



ISAO Standards Organization

Improving the Nation's Cybersecurity Posture



YEAR IN REVIEW

2016





PROMOTING CYBERSECURITY INFORMATION SHARING

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

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

A LETTER FROM THE EXECUTIVE DIRECTOR

The past year has represented several giant steps forward for the Information Sharing and Analysis Organization (ISAO) Standards Organization (SO) and the information sharing community at large.

While cybersecurity information sharing has been a topic of discussion for well over a decade, the creation of a new type of information sharing organization, the ISAO, began two years ago. In February 2015, Executive Order 13691 established the need for the ISAO SO and tasked it to develop voluntary standards or guidelines to "further the goal of creating robust information sharing related to cybersecurity risks and incidents with ISAOs and among ISAOs to create

deeper and broader networks of information sharing nationally, and to foster the development and adoption of automated mechanisms for the sharing of information."

In October 2015, the U.S. Department of Homeland Security selected a team led by The University of Texas at San Antonio with support from LMI and the Retail Cyber Intelligence Sharing Center (R-CISC) as its ISAO SO.

This Year-in-Review publication represents the work of the entire community since October 2015. We're gratified to reflect on the support of over 160 working group members, the registration of 47 information sharing organizations, dynamic exchanges at four in-

person public forums, the publication of four voluntary guideline documents, and a strategic roadmap ahead for 2017.

I want to thank the entire community for their contributions to the success of the ISAO project. This work would not be possible without the tireless contributions of our leadership team, the working groups, the Department of Homeland Security, and members of the public.

We are pleased to celebrate the progress, but recognize the challenge of the work to be done in 2017. We continue to seek to improve the Nation's cybersecurity posture by identifying standards, guidelines, and the other products needed for robust and effective information sharing and analysis related to cybersecurity risks, incidents, and best practices.

Working together, we will create a more secure and resilient information sharing community that is connected, informed, and empowered.

Sincerely,

Gregory B. White, Ph.D.
Executive Director
ISAO Standards Organization



INFORMATION SHARING COMMUNITY

CREATING A COMMUNITY

The ISAO SO was tasked to 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. In its first year, the ISAO SO promoted collaboration across the entire information sharing community to create initial voluntary guidelines. Our process has remained consistent: our working groups use a transparent consensus-driven standards development process to synthesize the best inputs from diverse community stakeholders and the public. 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.

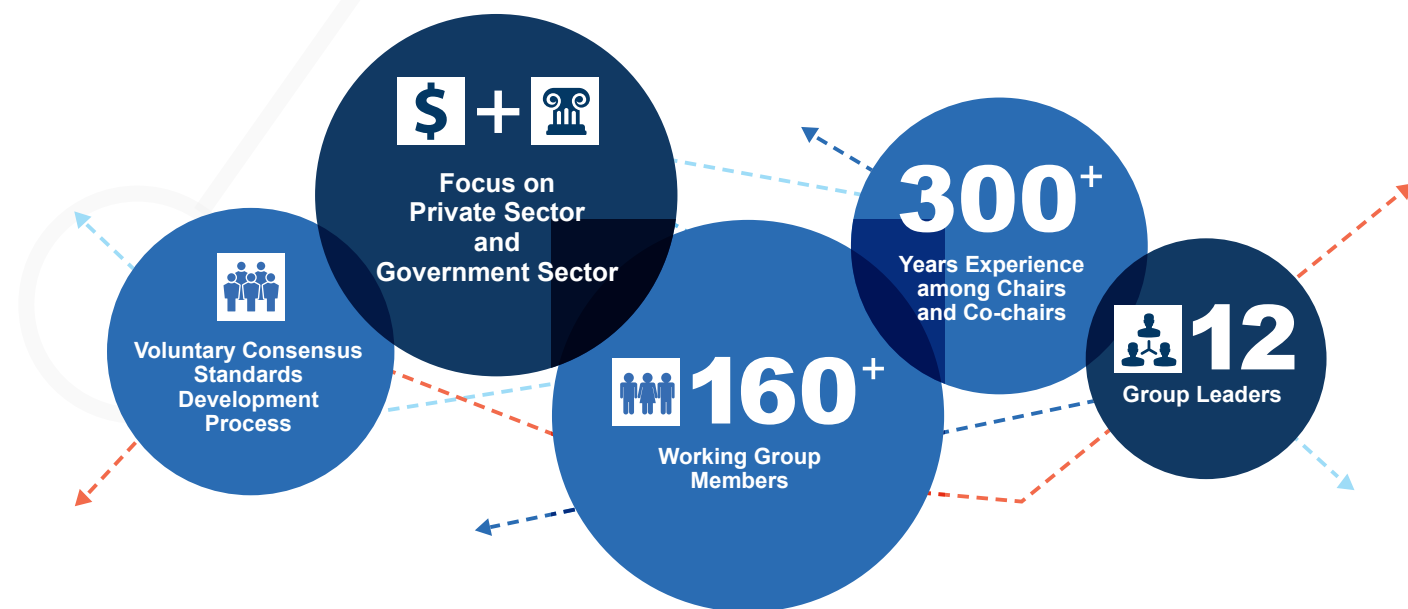
WHO IS IN THE INFORMATION SHARING ECOSYSTEM?

