ISAO Standards Organization

ISAO 100-1: Introduction to Information Sharing and Analysis Organizations (ISAOs)

v1.01

October 14, 2016

ISAO 100-1

Introduction to Information Sharing and Analysis Organizations (ISAOs)

v1.01
ISAO Standards Organization
October 14, 2016

Acknowledgements

This publication was developed by the Information Sharing and Analysis Organization Standards Organization (ISAO SO) with representatives from industry, government, and academia in an ongoing effort to produce a unified voluntary set of guidelines and guidance for information sharing. The ISAO SO and the Working Group leadership are listed below.

ISAO Standards Organization

Gregory B. White, Ph.D.
ISAO SO—Executive Director
Director, Center for Infrastructure Assurance and Security, UTSA

Richard Lipsey
ISAO SO—Deputy Director
Senior Strategic Cyber Lead, LMI

Brian Engle
Executive Director
Retail Cyber Intelligence Sharing Center

Working Group One—ISAO Creation

Frank Grimmelmann
President & CEO
Arizona Cyber Threat Response Alliance (ACTRA)

Deborah Kobza
President & CEO
Global Institute for Cybersecurity & Research

Working Group Two—ISAO Services and Capabilities

Denise Anderson
President
National Health Information Sharing & Analysis Center
Chair, National Council of ISACs (NCI)

Fred Hintermister
Manager
Electricity Information Sharing and Analysis Center
North American Reliability Corporation
Vice Chair, National Council of ISACs (NCI)

Working Group Three—Information Sharing

Kent Landfield
Director, Standards and Technology Policy
Intel Corporation

Michael Darling
Director, Cybersecurity and Privacy
PwC

Working Group Four—Privacy and Security

Rick Howard
Chief Security Officer
Palo Alto Networks

David Turetsky
Partner
Akin Gump Strauss Hauer & Feld LLP

Working Group Five—ISAO Support

Carlos Kizzee
Executive Director
Defense Security Information Sharing Exchange

Alex Crowther
Director of Research
Center for Technology and National Security Policy
National Defense University

Working Group Six—Government Relations

Doug DePeppe
Founder
***eos**edge Legal*

David Weinstein
Chief Technology Officer
State of New Jersey

The ISAO SO leadership would also like to acknowledge those individuals who contributed significantly in the development of these guidelines:

Scott Algeier of IT-ISAC, Jon Baker of The MITRE Corporation, Adam Buteux of PWC, Roger Callahan of FS-ISAC, Meeta Sidhu of Price Waterhouse Coopers, and Bobbie Stempfley of The MITRE Corporation.

Special thanks from the authors goes to the ISAO SO Advisors and staff who helped greatly along the way in the development of this document. Brad Howard, Daniel Knight, James Navarro, Chris Rutherford, Larry Sjelin and, Natalie Sjelin.

Revision Updates

Item	Version	Description	Date
1	1.0	Initial Publication	September 30, 2016
2	1.01	Editorial Update/Corrections	October 14, 2016

Table of Contents

1 EXECUTIVE SUMMARY

This document serves as an introduction to the topic of Information Sharing and Analysis Organizations (ISAOs) and to the series of documents developed to assist newly forming ISAOs.

The establishment of ISAOs allows communities of interest to share cyber threat information with each other on a voluntary basis and to then analyze the shared information to provide guidance or assistance to ISAO members. The goal is to create deeper and broader networks of information sharing to elevate the security of the nation and those entities participating in ISAOs.

