ISAO SO Product Outline

Draft Document – Request For Comment

ISAO SO – 2016 v0.2

ISAO Standards Organization
Dr. Greg White, Executive Director
Rick Lipsey, Deputy Director

May 2, 2016

Table of Contents

PURPOSE AND USE

This outline serves as a unifying framework to identify and organize the topics to be addressed by the ISAO Standards Organization (ISAO SO). These topics were identified through a series of public meetings and data calls, and will be refined through the work of the ISAO SO's Standards Working Groups (SWGs). Topics may be addressed through statements of principle, policies, process descriptions, guidelines, templates, data standards, and other products. The sequence of document development and publication will be determined by the ISAO SO in consultation with the SWG chairs. While these source documents will ultimately be consolidated or synopsized to appear in a single volume for ease of reference, they will each be released as they are developed to meet the urgent needs of private and public organizations to improve their cybersecurity posture through effective information sharing and analysis.

Many of these topics will require inputs from multiple SWGs to ensure the cohesion of the complete body of work. The designation of a specific SWG or the ISAO SO in the outline below implies responsibility to consolidate applicable inputs to address the topic.

INTRODUCTION

The importance of information sharing to computer 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 the nation's critical infrastructures. 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 (ISAOs)." These new entities could be "organized on the basis of sector, sub-sector, region, or any other affinity," which greatly expanded the number and type of information sharing organizations that will be developed. To help with their establishment, EO 13691 directed DHS to "enter into an agreement with a nongovernmental organization to serve as the ISAO Standards Organization" (ISAO SO).

In developing the standards, guidelines, and other documents that are needed to help entities create and operate ISAOs, the ISAO SO established a number of Standards Working Groups. These groups were created to address specific areas pertinent to creating or operating ISAOs. When developing the various documents, the SWGs must consider the two overarching efforts important to ISAOs: the sharing of cybersecurity information, and the analysis of the information that has been shared. The purpose of these efforts is ultimately to improve the Nation's ability to "detect, investigate, prevent, and respond to cyber threats," while protecting the privacy and civil liberties of citizens.

To accommodate the expanded list of entities that can form ISAOs described in EO 13691, there will be different types of ISAOs with different objectives and capabilities. There will also be varying levels of organizations within the ISAOs, and there may be commercial entities that form to provide services to ISAOs. Some ISAOs may be formed on a very informal basis and may have little or no desire to collect and analyze the 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 its members and may have as an objective the ability to help respond to security incidents affecting its members.

Additionally, an ISAO may initially form with limited objectives and target capabilities but then evolve over time to increase its ability to assist its members by adding additional capabilities and objectives. 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 the capability to analyze shared information to better detect and prevent cybersecurity attacks; then ultimately add a 24/7 operational capability to assist its members with ongoing cybersecurity incidents. Conversely, an ISAO may elect to maintain limited capabilities to best serve the needs and capabilities of its constituents. The goal of the ISAO SO is to be as inclusive as possible in finding a place for any individual or organization that wishes to be part of the Nation's overall information sharing effort.

This product outline is designed to take into consideration the different types of ISAOs that may be formed and the various levels of capabilities each may incorporate. It presents an organized approach to developing the various documents pertinent to ISAOs while considering the immediate needs of emerging ISAOs. Individual SWGs will develop and refine specific products in coordination with other SWGs as directed by the ISAO SO, and will consider how each product must fit into the larger framework defining the creation and operation of an ISAO.

PROBLEM STATEMENT

EO 13691 clearly lays out the problem that is being 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

> (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.

To address this problem 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, the undertaking needs to consider how the efforts of individual ISAOs can be combined into an overarching information sharing network for the Nation to improve the cybersecurity resiliency of participants. The effort must be as inclusive as possible, appropriately incorporating vetted information from multiple sources. Due consideration must be given to determining the level of trust that can be placed in such information, which requires that the national effort address issues such as trust, reliability, and information overload.

WHAT IS AN ISAO?

The term “Information Sharing and Analysis Organization,” or ISAO, means any entity or collaboration created or employed by public- or private-sector organizations, for purposes of:

- gathering and analyzing critical cyber and related information in order to better understand security problems and interdependencies related to cyber systems, so as to ensure their availability, integrity, and reliability;
- communicating or disclosing critical cyber and related information to help prevent, detect, mitigate, or recover from the effects of an interference, compromise, or incapacitation problem related to cyber systems; and

- voluntarily disseminating critical cyber and related information to its members; federal, state, and local governments; or any other entities that may be of assistance in carrying out the purposes specified above.

[NOTE: This definition was coordinated with SWG chairs in late February 2016, but will be refined in concert with standards development deliberations.]

EXPLANATION AND EXAMPLES

- ISAOs consolidate, analyze, and distribute cyber information to their members
- Overview of ISAO categories and capabilities

CATEGORIES OF ISAOS (SWG 2)

ISAO SUPPORT FOR ORGANIZATIONS (SWG 2)

While recognizing there is no single description of capabilities that will fit all ISAOs, it is important to consider a description of the functions that a “fully capable” ISAO will have to support its members. This discussion will help emerging ISAOs determine the capabilities and objectives they wish to develop—keeping in mind that the initial set of objectives and capabilities may evolve as the ISAO matures.

