



Information Sharing and Analysis Organization (ISAO) Standards Organization

Online Public Forum

26 JANUARY 2017

A secure and resilient Nation – connected, informed and empowered.



 @ISAO_SO
 www.isao.org
 [Inked.in/ISAO_SO](https://www.linkedin.com/company/isao-so)

Agenda



- Why We're Here
- DIB ISAO Case Study
- 2016 Year in Review
- Future Documents
- Call for Participants: Analysis Working Group
- Growing the Community
- Building Capability
- Questions & Answers

Why We're Here



“The cyber threat is one of the most serious economic and national security challenges we face as a Nation.”

President Barack Obama, March 2010

Mission: Improve the Nation’s cybersecurity posture by identifying standards and guidelines for robust and effective information sharing and analysis related to cybersecurity risks, incidents and best practices.

Vision: A more secure and resilient Nation that is connected, informed and empowered.

Defense Industrial Base Information Sharing and Analysis Organization

An ISAO Case Study:

Who are we, how did we get here, and where did we come from?

Defense Security Information Exchange

Carlos P. Kizzee, Executive Director



Unique History

- February 19, 2008 - Defense Security Information Exchange established.
 - 5 Defense Industrial Base (DIB) founding members.
 - Now 75 members; most but not exclusively DIB.
 - Enables secure threat information sharing and collaboration.
 - Cyber Sub-Council of the DIB Sector Coordinating Council.
 - Legacy cyber security center of excellence for the DIB.
 - Key partner of Department of Defense Cyber Crime Center (DC3).
- March 10, 2014 - DIB Information Sharing and Analysis Organization created (doing business as DSIE).
 - Incorporated as 501(c)(6) non-profit organization.
 - Retaining DSIE trade name and activities (doing business as).
 - Developing additional capabilities and services for DIB and their suppliers.

Unique Culture

- DSIE is the DIB's Legacy Cyber Center of Excellence providing:
 - An almost 10 year history of DIB companies working together to mature a mutual understanding of current and emerging threats.
 - Collective analysis and collaboration of threats, solutions, tools, processes, resources, and threat detection and mitigation strategies.
 - A unique trust model producing the highest-quality threat sharing in industry.
 - Active and candid collaboration yielding high confidence in shared data.

Center of excellence
for high quality
cyber threat
collaboration

- The DSIE organizational collaborative model is relatively unique, in that most if not all organizational threat information sharing and collaborative coordination is done with full attribution among the participant DSIE members. This unique trust model fosters greater collaboration and provides a reliability in the source of data shared that enables that data to be rapidly actioned upon with confidence.
- The dialogue and activities of member companies within the collective DSIE operating environment is a core DSIE capability valued by all. Analysts engage in open threat information dialogue that is visible to any member across forum and discussion thread spaces.
- This ongoing analytical collaborative dialogue is constantly being updated with the sharing of additional knowledge, context, and the results of ongoing research across the environment among analysts who are detecting, researching, and mitigating threats to our company networks and systems and leveraging the portal as a clearinghouse for data as well as a point of collaboration about that data.

**Reduce risk through
continuous improvement
of member intelligence
and analytic capabilities**

- DSIE members, work together to discuss and mature one another's understanding of key contemporary threats.
- They explore tools, resources, and strategies that are most effective in the detection and mitigation of threat activity.
- This unique candor promotes a “member-helping-member” environment where companies are continually improving their enterprise capabilities and reducing risk based on effective practices shared by and valuable lessons learned from others.

**Jointly developing
and leveraging
common platforms
and services**

- That trust extends to Members working together in concert across multiple working groups with numerous work stream efforts in order to identify, develop, test, and implement common solutions across the membership; addressing common problems and ensuring collective effort leads to mutual benefit.
- Whether the topic of member engagement is threat sharing, collaboration, or coordination around solution development; the member interaction occurs with the confidence that nothing shared, including the originator source of data or the information itself, is attributed beyond the trusted environment.

Our Future

- DSIE organizational intent and activities have matured significantly since the initial 2006 vision of a DIB collaborative environment. Our DSIE today is focused on fostering continuous cyber security maturity for member companies within the Defense Industrial Base, our extended supply chain, and other mature generators of high quality threat intelligence from other sectors of industry. We are continuing to accomplish this through collaboration, mentoring, and the development and provision of relevant products, tools, and services.
- While our DSIE organizational scope, breadth, and activities continue to mature to suit our requirements as members; maintaining a trusted collaborative environment for our sharing of high-quality threat intelligence is and will remain our core and most valued product.



