Defense Security Information Exchange (DSIE)
A partnership for the Defense Industrial Base

Background

In 2007, several members of the Network Security Information Exchange (NSIE) that were also defense contractors discussed the formation of a similar organization to be focused on the Defense Industrial Base. The NSIE was established in 1991 as a sub committee of the Network Security Telecommunication Advisory Committee (NSTAC), the Industry NSIE meets with their Government NSIE counterparts for sharing information on protection for the CI/KR of the Telecommunication industry. From this concept the DSIE was formed using a similar trust model developed among over 20 of the leading DIB companies. In February of 2008, the DSIE was formalized under the DIB Sector Coordinating Council as the Cyber Sub-Council. The members use their trust relationships to share intelligence on cyber related attacks. This sharing has enabled the industry partners to quickly alert others of any ongoing incident and share mitigation strategies for the protection of the DoD CIKR under their control.

Information Sharing Rules

The information sharing rules, modeled after those used in the NSIE are simple. All members and their companies have formally signed a Non-Disclosure agreement (NDA) that allows sharing on three levels:

- Non-attributional (All information)
- For DSIE eyes only, not to be shared outside the group
- Public Domain information

All information is considered non-attribution outside of the DSIE. There is also a level of sharing where the information itself can not be used outside of the DSIE as well as sharing information that is in the public domain. All sharing is by default non-attributional and can not be shared outside of the constraints of the DSIE without permission from the data owner.

DSIE Structure and Membership Responsibility

There are two subcommittees within the DSIE; one tactical, real time sharing of cyber events and a higher level strategic committee. The strategic committee represents the DIB SCC in their strategic goals and metrics related to cyber defense as dictated in the Sector Specific Plan. The overall mission of the DSIE is to protect the Key Resources and Critical Infrastructure of the DoD that are under the control of the DIB. Since the vast majority of the assets within the sector are controlled by the DIB contractor community, it is imperative that these assets are protected. The NIPP defines a multidirectional, networked information sharing process that is followed by the DSIE. The sharing is both vertical and horizontal across companies within the DIB. As a sub council of the DIB SCC, the DSIE attends the joint CIPAC meetings with the DIB Government Coordinating Council where we partner on providing strategic direction through the development of the Sector Specific Plan. Strategic committee members of the DSIE represent the DIB in several joint cyber committees such as the Cross Sector Cyber Security Working Group and the annual CIPAC Plenary sessions.

The DSIE also holds bi-monthly meetings where all members share information relating to the areas impacting their specific company cyber concerns. This sharing is done at a non-attribution level. Such sharing helps all companies within the DSIE to better strengthen their cyber security posture. All members are required to be able to attain a minimum of a secret level clearance to enable future classified briefings when needed. The future goal of the DSIE is to expand membership in the tactical information sharing committee to include all DIB members whose responsibility includes protection of the cyber CIKR of the DoD. We will continue working within the DIB SCC/GCC structure for future partnering with the DoD, our Sector Specific Agency (SSA).

Summary

The success of the DSIE has been the result of establishing the trust model used by the NSIE for so many years. The trust began within several closely held networks involving personal relationships between cyber forensic personnel at the various companies. With this as a backbone, the DSIE rapidly gained acceptance as more of the information sharing continued without an incident or breach of confidentiality. In today's expanding and persistent threat environment, it is important to build on these successful sharing models to combat attackers. All information sharing is done voluntarily within the confines of the NDA. The success of the DSIE is also the ability to use established tools and techniques for the rapid and effective sharing of threats and attack vectors. It is not uncommon for information to be shared with the entire membership within minutes. The DSIE will continue to expand membership through the DIB SCC structure following the guidelines from the NIPP. As the DIB GCC seeks to engage a similar organization, the DSIE will be able to begin sharing information through the CIPAC process with members of that organization. The DSIE is also working with the UK Aerospace Defense Manufacturing Exchange for future sharing between the US and the UK defense industries. The DSIE has now expanded to include over 28 companies that share information daily. The success and the strength of the DSIE process is due to the dedication of the individual members. Their commitment to this effort has been extraordinary. Through their continued support, they have made the DSIE, their organization, what it is today.