for physical and cyber alerts to the telecommunications industry, the ISAC collects, analyzes and disseminates information on vulnerabilities, threats, intrusions and anomalies to carriers, ISPs, satellite providers, broadcasters, vendors and other stakeholders. The Communications ISAC operates 24/7 and is an operational component within the National Cybersecurity and Communications Integration Center.

DEFENSE INDUSTRIAL BASE ISAC

www.dibisac.net

The objective of the DIB ISAC is to facilitate collaboration among the chapter's members to defend corporate key resources and critical infrastructure against security threats and to collectively encourage their use of national DIB ISAC resources. The DIB ISAC primary functions are to gather and share information/analysis on security issues related to cyber or physical events, threats or intrusions; to facilitate security best practice sharing; and to enhance the ability of the DIB sector to prepare for, respond to and mitigate risk due to security threats, vulnerabilities and incidents.

DOWNSTREAM NATURAL GAS ISAC

www.dngisac.com

The DNG ISAC serves natural gas utility (distribution) companies by facilitating communications between participants, the federal government and other critical infrastructures. Specifically, the DNG-ISAC coordinates very closely with the Electricity ISAC and shares information back and forth between electric, combination (natural gas and electric) and natural gas utilities. The DNG-ISAC promptly disseminates threat information and indicators from government and other sources and provides analysis, coordination and summarization of related industry-affecting information.

ELECTIONS INFRASTRUCTURE ISAC

https://www.cisecurity.org/ei-isac/

Since starting in 2018, the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) has evolved from an idea to a formalized collective of dedicated election officials, their staff members, associations, technology vendors, federal partners, and cybersecurity experts who work tirelessly to help secure the U.S. elections infrastructure. From sharing threat landscape information, to creating educational opportunities and implementing technical cybersecurity controls, the EI-ISAC's members and staff, do everything they can to ensure the security and integrity of our elections. The EI-ISAC was conceived in 2018, as a means of leveraging the many capabilities and the infrastructure of the MS-ISAC. Both the MS-ISAC and EI-ISAC benefit by operating under the auspices of CIS® (Center for Internet Security, Inc). This allows them to work together to educate and protect U.S. State, Local, Tribal, and Territorial governments. The EI-ISAC is a voluntary and collaborative effort based on a strong partnership between CIS, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, and the Election Infrastructure Subsector Government Coordinating Council.

ELECTRICITY ISAC

www.eisac.com

The E-ISAC establishes situational awareness, incident management, coordination, and communication capabilities across the electricity industry through timely, reliable, and secure information exchange. The E-ISAC, in collaboration with the Department of Energy and the Electricity Subsector Coordinating Council (ESCC), serves as the primary security communications channel for the electricity industry and enhances industry's ability to prepare for and respond to cyber and physical threats, vulnerabilities, and incidents.

Copyright© NCI 2019

EMERGENCY MANAGEMENT AND RESPONSE ISAC

www.usfa.dhs.gov/emr-isac

The mission of the EMR ISAC is to collect and analyze critical infrastructure protection and resilience information having potential relevance for Emergency Services Sector departments and agencies and to synthesize and disseminate the information to leaders, owners, and operators of the emergency services.

FINANCIAL SERVICES ISAC

www.fsisac.com

The FS-ISAC – a non-profit corporation established in 1999 and funded by its member firms – helps assure the resilience and continuity of the global financial services infrastructure through sharing threat and vulnerability information, conducting coordinated contingency planning exercises, managing rapid response communications, conducting education and training programs and fostering collaborations with and among other key sectors and government agencies.

HEALTH ISAC

www.h-isac.org

The H-ISAC is a private sector, non-profit organization that provides a trusted community for the sharing of timely, relevant and actionable physical and cyber information among stakeholders to ensure the resilience and maintain the continuity of the health sector against cyber and physical threats, incidents, vulnerabilities and risks. Members include direct patient care providers, health information technology companies, health plan payers, medical device manufacturers, and laboratory, blood and pharmaceutical organizations. The H-ISAC also collaborates with its peer ISACs and government partners and has a presence on DHS's NCCIC and NICC watch floors.

HEALTHCARE READY

www.healthcareready.org

Heathcare Ready (formerly Rx Response) helps to strengthen healthcare supply chains and enhance community resiliency by fostering collaboration between public health and the private sector and by addressing pressing issues before, during and after disasters. As the independent, nonprofit convener of industry and government, Healthcare Ready safeguards patient health by providing solutions to critical problems and sharing best practices for healthcare preparedness and response. Healthcare Ready also provides training and education to officials, policymakers, businesses and the public on the importance of building resiliency into everyday operations and activities.

INFORMATION TECHNOLOGY ISAC

www.it-isac.org

The Information Technology-Information Sharing and Analysis Center (IT-ISAC), was founded in 2000 and achieved operational capability in 2001. The IT-ISAC is a non-profit, limited liability corporation formed by members within the Information Technology sector as a unique and specialized forum for managing risks and corporations' IT infrastructure. Our mission statement is to grow a diverse community of companies that leverage information technology and have in common a commitment to cyber-security; to serve as a force multiplier that enables collaboration and sharing of relevant, actionable cyber threat information and effective security policies and practices for the benefit of all.