Member Engagement
Defense Security Information Exchange
(202) 888-2724 Ext. 1
MemberAdmin@dsie.org

Questions and Answers



Please use the Question and Answers box in the GoToWebinar Control Panel to submit questions for Mr. Kizzee

ISAO SO Year in Review



- We've fostered a community and made good progress in our first year, but. . .
- We're not done yet! See our report at www.ISAO.org



PUBLIC OUTREACH

2016 SPEAKING ENGAGEMENTS

- FS-ISAC Fall Summit
- Cross-Sector Leadership Forum
- Defense Transportation Fall Conference
- Midwest Cyber Center
- MS-ISAC Annual Meeting
- IT and Communications Sector Annual Meeting
- San Antonio Cyber Committee Cyber Southwest

Social Media Web Growth
ISAO.ORG INCREASED IN PAGE VIEWS AND UNIQUE VISITS EVERY 3-MONTH PERIOD OF 2016
TOTAL PAGE VIEWS **45,546** TOTAL USERS **7,571**
9X increase in the 3rd quarter of 2016
250+ followers on Twitter
100,000+ views on YouTube

In the News

FEATURED IN OVER 35 PUBLICATIONS IN YEAR 1



GROWING AND SUPPORTING THE ECOSYSTEM

VOLUNTARY CONSENSUS STANDARDS DEVELOPMENT

One major tenet of the ISAO SO is to foster the development and growth of ISAOs by creating, curating, and disseminating resources in a single location. We aim to equip new, emerging and established ISAOs with additional resources they need to succeed. By serving as a community hub, the ISAO SO is able to host critical resource documents and facilitate important conversations between community members.

RESOURCE LIBRARY

The Resource Library is a hub for members of the information sharing community to find guidelines, tools, templates, checklists, professional associations, and other resources to support information sharing and analysis.

ISAO REGISTRY

In September 2016, the ISAO SO launched a National Registry of ISAOs for new and established ISAOs. As the ISAO ecosystem grows, the registry will serve as a centralized location to find information regarding existing and emerging organizations.

ISAO ROUNDTABLES

The ISAO SO has hosted five online roundtables for new and emerging ISAOs in 2016. These monthly online discussions are designed to provide a platform for new and emerging ISAOs to share ideas, present challenges and discuss solutions.



INFORMATION SHARING COMMUNITY

CREATING A COMMUNITY

In its first year, the ISAO SO promoted collaboration across the entire information sharing community to create initial voluntary guidelines. The ISAO SO has prioritized bringing together a diverse community of experts to contribute to the common goal of improving the Nation's cybersecurity posture.



Future Documents



- Next voluntary guideline topics approved for development:
 - Governance FAQs for an ISAO **WG1**
 - State, Local, Territorial, Tribal, and Regional Considerations **WG6**
 - Introduction to ISAO Capabilities and Services **WG2**
 - Automated Information Sharing Methods **WG3**
 - Intro to Privacy and Security **WG4**
 - Common Considerations and FAQ's for General Counsels' for ISAOs **WG4**
 - Intro to Analysis **(New Working Group Forming)**

Evolving the Community Body of Knowledge

Call for Volunteers: Analysis Working Group



- We're seeking industry and government volunteers to help shape documents and products related to *Information Sharing Analysis*
- The Analysis Working Group will be focused on developing documents to address these and other issues:
 - Define the ability of an ISAO to perform analysis on member information that is shared within the ISAO and on information shared from external sources.
 - Some ISAOs will have strong analytical capabilities but others likely will be limited to sharing and will lack analysis capabilities. Define a process that will accommodate this disparity.
 - Prescribe the level of analysis (e.g. network traffic, malware, mitigation action) to be done by ISAOs.
 - Introductory and Intermediate Analysis guidelines for new, emerging and established ISAOs
- Apply to be part of Working Group 7 Leadership (Chair, Vice-Chair), a core development team, and general members on ISAO.org

Building the Community



- Spreading the Word to Promote Information Sharing
 - FS-ISAC Fall Summit
 - Cross-Sector Leadership Forum
 - Defense Transportation Fall Conf
 - Midwest Cyber Center
 - MS-ISAC Annual Meeting
 - IT and Comm Sector Annual Meeting
 - San Antonio Cyber Committee
 - Cyber Southwest
- Developing Venues for Online and Face-to-Face Interaction





The ISAO SO is on the road...come see us at RSA!
North Expo Hall, Booth #4436

ISAO SO Breakout Meeting
Wednesday, February 15 at 2pm
Nob Hill A - Marriott Marquis SF



Reaching Out to Grow the Community

International Information Sharing Conference



Fall 2017 in the National Capital Region

- ISAOs
- Service Providers
- Training Sessions
- Call for Ideas
 - Papers
 - Demos
 - Speakers



Bringing the Community Together

New and Emerging ISAOs Roundtable



- Open to new and emerging ISAOs
- Opportunity to share knowledge and ask questions
- Register your ISAO on [ISAO.org](https://www.isao.org) to participate in Roundtable discussions
- February date and time TBD

Building Capability and Capacity

Mark Your Calendars



- Online public meeting February 23rd at 1pm Central Time
- Information sharing insights, updates from the ISAO SO, and your chance to engage with the community

February 2017 						
Su	Mo	Tu	We	Th	Fr	Sa
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28				

Ongoing Engagement

Questions and Answers



Please use the Question and Answers box in your GoToWebinar Control Panel to submit questions to the ISAO SO.

Thanks for joining our online meeting today!