2 INTRODUCTION

The importance of information sharing to data security has been discussed for well over a decade. Early realization of its importance led to the creation of Information Sharing and Analysis Centers (ISACs) for critical U.S. infrastructures to ensure the protection of information systems and the physical assets supporting them. While this was an important step toward establishing a system for sharing information related to cybersecurity, the majority of organizations in government and industry are not part of a critical infrastructure. In February 2015, the White House issued Executive Order (EO) 13691, “Promoting Private Sector Cybersecurity Information Sharing,” which called for the Secretary of the Department of Homeland Security (DHS) to “strongly encourage the development and formation of Information Sharing and Analysis Organizations.” This EO acknowledged that broader information sharing (beyond critical infrastructures) was needed to better protect the nation from cyber incidents. These new entities could be “organized on the basis of sector, subsector, region, or any other affinity,” greatly expanding the number and type of potential information sharing organizations developed to meet the goal of a more comprehensive information sharing environment.

Additionally demonstrating the increased interest in cybersecurity information sharing, Congress passed the Cybersecurity Information Sharing Act (CISA) in December 2015. While not directly tied to the ISAO initiative, CISA nonetheless has helped to raise public awareness of cybersecurity information sharing.

To help with the establishment of ISAOs, EO 13691 directed DHS to “enter into an agreement with a nongovernmental organization to serve as the ISAO Standards Organization.” The ISAO Standards Organization (SO), in turn, established a number of working groups made up of leading information security community professionals to address specific areas pertinent to creating or operating ISAOs. When developing the various documents, the working groups considered the two primary functions important to ISAOs: the sharing of cybersecurity information and the analysis of the shared information. The purpose of these efforts is ultimately to improve the ability of organizations to, as outlined in the EO, “detect, investigate, prevent, and respond to cyber threats” while protecting the privacy and civil liberties of citizens.

Diverse communities of interest require a flexible and scalable framework tailored to meet the unique needs of each constituent group while remaining grounded in a shared set of principles. Accordingly, ISAOs will vary in terms of size, objectives, and capabilities. Both commercial and not-for-profit entities have been (and will be) formed to provide services to ISAOs or to become ISAOs themselves. Some ISAOs may be formed informally and may have little or no desire to collect and analyze information in near-real-time for its members. Other ISAOs may be highly interested in near-real-time analysis and dissemination of actionable information to better protect their members and may have a goal to help respond to security incidents affecting their members. Which type of ISAO is formed and what services it offers will be decided by its members to address their needs and their cyber risk management objectives. Specific capabilities may also be required before sharing cybersecurity information with certain government agencies or industry organizations. While not part of the reason for sharing information, establishing ISAOs may have the additional benefit of spurring innovation and the creation of new services and techniques to assist in the goal of securing the nation and, especially, the digital economy.

An ISAO may initially form with limited objectives and target capabilities but then transform over time to meet the changing needs of its members by modifying its objectives and supporting services. For example, an ISAO may initially be created to simply share cybersecurity-related information among security professionals in its member organizations; then increase the type and frequency of information it shares, and add more robust capabilities to analyze shared information to better detect and prevent cybersecurity attacks; and then ultimately add a 24/7 operational capability to assist its members with ongoing cybersecurity incidents. Conversely, an ISAO may elect to maintain narrowly focused capabilities to best serve the needs and capabilities of its members. The goal of the ISAO SO is to be as inclusive as possible in finding a place for an individual or organization wishing to be part of the overall information sharing effort.

The guidelines for the ISAO 100 Series, “Establishment and Operation of ISAOs,” take into consideration the different types of ISAOs that may be formed and the capabilities each may incorporate. Collectively, they present an organized approach to the various topics pertinent to ISAOs while considering the immediate needs of emerging ISAOs.

