National Defense ISAC

HISTORY OF NATIONAL DEFENSE ISAC

Information Security and Analysis Center (ISAC) Background Information

In 1998, the White House published Presidential Decision Directive 63 (PDD-63), directing federal agencies with a leadership role in specific sectors to identify a sector coordinator to represent the industry perspective on information assurance and critical infrastructure protection programs. As a result and in that same year, a White House Advisory Committee, the National Security Telecommunications Advisory Committee made a recommendation for the creation of mechanisms for information assurance and critical infrastructure protection coordination specifically focused on information and communications technology.

The Network Security Information Exchange (NSIE) was formed as an informal public-private collaboration to serve in this role for the broad information and communications technology community, and its industry members served as an overall sector coordinator role for this broad industry. In 1999, many of the NSIE members began to see potential and value in leveraging the NSIE model of collaboration and coordination for information assurance and cyber security coordination within other sectors and segments of industry. The defense sector is one sector that evolved the NSIE model into the Defense Industrial Base (DIB) sector's equivalent organization, the Defense Security Information Exchange (DSIE).

During the ensuing years, the nation's critical infrastructure protection model was greatly influenced by the threat and impacts of terrorist activities globally and on U.S. soil. With the creation of the Department of Homeland Security (DHS), the term "Information Sharing and Analysis Organization" (or "ISAO") was codified in the Homeland Security Act of 2002. Early in the following year (2003), the White House published Homeland Security Presidential Directive 7 (HSPD 7) which refined the national agenda for critical infrastructure protection collaborative models based on industry coordination and engagement with government across critical business sectors. Also during 2003, the National Council of ISACs (NCI) was established and recognized across industry as a counsel of ISAO organizations who were organized and or recognized by the critical sector industry body for their respective sectors of industry for collaboration with their sector's federal or national lead government agency and cross-sector operational coordination with other sectors of industry.

The organizations that fulfill this unique and central role for sectors of industry are known as Information Sharing and Analysis Centers (ISACs). They are generally recognized as the first and most experienced and capable of organizations that were formed to meet the definition of ISAO published within the Homeland Security Act of 2002 and in some cases were formed or evolved from organizations that were formed before the statue and the creation of the DHS. The role of ISACs was further refined in national policy with the federal government's publication of the first National Infrastructure Protection Plan in 2006, which stated the role of ISACs as follows in Section 4.2.7, Private Sector Node:

> *"ISACs provide an example of an effective private sector information-sharing and analysis mechanism. Originally recommended by Presidential Decision Directive 63 (PDD-63) in 1998, ISACs are sector-specific entities that advance physical and cyber CI/KR protection efforts by establishing and maintaining frameworks for operational interaction between and among members and external security partners. ISACs typically serve as the tactical and operational arms for sector information-sharing efforts. ISAC functions include, but are not limited to, supporting sector-specific information/intelligence requirements for incidents, threats, and vulnerabilities; providing secure capability for members to exchange and share information on cyber, physical, or other threats; establishing and maintaining operational-level dialogue with appropriate governmental agencies; identifying and disseminating knowledge and best practices; and promoting education and awareness."*

The combination of an NSIE model and the NSPD-7 sector-based organizational structure, suggested a method for trusted industry security coordination and collaboration for NSIE members who were also members of the DIB. These NSIE members who were also members of the DIB particularly recognized the importance to the Department of Defense (DoD) as well as the DIB for maintaining such a coordination mechanism among the DIB companies with developing cyber capabilities.

DSIE History

In the early 2000's, these members began to informally collaborate about cyber security threats and practices necessary to ensure industry compliance with security concerns as well as any regulatory security requirements or standards defined by DoD or industry best practices. The trust and value established

Copyright© NDISAC 2019

HISTORY OF NATIONAL DEFENSE ISAC

over several years of their informal coordination and collaboration led to the 2007 creation and 2008 chartering of a DIB-specific information sharing and analysis mechanism chartered as the DIB organization's partner with DoD, a member of the National Council of ISACs, and as the cyber security committee and SME component of the DIB Sector Coordinating Council (SCC). It was simply named DSIE, and maintained an organizational existence as an industrial working group of the National Defense Industrial Association; its then parent trade association.