MARITIME ISAC

www.maritimesecurity.org

The Maritime ISAC serves ocean carriers, cruise lines, port facilities and terminals, logistics providers, importers, exporters and related maritime industries throughout the world. Its mission is to advance the security of the U.S. and international maritime community by representing maritime interests before government bodies; acting as liaison between industry and government; disseminating timely information; encouraging and assisting in the development of industry-specific technologies; and convening educational and informational conferences for its membership and government partners.

Copyright© NCI 2019

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

MULTI-STATE ISAC

www.ms-isac.org

The Multi-State Information Sharing and Analysis Center (MS-ISAC) is a focal point for cyber threat protection, response and recovery for the nations State, Local, Tribal and Territorial (SLTT) governments. The MS-ISAC's 24x7 cyber security operations center provides real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification and mitigation and incident response services. The U.S. Department of Homeland Security has designated the MS-ISAC as its key cybersecurity resource for SLTTs, including Chief Information Security Officers, Homeland Security Advisors and Fusion Center Directors. The MS-ISAC membership is open to all SLTT government entities.

NATIONAL DEFENSE ISAC

www.ndisac.org

The National Defense Information Sharing and Analysis Center (NDISAC) is the national defense sector's non-profit organization formed to enhance the security and resiliency of the defense industry and its strategic partners. NDISAC provides defense sector stakeholders a community and forum for sharing cyber and physical security threat information, best practices and mitigation strategies and is developed to serve as the Defense Industrial Base (DIB) sector's critical infrastructure protection operational coordination mechanism. Formerly known as the DIB-Information Sharing and Analysis Organization (DIB-ISAO) and Defense Security Information Exchange (DSIE), NDISAC is the defense sector's cyber threat sharing center of excellence.

OIL & NATURAL GAS ISAC

www.ongisac.org

ONG-ISAC provides cyber threat information for the oil and natural gas industry. Its main goal is to assist in increasing the security posture of the industry's exploration and production, transportation, refining, and delivery systems from cyber-attacks through the analysis and sharing of timely and trusted cyber intelligence. As an industry owned and operated organization, ONG-ISAC provides a mechanism for members to share information anonymously across its membership, increasing the speed, quality, and flow of cyber intelligence.

REAL ESTATE ISAC

www.reisac.org

The RE-ISAC is a non-profit organization managed by the Real Estate Roundtable to support the commercial facilities sector by facilitating information sharing on terrorist threats, warnings, incidents, vulnerabilities and response planning — to counter terrorism and protect buildings and the people who occupy and use them. The RE-ISAC works closely with members, government partners at the federal, state and local levels and across the critical infrastructure community and other partners. Members consist of the major trade organizations from the lodging, retail, gaming, multifamily housing, commercial office building, sports leagues, resorts and outdoor events subsectors as well as owners and operators of commercial properties nationwide.

RESEARCH AND EDUCATION NETWORKS ISAC

www.ren-isac.net

The REN-ISAC serves over 620 member institutions within the higher education and research community by promoting cybersecurity operational protections and response. The REN-ISAC member institutions benefit from Security Event System (SES) threat intelligence and other automated data collection and sharing tools to enable informed decisions about threats and events, as well as peer assessment services to improve the institution's overall security posture. The REN-ISAC offers members daily cybersecurity news reports, alerts and advisories, analysis reports of cybersecurity threats and mitigation, and an active, interested community that provides feedback on practices and standards from subject matter experts. The REN-ISAC fosters professional training and development through monthly webinars, regional workshops, and an aggregate purchasing program with the SANS Institute. The REN-ISAC also acts as the Computer Security Incident Response Team (CSIRT) for the research and education community at large.

Copyright© NCI 2019

RETAIL & Hospitality ISAC

www.rhisac.org

The RH-ISAC was formed in 2014 as the home of the Retail and Hospitality Information Security and Analysis Center (ISAC) and operates as a central hub for sharing sector-specific cyber security information and intelligence. The association connects information security teams at the strategic, operational and tactical levels to work together on issues and challenges, to share practices and insights, and to benchmark among each other – all with the goal of building better security for the retail and hospitality industries through collaboration. RH-ISAC currently serves companies in the retail, hospitality, gaming, travel and other consumer-facing entities.

SURFACE TRANSPORTATION, PUBLIC TRANSPORTATION AND OVER-THE-ROAD BUS ISACS

www.surfacetransportationisac.org

The ST, PT and OTRB ISACs are trusted, transportation sector specific, 24/7 incident reporting and threat warning entities that establish the transportation sector's specific information/intelligence requirements for incidents, threats and vulnerabilities. Based on its sector-focused subject matter analytical expertise, the ST, PT and OTRB ISACs collect, analyze and disseminate alerts and incident reports to their membership and help the Government understand impacts for their sector. They provide an electronic trusted ability for the membership to exchange and share information on cyber, physical and natural threats in order to defend critical infrastructure.

WATER ISAC

www.waterisac.org

WaterISAC, a nonprofit organization established in 2001, is the information sharing and operational arm of the U.S. water and wastewater sector. WaterISAC helps members strengthen their physical and cyber security, recover from natural and man-made disasters and improve overall preparedness and resilience. Through a secure web portal, twice-weekly e-newsletters, alerts and webinars, WaterISAC delivers a rich and thorough library of physical and cyber threat information; guidance on risk management, mitigation and resilience; contaminant databases and much more. Members include hundreds of utilities, serving more than 200 million people in the U.S., as well as state, local and federal agencies and consulting firms.

Copyright© NCI 2019