3 WHAT IS AN ISAO?

A common and natural question continually arising is, “What is an ISAO?” There have been various definitions published with slight variations between them. The primary characteristic of an ISAO in the cybersecurity information sharing ecosystem is that the ISAO analyzes and shares information related to cybersecurity risks and incidents between and among its membership. This holds true across a wide range of ISAOs with varying constituent membership organizations, regardless of whether they are affiliated with a critical infrastructure. The definition often referenced in the United States is found in 6 U.S.C. §131(5) and reads as follows:

> The term “Information Sharing and Analysis Organization” means 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, including information related to cybersecurity risks and incidents, in order to better understand security problems and interdependencies related to critical infrastructure, including cybersecurity risks and incidents, and protected systems, so as to ensure the availability, integrity, and reliability thereof;
>
> (B) communicating or disclosing critical infrastructure information, including cybersecurity risks and incidents, to help prevent, detect, mitigate, or recover from the effects of a interference, compromise, or a incapacitation problem related to critical infrastructure, including cybersecurity risks and incidents, or protected systems; and
>
> (C) voluntarily disseminating critical infrastructure information, including cybersecurity risks and incidents, 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).

Despite the statute’s language on critical infrastructure information, ISAOs are important to the cybersecurity information sharing ecosystem because they enable the analysis and sharing of information related to cybersecurity risks and incidents between and among members or customers, which may or may not be affiliated with a critical infrastructure.   It is clear from reading EO 13691 that there is a recognition that ISAOs will be formed in sectors and communities not directly tied to any critical infrastructure. For the ecosystem to flourish, it will include ISAOs that may not exchange information with a critical infrastructure.

4 VALUE PROPOSITION

Fundamental to the establishment of an ISAO is the “value proposition” offered to its participants, members, and collaborators. An ISAO must provide a tangible benefit for it to attract and enroll members. ISAOs offer a number of benefits to their members and other ISAOs, including the following:

- ISAOs provide an informative set of cybersecurity threat information and operational practices to help individual members be more secure.
- ISAOs help establish and maintain trust relations among members by establishing a framework of common, shared values and expectations.
- Members enhance their situational awareness and knowledge about how to protect themselves from, detect, and react to cyber-attacks.
- By aggregating information from multiple organizations, ISAOs can present a richer picture of malicious activity taking place within a specific sector, a geographic region, the nation, or the world. Member organizations can use this

enriched information to improve their individual and collective security, blocking attacks they would not have seen otherwise.

- ISAO members can exchange and then carry out effective and timely responses when they discover cybersecurity incidents, attacks, or unauthorized intrusions.
- ISAOs whose members share non-incident information such as best practices, training opportunities, processes and procedures, and product information can help enhance a member's security program.
- ISAOs result in lower costs and barriers of entry for cybersecurity information sharing.

5 THE INFORMATION SHARING ECOSYSTEM

The public-private partnership established by government and industry to meet the needs of critical infrastructures has made significant progress in improving the nation's cybersecurity posture. Additionally, commercial entities have emerged that provide a number of useful cybersecurity services on the open market. Nevertheless, an expanded cybersecurity information sharing landscape is envisioned to include many more ISAOs to join the group of existing ISAOs and ISACs. Collaboration among entities within this ecosystem will improve the efforts of those tasked with managing cybersecurity risks. EO 13691 clearly lays out the challenges addressed by the creation of a network of ISAOs. It states:

> In order to address cyber threats to public health and safety, national security, and economic security of the United States, private companies, nonprofit organizations, executive departments and agencies, and other entities must be able to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible.
>
> Organizations engaged in the sharing of information related to cybersecurity risks and incidents play an invaluable role in the collective cybersecurity of the United States. The purpose of this effort is to encourage the voluntary formation of such organizations, to establish mechanisms to continually improve the capabilities and functions of these organizations, and to better allow these organizations to partner with the Federal Government on a voluntary basis.
>
> Such information sharing must be conducted in a manner that protects the privacy and civil liberties of individuals, that preserves business confidentiality, that safeguards the information being shared, and that protects the ability of the Government to detect, investigate, prevent, and respond to cyber threats to the public health and safety, national security, and economic security of the United States.

Addressing these challenges effectively will require more than just establishing a number of disparate information sharing organizations. It will require a coordinated effort that effectively identifies and considers the existence and ongoing formation of ISAOs to understand where information sharing is occurring and its impact. Additionally, it will require considering how the efforts of individual ISAOs can be combined into a voluntary, trusted information sharing network fitting into a much larger cybersecurity information sharing ecosystem.