The Information Sharing Ecosystem is a diverse community consisting of government agencies, fusion centers, commercial for-profit and non-profit entities, and public and private sharing organizations, along with their members, vendors, and affiliates.

DIGEST OF INFORMATION SHARING ORGANIZATIONS REGISTERED IN 2016



“THE ISAO SO HAS WELCOMED INPUT FROM ALL PARTICIPANTS—ACADEMIA, GOVERNMENT, INDUSTRY, AND MEMBERS OF THE PUBLIC.”



“PUBLIC FEEDBACK AND COLLABORATION CONTINUES TO BE THE CORNERSTONE OF OUR WORK TO IMPROVE THE NATION’S CYBERSECURITY POSTURE.”

—DR. GREGORY B. WHITE,
EXECUTIVE DIRECTOR, ISAO SO

WORKING GROUP OVERVIEW

WORKING GROUPS

Based on input from our first public forum, the ISAO SO established six initial working groups (WG) to facilitate open dialog about ISAOs and information sharing.

WG 1: ISAO CREATION

Working Group 1 identified and captured the elements necessary for an interested organization to stand up an ISAO. These elements serve as the basis for creating an ISAO and have enough flexibility in design to fit the needs of diverse interested organizations.

WG 2: ISAO CAPABILITIES

Working Group 2 identified and captured the capabilities necessary for an interested organization to effectively operate an ISAO. These capabilities support day-to-day operation of the ISAO and support the ISAOs main function: to share, receive and analyze cyber information in a timely and effective manner. The identified capabilities must allow for the most basic ISAO and also support more sophisticated organizations.

WG 3: INFORMATION SHARING

Working Group 3 developed the introductory guidance necessary for an interested organization to effectively share cyber threat indicators, vulnerabilities, and best practices within an ISAO or externally.

WG 4: PRIVACY AND SECURITY

Working Group 4 identified and captured the basic steps to safeguard information (both proprietary and privacy related). This group also addressed the processes and procedures required to prevent unauthorized release or access to information not cleared for release, and how to meet federal, state, local, and tribal laws regarding privacy.

WG 5: ISAO SUPPORT

Working Group 5 was a group of individuals familiar with the creation and operation of information sharing organizations who worked to develop processes and tools to support emerging ISAOs as they were created. This working group worked closely with the ISAO SO to provide assistance to emerging ISAOs.

WG 6: GOVERNMENT RELATIONS

Working Group 6 identified and addressed issues associated with ISAO interactions with the intelligence community, law enforcement, US regulators, and Homeland Security.

THE POWER OF ISAOs

The ISAO construct is powerful because of its potential to widely and rapidly propagate critical cybersecurity threat and incident response information across numerous communities of interest that are currently underserved from a cybersecurity perspective.

COMMUNITY SUCCESS STORIES

- The Legal Services ISAO has attracted over 100 members in its first year.
- The Sports ISAO actively supported the 2016 Summer Olympics in Rio de Janeiro.
- The Arizona Cyber Threat Response Alliance improved member resilience through participation in the annual national Cyber Guard exercise.



COLLABORATION

WORKING TO IMPROVE THE CYBERSECURITY POSTURE OF THE NATION

The ISAO SO facilitated meetings, forums, and roundtables through the past year to increase dialogue and grow the community:

- 11 Public Online Meetings
- 4 In-Person Public Forums
- 2 Public Request-for-Comment Periods
- Bi-Weekly Leadership Calls



The ISAO SO hosted four In-Person Public Forums since November 2015. The first meeting in Tysons, Virginia, focused on community building and establishing values. The community came together again in February 2016, as the focus shifted to document conception and working group meetings. The third public forum was hosted in May 2016 in Anaheim with a focus on document development. The year came to a close in Tysons, as the conversation turned to the way ahead. These meetings provided critical opportunities for public feedback and dialogue on the development of information sharing standards and guidelines.



DOCUMENT DEVELOPMENT

The ISAO SO working groups consist of over 160 professionals providing feedback and input into the creation of the ISAO series documents. Working groups have been established to develop specific guidelines for the creation and functioning of ISAOs.

The ISAO SO developed a voluntary consensus standards development process that leveraged industry, government, and academic expertise through public working groups. This consensus-based process was the foundation of all conversations and document production. Working groups released documents in two request-for-comment periods. After these comments were received, working group members reviewed and adjudicated each comment to improve the document. The adjudication of these comments was made available on ISAO.org to increase transparency. In the first year of the ISAO SO, working groups regularly met to discuss documents and produce materials for publication. This work continues into year two as seven documents are currently under development.