A fully capable ISAO will provide a variety of services to support its members. These services, and the capabilities that are needed to provide them, should be designed to support ISAO members as they manage strategic and tactical cyber-related risks. The type of support can be grouped into three broad categories, with some overlap between them. These categories are:

- *Situational awareness:* ISAO members need to understand both the tactical and strategic aspects of the environment in which they are managing risks. This support includes activities to collect and share information, analyze it, and recommend what to do with it.
- *Decision-making:* ISAOs need to disseminate actionable information that will enable their members to make decisions related to their current security posture and allocation of security and IT resources. This support involves receiving information, establishing its relevance to the organization, assessing potential impacts, identifying potential actions, and selecting the best course of action.
- *Actions:* ISAO members ultimately will take actions based on received information and analysis. Organizations will develop detailed actions and assign

responsibilities, implement the actions, and evaluate their effectiveness, providing feedback for further consideration.

For each type of support, individual members or organizations will have responsibilities addressing their own needs as well as responsibilities to the ISAO. The ISAO in turn also has responsibilities for each of these categories that address the ISAO membership as a whole.

VALUE PROPOSITION

ISAOs offer the following benefits to their members and other ISAOs:

- An informative set of cybersecurity threat indicators and best practices provided by ISAOs will make individual members more secure.
- ISAOs implemented in accordance with a consistent yet flexible framework can replicate and extend current trust relationships by establishing a common, shared set of values and expectations.
- Members enhance their knowledge about how to protect themselves from, detect, and react to cyber threats.
- By aggregating information from multiple organizations, ISAOs present a richer picture of malicious activity taking place around the country and 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 carry out effective and timely responses if they discover unauthorized intrusions.

PRODUCTS

The following sections list areas of support and the products that the ISAO SO or SWGs identified in parentheses will develop.

GOVERNANCE (SWG 1)

- Charter/legal construct
- For-profit and not-for-profit considerations
- Single-company ISAOs
- Conditions under which information is shared (SWG 3)
- Code of conduct
- Participation guidelines

- Common lexicon
- Legal framework for sharing
- ISAO contracts and agreements (including non-disclosure agreements)
- Membership qualifications
- ISAO certification (multiple types)
- Process for handling, storing, and sharing personally identifiable information (SWG 4)
- Intellectual property rights
- Member outreach by the ISAO
- Compliance and separation policy (SWG 4)
- Interaction of member organizations
- Information sharing concept and rules of the road (SWG 3)

SERVICE OFFERINGS (ISAO CAPABILITIES) (SWG 2)

- Vulnerability management
- Best practices library
- Situational awareness
- Threat warning (actionable intelligence)
- Operational support and assistance
- Support for incident response and recovery
- Risk management
- Information management and analysis
- Trusted information sharing and collaboration environment/services

OPERATING MODELS (TYPES OF ISAOS) (SWG 2)

- Categories of ISAOs
  - Risk-based (e.g., ecosystem-wide vulnerability)
  - Threat-based (general or specific, either methods or individual actors)
  - Individuals and informal group-based
  - Industry- and sector-based
  - Geographically based
  - Technology-based
  - Issue-based

    - Limited time or special event-driven
    - Clearinghouse versus membership
- Structuring ISAOs for state, local, sector, etc.
- Outsourcing analysis considerations
- Scaling of ISAOs
- Operational cost of ISAO based on ISAO maturity/capability

INFORMATION SHARING POLICY (SWG 3)

- Use of shared information
- Prioritization of information for exchange
- Vetting of data and information received
- Ownership of information
- Liability of sharing information
- Minimizing data shared
- Anonymity of data shared
- Anonymity of information sources
- Integrity of information shared
- Framework for sharing between ISAOs
    - One-way information sharing
    - Two-way information sharing
    - Information sharing networks
- Procedures for capability for real or near-real time exchange
- Handling sensitive information (SWG 4)
- Handling classified information (SWG 4)
- Privacy protections (SWG 4)
- Considerations when sharing with the federal government (SWG 6)
- International considerations (SWG 6)

INFORMATION COLLECTION AND DISSEMINATION (SWG3)

- Process to identify what’s important to members
- Data model for sharing information

- Level of analysis to be provided
- How to get companies to share
- Triggers for sharing
- Effective information control policies or principles

SHARING MODELS AND MECHANISMS (SWG 3)

MODELS

- Mesh network
- Hub and spoke
- Publish-subscribe
- Peer to peer
- Flooding
- Portal

MECHANISMS

- Face to face
- Telephone
- Email/listserv
- Website postings
- Automated (primary indicator and defensive measures, then follow on information)

SECURITY OF DATA AND SYSTEMS (SWG 4)

- Infrastructure (on premises and cloud)
- Member anonymity
- Data and dissemination assurance
- Distribution discrimination

FUNDING MODELS (SWG 1)

- Membership
- Subscription
- For profit
- Non profit

START-UP ACTIVITIES/KEY PLANNING FACTORS (SWG 1)

- Establishing the ISAO's purpose and strategy
- Standard criteria and terminology
- ISAO contracts and agreements
- Member outreach by the ISAO
- Marketing the ISAO
- Membership benefits
- ISAO staff certifications and qualifications
- Core components of ISAO: trust, requirements, business
- Information sharing procedures, process, and standards
- Business plans, organizational structures, roles and responsibilities
- Definition of ISAO service offering
- Creating ISAO capabilities and structure
- Operating a new ISAO
- Measures of effectiveness

PARTNERSHIPS AND SUPPORT (SWG 5)

- Peer relationships and inter-ISAO collaboration
- Relationships with national, tribal and regional entities (SWG 6)
- Mentoring
- ISAO SO support (ISAO SO)
- Commercial/industry support
- Government programs (SWG 6)

GOVERNMENT RELATIONS (SWG 6)

- Partnership with the government (information exchange and collaboration)
- Law enforcement liaison
- Information sharing and regulator relations
- Protections when sharing with regulators

APPENDIX

- Definitions
- References