While ISAOs (including ISACs) will make up a significant portion of the cybersecurity information sharing ecosystem, there are many other potential information sharing entities to be considered and planned for in the ecosystem. This is why the ecosystem is not referred to as simply the ISAO ecosystem. Ultimately the goal is to allow any entity willing to share information for the purpose of enhancing the nation's security posture to be part of the ecosystem. To fully understand the scope of the ecosystem requires an examination of the various ways entities could become part of it.

5.1 INDUSTRY AND GEOGRAPHIC ISAOS

It is common for ISAOs to be formed around a specific industry or sector. The members will determine what services and capabilities the ISAO will offer. A common thread linking them together is the business they are involved in. The industry ISAO may have an international reach, it may be national in scope, or it may have a regional or local focus—depending on the goals and desires of its members. Examples might include an electronic gaming industry ISAO or a shoe industry ISAO. The information shared will be related to threats to this industry or sector and may also include information pertaining to common systems and applications frequently used by members of the ISAO.

There has been increased interest in ISAOs to meet the needs of a geographic region such as a city or state. Members in this case will include organizations residing within the boundaries of the geographic region covered by the ISAO. As a result, members may come from many different sectors and industries as well as government entities residing within the geographic region. The purpose of the ISAO would be to address issues common to the organizations residing within the boundaries of the ISAO's area. Facilitating face-to-face interactions within a geographic community can also help establish trust relationships. Because membership in an ISAO based on a geographic region will include entities from many different industries or sectors, it will likely contain entities that are members of another ISAO. This interweaving of ISAO coverage, if done correctly, could enhance the effectiveness of the overall ecosystem.

5.2 OVERLAPPING ISAOS

The overlapping of ISAOs as a result of membership in both industry and geographic ISAOs will not be the only instance of entities having membership in multiple ISAOs. Another possibility is overlapping that results from varying scopes of geographic ISAOs in a specific industry or sector. To illustrate, using the example of the shoe industry ISAO mentioned earlier, there may be a national shoe industry ISAO but also a Western States shoe ISAO and even a Texas State shoe ISAO. The reason for the overlapping ISAOs is not to duplicate efforts but rather to address issues that might not be applicable to all members of the ISAO but that may impact a subset of the larger ISAO. It will be up to the members to determine whether to handle this by forming a subsection of the larger ISAO or by forming a separate ISAO.

5.3 COMMERCIAL ISAOS AND SERVICES

An important part of the ecosystem will be formed by companies that provide services that can be used by ISAOs or companies that are ISAOs themselves. For example, if a specific shoe store wanted to be part of an ISAO, but there was no shoe industry ISAO or any other ISAO that it could logically fit under, it might approach an established ISAO offering membership for a fee. By signing up it could obtain the benefits of being part of the ecosystem even though there was no specific ISAO covering its industry.

Alternatively, an ISAO may choose to outsource certain capabilities or services it doesn’t want to develop organically. There are many benefits to this approach, including reduced costs through economies of scale as well as quickly obtaining a level of expertise that might otherwise take years to develop.

5.4 NON-ISAO INFORMATION SHARING OR ANALYSIS ENTITIES

The cybersecurity information sharing ecosystem includes entities that are not ISAOs but that may share information with each other, a specific ISAO, a group of ISAOs, or a government organization. While not providing the services of an ISAO or being organized as an ISAO, these entities are nonetheless important to the ecosystem and can provide valuable services to their members. An example of this might be a group of individuals within a community who come together monthly to discuss issues they have faced and how they have addressed them. This informal sharing of information can be very valuable and should be encouraged even if the group does not desire to form an ISAO. Another example might be commercial service providers providing threat correlation or other analytical products and services not targeted toward ISAOs.