2016 PUBLISHED PRODUCTS ON ISAO.ORG

- ISAO 100-1: Introduction to ISAOs
- ISAO 100-2: Guidelines for Establishing an ISAO
- ISAO 300-1: Introduction to Information Sharing
- ISAO 600-2: U.S. Government Relations, Programs & Services



DOCUMENTS CURRENTLY UNDER DEVELOPMENT IN 2017

The ISAO SO is committed to building an evolving community of knowledge. Working groups have begun development on future documents following the publication of the four initial guideline documents in 2016. Based on feedback from a public survey, the ISAO SO has identified the topics below for development in 2017.

Frequently Asked Questions for Governance of an ISAO

A publication designed to provide answers to the most needed and urgent questions for ISAO governance

Introduction to Capabilities and Services

A mid-level discussion of the capabilities and services that an ISAO could provide to its membership

Automated Information Sharing

A mid-level technical discussion of automated information sharing and its impact on the ecosystem

Introduction to Privacy and Security

Common practices to advance privacy and security in private sector information sharing

Common Considerations and Frequently Asked Questions for General Counsels for ISAOs

An introductory to mid-level discussion of the legal FAQs and considerations that arise in forming/operating an ISAO

Introduction to Analysis

A mid-level discussion of information sharing analysis

State, Local, Tribal, Territorial, and Regional Considerations

Explores the issues for sharing information with governmental organizations at the state, local, tribal, territorial, and regional levels



GROWING AND EQUIPPING THE COMMUNITY

PROVIDING THE TOOLS NEEDED TO LEARN AND COLLABORATE



The ISAO SO is dedicated to fostering the growth and development of the information sharing community by making practical “how to” information readily available and facilitating interactions among community members.

The ISAO SO has launched several initiatives to grow and support the information sharing community in our first year.

Resource Library

The Resource Library is a hub for members of the information sharing ecosystem and the general public to find guidelines, tools, templates, checklists, professional associations, and other resources to support cybersecurity information sharing and analysis. The library is a living and breathing repository of knowledge and resources. Over 50 resources and tools have been included in the Resource Library in the first quarter of use. The library continues to grow and evolve

as the needs for ISAOs are identified.

National Registry of ISAOs

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 Roundtable Discussions

The ISAO SO has hosted five online roundtable discussions 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 with peers, present challenges and discuss solutions, and to highlight resources, tools and training opportunities for the community.

International Information Sharing Conference

The ISAO SO will host its inaugural International Information Sharing Conference in Fall 2017. The event will bring together current and prospective information sharing organizations, vendors, members, and industry leaders for two days in the National Capital Region.


PUBLIC OUTREACH

ENGAGING STAKEHOLDERS AND THE PUBLIC TO PROMOTE ISAOs AND INFORMATION SHARING

2016 Speaking Engagement Highlights:

- 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

 **9X** Impressions have increased in the 2nd half of 2016

250 Followers interact with the ISAO SO account

100,000 Over 100,000 impressions in 2016

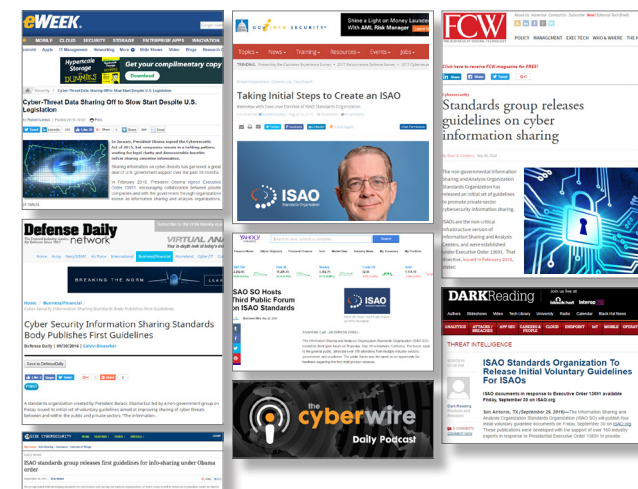
Web Growth

ISAO.ORG INCREASED IN PAGE VIEWS AND UNIQUE VISITS EVERY 3-MONTH PERIOD OF 2016

TOTAL PAGE VIEWS **45,546** TOTAL USERS **7,571**

In the News

FEATURED IN OVER 35 PUBLICATIONS IN YEAR 1



ABOUT US

The Center for Infrastructure Assurance and Security (CIAS) at The University of Texas at San Antonio (UTSA), LMI, and the Retail Cyber Intelligence Sharing Center (R-CISC) form the ISAO Standards Organization. The team brings experience in both cybersecurity and standards development.



VISIT US
www.ISAO.org

FOLLOW US
[@isao_so](https://twitter.com/isao_so) | [in](https://www.linkedin.com/company/isao-so/)

CONTACT US
Contact@isao.org



UTSA has a national reputation for innovation in cybersecurity programs, exercises, competitions, and training, especially with sectors, states, and communities.

LMI is a mission-oriented consulting firm with 55 years of public service, including developing open standards, engaging communities, and building trust among competitors.

R-CISC operates the Retail Information Sharing and Analysis Center, and effectively promotes cybersecurity and data privacy for the \$500 billion retail/services industry.