Between 2007 and 2014, the DSIE trusted information sharing environment matured in depth, value, and scope to a point where it outgrew its home as a trade association committee. Again, a number of the DSIE member companies through the DSIE Board of Directors initiated activities to establish DSIE as an independent incorporated organization. On March 10, 2015, DSIE was incorporated as a 501(c)(6) not-for-profit organization under the name of the Defense Industrial Base Information Sharing and Analysis Organization™ (DIB-ISAO™). Because the DIB-ISAO continues the legacy that began in 2006, we continue to do business as the DSIE. In this capacity, DSIE was (and currently is) recognized by DoD in the role as the cyber security center of excellence for the DIB, and as the industry's central operational component for sector and cross-sector operational coordination and collaboration as defined in Federal statute and policy.

DSIE exists to enable secure threat information sharing and collaboration activities among its members; allowing them to defend their networks and systems, and to continually improve their analytical and security operations capabilities in collaboration with their most capable and trusted peers. DSIE members engage in a high-quality threat information sharing and collaboration environment. The DSIE organizational trust model is relatively unique in that a large amount of threat information sharing and collaborative coordination is done with full attribution among the participant DSIE Members. DSIE interaction occurs with the confidence that all information shared, including the source of the shared data, will not be attributed beyond the trusted environment. The result is a unique high-trust, high-quality, and high-activity environment that offers DSIE members an exceptional incentive for collaboration and that provides a reliability in the source of data shared that enables that data to be rapidly actioned upon with absolute confidence in the data validity.

Active participation in the DSIE threat intelligence sharing environment enhances every DSIE member's ability to defend their corporate network enterprises against significant and advanced security threats. Through effective collaboration mechanisms, DSIE members are able to not only share threat intelligence among trusted security practitioners, they are also able to capture, document, collaborate on the development of, and share cyber security best practice information. Additionally, DSIE members collectively engage to explore tools, resources, and strategies that are most effective in the detection and mitigation of threat activity.

DSIE offers and its members take advantage of continuous threat sharing, periodic hosted technical exchanges, WebEx training discussions, member-to-member mentoring relationships, and working groups that are actively focused on the collective research, development, and implementation of solutions designed to benefit our member's corporate enterprise, our member's overall security posture, and the enterprise risk management functions across the entire DIB community including interdependent security interests.

The DIB-ISAO is committed, through DSIE, to another decade of meeting its member's security and enterprise risk management requirements through a trusted collaborative environment for sharing of high-quality threat intelligence as its core and most valued product.

The DIB-ISAO is also committed to fostering cyber security maturity among the entire DIB including our extended supply chain; many of whom may function within other related sectors of industry. The DIB-ISAO will accomplish this in part through collaboration and mentoring partnerships between DSIE and peer organizations.

Legacy efforts in other sectors have helped infrastructure owners and operators within sectors of industry collectively engage to protect their facilities, personnel and customers from cyber and physical security threats and other hazards since 1999. These organizations provide vital services and products relating to or connected with developing, reviewing, refining, and enhancing standards and practices to assure the security of significant commercial infrastructure and assets. They collect, analyze and disseminate actionable threat information broadly across their sectors of industry and provide the sector with mechanisms and tools to mitigate risks and enhance resiliency. These organizations, ISACs, are a vital part of the national economic security architecture.

For this reason, the DIB-ISAO announced its sponsorship and creation of the National Defense Information Sharing and Analysis Center™ (NDISAC™) during the 10-year anniversary of DSIE to further fill that role for the DIB sector and key suppliers to the DIB sector.

About NDISAC

The NDISAC will further broaden the ability for the DIB community and our critical supplier partners to develop and leverage threat and threat mitigation information and related best practice products, tools, and services. The NDISAC will be able to reach deeply into and broadly across our unique sector of industry and its interdependent interests. The NDISAC will also support and inform the DIB SCC policy coordination among industry and with the government departments and agencies relevant to the DIB.

The 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 DIB sector's critical infrastructure protection operational coordination mechanism.

Contact NDISAC Today!

National Defense ISAC
1050 Connecticut Ave NW #500
Washington, DC 20036

Email: info@ndisac.org
Phone: (202) 888-2724
Website: www.ndisac.org

Copyright© NDISAC 2019