5.5 OTHER CONSIDERATIONS

Individuals considering forming an ISAO have a number of other issues they should consider beyond the initial decisions related to establishing the ISAO. Critical considerations include the type of ISAO and its place within the ecosystem, whether a service provider will be contracted to offer specific capabilities, and whether an ISAO may already exist that could meet the needs of the target community of interest. After the decision is made to continue with establishing a new ISAO, these other considerations will need to be addressed. Some of these are discussed briefly in the next sections.

5.5.1 SHARING OF INFORMATION

There are many issues to be addressed when an ISAO considers its involvement in the actual sharing of information—and as always, this will be decided by its members and their objectives. For example, what information will the members be asked to share? How will the sharing of information be accomplished? How will privacy be maintained? What level of trust can the members place in the information? Will the ISAO receive information from other non-member entities (such as the government or other ISAOs), and if so, will this be a one-way sharing of information or will it be bi-directional? ISAOs will exist in the ecosystem in every combination of sharing as discussed here. These issues are at the heart of any information sharing program. An emerging ISAO does not need to face these issues in isolation, however, as there are individuals and organizations (such as the ISAO SO) that they can turn to in order to address these issues systematically.

5.5.2 MEMBERSHIP FEES

Whether or not an ISAO charges its members a fee will depend on the goal of the ISAO and the services it offers. Many things can be done to share information without requiring a full-time ISAO staff or a membership fee. There are other services and capabilities requiring full-time personnel to accomplish that may drive consideration of a fee-based business model. Some ISAOs may have a mix of paid memberships and unpaid memberships that offer a combination of free and premium services.

5.5.3 ANALYSIS OF INFORMATION

Up to this point, the emphasis has been on the sharing of information, but an important function of an ISAO is the dissemination of actionable information. This requires analysis. The extent of the analysis needed will depend on the goal of the ISAO and its members. A well-tailored analytical capability will make the difference between inundating members with data that provides no help and disseminating information that can help members take actions to enhance their security posture.

6 THE ISAO DOCUMENT SERIES

The ISAO ecosystem is being developed by an evolving community body of knowledge through a consensus-based development process. While a complete catalog of the ISAO series is not possible yet due to the evolving nature of the environment, the following represents the current expected document series in which specific documents will be developed:

- ISAO 100 Series: Establishment and Operations of ISAOs
- ISAO 200 Series: ISAO Services and Capabilities
- ISAO 300 Series: Information Sharing

- ISAO 400 Series: Privacy and Security
- ISAO 500 Series: Analysis
- ISAO 600 Series: Government Relations
- ISAO 700 Series: Global Information Sharing.

APPENDIX A GLOSSARY

Selected terms related to cybersecurity are defined below.

Analysis: A detailed examination of data to identify malicious activity and an assessment of the identified malicious activity to existing threat information to say something greater about the data at hand.

Automated Cybersecurity Information Sharing: The exchange of data-related risks and practices relevant to increasing the security of an information system utilizing primarily machine programmed methods for receipt, analysis, dissemination, and integration.

Cyber Threat Information: Information (such as indications, tactics, techniques, procedures, behaviors, motives, adversaries, targets, vulnerabilities, courses of action, or warnings) regarding an adversary, its intentions, or actions against information technology or operational technology systems.

Cybersecurity Information: Data-related risks and practices relevant to improving the security of an information system.

Cybersecurity Information Sharing: The exchange of data-related risks and practices relevant to increasing the security of an information system.

Cybersecurity Purpose: The purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability.

Cybersecurity Threat: An action on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system. The term does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

Incident: A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

Situational Awareness: Comprehension of information about the current and developing security posture and risks, based on information gathered, observation, analysis, and knowledge or experience.

Threat: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.

APPENDIX B ACRONYMS

CISA	Cybersecurity Information Sharing Act of 2015
DHS	Department of Homeland Security
EO	Executive Order
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
IT	Information Technology
SO	Standards Organization