National Defense ISAC

HISTORY OF NDISAC

Information Security and Analysis Center (ISAC) Background

In 1998 the White House published Presidential Decision Directive 63 (PDD-63),[1] 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[2] made a recommendation for the creation of mechanisms for information assurance and critical infrastructure protection coordination specifically focused on information and communications technology.[3]

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.[4] Launched in 1999, the Financial Services Information Sharing and Analysis Center was established by the Financial Services Sector, also in response to the 1998 Presidential Decision Directive. At the same time, 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.[5] The Defense Sector is one sector that evolved the NSIE model into the Defense Industrial Base Sector's equivalent organization, the Defense Security Information Exchange.

> ***The Defense Sector evolved the NSIE model into the Defense Industrial Base Sector's equivalent organization, the Defense Security Information Exchange.***

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, the term "Information Sharing and Analysis Organization (or ISAO) was codified in the Homeland Security Act of 2002, (Pub.L. 107–296, 116 Stat. 2135, enacted November 25, 2002). Within that statute, the term ISAO was defined in section 131(5)[6] as follows:

> *"…any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of—*
>
> *(A) gathering and analyzing critical infrastructure information in order to better understand security problems and interdependencies related to critical infrastructure and protected systems, so as to ensure the availability, integrity, and reliability thereof.*
>
> *(B) communicating or disclosing critical infrastructure information to help prevent, detect, mitigate, or recover from the effects of a[n] interference, compromise, or a[n] incapacitation problem related to critical infrastructure or protected systems; and*
>
> *(C) voluntarily disseminating critical infrastructure information to its members, State, local, and Federal Governments, or any other entities that may be of assistance in carrying out the purposes specified in subparagraphs (A) and (B)."*

Early in the following year (2003), the White House published Homeland Security Presidential Directive 7 (HSPD 7)[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)[8] 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

1 https://www.gpo.gov/fdsys/pkg/FR-1998-08-05/pdf/98-20865.pdf
2 https://www.dhs.gov/national-security-telecommunications-advisory-committee
3 https://www.dhs.gov/sites/default/files/publications/Information%20Infrastructure%20Group%20Report_1998.pdf
4 https://www.dhs.gov/sites/default/files/publications/NSTAC_08.pdf
5 https://www.dhs.gov/sites/default/files/publications/Information%20Infrastructure%20Group%20Report_1999.pdf
6 https://www.gpo.gov/fdsys/pkg/USCODE-2010-title6/pdf/USCODE-2010-title6-chap1-subchapII-partB-sec131.pdf
7 https://www.gpo.gov/fdsys/pkg/PPP-2003-book2/pdf/PPP-2003-book2-doc-pg1739.pdf
8 https://www.nationalisacs.org/about-nci

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 or "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 Department of Homeland Security. The role of ISACs was further refined in National policy with the Federal government's publication of the first National Infrastructure Protection Plan[9] 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 sector partnership model recognizes that not all CI/KR sectors have established ISACs. Each sector has the ability to implement a tailored information-sharing solution that may include ISACs; voluntary standards development organizations; or other mechanisms, such as trade associations, security organizations, and industry-wide or corporate operations centers, working in concert to expand the flow of knowledge exchange to all infrastructure owners and operators. Most ISACs are members of the ISAC Council, which provides the mechanism for the inter-sector sharing of operational information. Sectors that do not have ISACs per se use other mechanisms that participate in the HSIN and other CI/KR protection information-sharing arrangements. For the purposes of the NIPP, these operationally oriented groups are also referred to collectively as ISACs.*
>
> *ISACs vary greatly in composition (i.e., membership), scope (e.g., focus and coverage within a sector), and capabilities (e.g., 24/7 staffing and analytical capacity), as do the sectors they serve. As the sectors define and implement their unique information-sharing mechanisms for CI/KR protection, the ISACs will remain an important information-sharing mechanism for many sectors under the NIPP partnership model."*

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 Defense Industrial Base (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.

> ***The trust and value established over several years of members informal coordination and collaboration led to the 2007 creation and 2008 chartering of a DIB-specific information sharing and analysis mechanism, named DSIE.***

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 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. It was simply named DSIE (Defense Security Information Exchange), and maintained an organizational existence as an Industrial Working Group of the National Defense Industrial Association;[10] 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 in the District of Columbia 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 Defense Security Information Exchange. 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

9 https://www.dhs.gov/xlibrary/assets/NIPP_Plan_noApps.pdf
10 http://www.ndia.org/

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.

> ***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.***

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 other sectors that the defense industry depends upon and with whom we share common 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 such as our recent affiliation and partnership with the Chemical Sector ISAC.[11] These peering partnership are important, but the DIB sector must coordinate more broadly.

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.

> ***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.***

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 Sector Coordinating Council's policy coordination among industry and with the government departments and agencies relevant to the DIB.

About NDISAC

The 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. 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.

The NDISAC is the umbrella organization for DSIE, and maintains a scope that includes all-hazards threat sharing; industry-wide alerts, warning and notifications capabilities; the ability to pull together and sustain working groups across diverse subject matter

11 http://www.prnewswire.com/news-releases/center-for-exchanging-cyber-threat-information-expanded-300405414.html

HISTORY OF NDISAC

areas relevant to the DIB; and the ability to develop and provide information and services supporting DIB interests.

NDISAC is recognized nationally within the U.S. as the ISAC for the nation's defense industry critical infrastructure sector by the DIB Sector Coordinating Council, the US Department of Homeland Security, the FBI, and the National Council of ISACs.

NDISAC Membership Benefits

NDISAC members participate in a confidential community of industry leaders and security experts. Members gain access to a secure portal that enables anonymous information sharing, real-time cybersecurity intelligence reports and analysis, the latest government threat advisories and recommendations, DFARS compliance assistance, and facilitates live interaction among industry stakeholders. Members also engage in sector-specific committees and working groups, and participate in exercises and workshops.

NDISAC members receive trusted and timely expert information that increases sector-wide knowledge of physical and cyber security threats. Some of the many NDISAC membership benefits include:

- Access to all-hazards threat intelligence
- Secure peer-to-peer and community-to-community collaboration
- Mentoring relationships with mature security teams
- Shared services and resources
- Threat information
- Best practices
- DFARS compliance assistance
- Alerts, notifications and warnings on relevant threats to the industry
- Latest government threat advisories and recommendations
- Cyber security analyst training opportunities'
- Defense industry focused working groups
- Service offerings geared for DIB companies and their suppliers

Join NDISAC today!

Joining the NDISAC 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.

Contact Information

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

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