ISAO Capabilities and Categories

Draft Document—Request for Comment

SWG G 2—2016 v0.2

ISAO Standards Organization
Standards Working Group 2: ISAO Capabilities
Denise Anderson, Chair
Fred Hintermister, Vice-Chair

May 2, 2016

Table of Contents

INTRODUCTION

The purpose of this voluntary Information Sharing and Analysis Organization (ISAO) Standards Organization (SO) Guide is to assist ISAOs, both new and existing, in describing how capabilities may support their organization. This guide presents options to consider when creating a new ISAO that may become part of a national ecosystem of cyber information sharing.

ISAOs can come in many different shapes and sizes. Each should reflect:

- the needs of its members, and
- the threats and vulnerabilities that its members face.

Our goal is to inform and advise ISAOs, whether they are just forming or already exist, to understand how ISAO capabilities support their operation and organization. The “shopping list” of capabilities an ISAO requires is determined by the nature of the particular ISAO itself.

DESCRIBING ISAO CAPABILITIES

ISAO capabilities are chosen by the organization and support the needs of its members. The capabilities generally fall into three types: foundational, additional, and unique. Most ISAOs will have capabilities chosen from some distinctive combination of these three types. As an example, a small group wanting to establish an ISAO may choose primarily foundational capabilities, in order to meet projected membership requirements.

- *Foundational* capabilities are generally considered more fundamental in nature for most ISAOs, depending on the needs of its members. Foundational capabilities are those from which most ISAOs might find a larger number of applicable capabilities to consider for serving their members. They might include using a standard method to send and receive cyber threat indicators, vetting members (a trust capability), and storing threat indicator information, to name a few.
- *Additional* capabilities typically might encompass those which further differentiate the ISAO or meet the needs and constraints of its particular operational or business environment, driven by its own member needs. Additional capabilities tend to represent enhanced capabilities beyond those afforded by foundational capabilities, in the case of most ISAOs, as they construct a portfolio of capabilities designed to address the needs of their members. An example might include analysis of incoming cyber information in order to assess its relevance to membership needs.

- *Unique* capabilities are special functions or activities developed or adopted by the organization itself to meet its own particular needs or opportunities. Unique capabilities are those that are not otherwise identified as foundational or additional. This construct deliberately refrains from specifying particular unique capabilities, because these are the specific capabilities that ISAOs design and apply for their members. In other words, a unique capability is electively created and applied by any individual ISAO, but has a common lexicon term to describe its type (unique) that is understood by all ISAOs. The existence of the term "unique" within the lexicon of this construct enables all members of the ISAO sharing community to understand immediately the type of capability being discussed, applied, or considered so that best practices, research, event programming, and development of active defense and resilience doctrine is better enabled. They might include understanding effective firewall settings, growing mentor-protégé opportunities, or instituting listserv mechanisms.

Capabilities an ISAO decides to choose depend on the service it wishes to provide to its members. There is no requirement to "package" or select any specific capability or groups of capabilities—it is a pick-and-choose environment. Experience may well reveal certain capabilities that all or most organizations consider essential in actual practice for an effective and secure information-sharing partnership.

The ISAO SO will develop a common lexicon to describe the capabilities so there will be an understanding of each capability in order to accelerate adoption and improve the ability for collaboration. Additionally, a common lexicon supports operational techniques, as well as procedural and doctrinal development, while fueling innovation. The better everyone understands ISAO capabilities in advance, the more we can accelerate and support an overall ecology of trusted sharing. This is because ISAOs—which include Information Sharing and Analysis Centers (ISACs)—that see a known indicator of recognized trusted sharing and analytic capabilities (a "Basic Voluntary Capability," as explained below) will instantly recognize it and can form collaborative partnerships and trusted relationships more readily and quickly than they otherwise might. This approach leverages the proven experience that well-crafted and minimal standardization can actually improve diversity and trusted collaboration. It acts as an accelerant and catalyst to prospective partners who will share data and knowledge for benefit of the entire ISAO community.

For this reason, we will develop a one-page *standard descriptive form* that states an ISAO's name, mission, purpose, and particular capability using a common lexicon built on the scheme of foundational, additional, and unique capabilities offered in this document. One portion of that form could contain a standard and recognizable icon representing the Basic Voluntary Capability. That symbol would reassure potential partners about the organization's understanding of the

capability level, thereby increasing the probability that trusted collaborative relationships will form which are mutually productive for not only the partner organizations but also the ISAO community as a whole. This is the intent of the ISAO voluntary standards development effort.

The *standard descriptive form* would avoid:

- Statements of any particular requirements for any ISAO, because all standards and guidelines are voluntary.
- Issues due to complexity or excessively detailed information.

This approach would feature:

- A comprehensive roadmap, informed by subject matter expertise, to consider for ISAO development that invites formation and informs sustainment.
- A standard lexicon and model to accelerate collaborative innovation within the growing community of ISAOs.
- A common lexicon that addresses, specifically names, and invites—but does not constrain or restrain—ISAO-specific and member-driven innovation and customization.
- A way ahead to standardize and simplify an essential ISAO Basic Voluntary Capability in order to accelerate ISAO partnering for trusted collaboration, a key resilience benefit, by using a universally understood approach to make it more efficient.
- An achievable, elective, and aspirational component to encourage a basic capability. New and evolving ISAOs might aspire to attain the Basic Voluntary Capability, but they would not be required to select its use because it is voluntary. ISAOs that do develop the Basic Voluntary Capability may find benefits that accrue for their members from more efficient ISAO collaborative partnerships and that may accelerate trusted relationships.

The following are among the foundational capabilities that a Basic Voluntary Capability should indicate:

- Administering day-to-day operations and providing sufficient support to members.
- Vetting new members. This is one aspect of demonstrating trustworthiness and credibility to current and potential members, as well as to partners.
- Enabling members to collaborate and share information among themselves and with ISAO administrators or analysts. This may include the capability to send and receive Suspicious Activity Reports (SARs) and incident reports.
- Analyzing incoming information to assess its relevance to members and implications for them.

- Managing and sharing restricted or otherwise sensitive information in a way that respects originators' preferences. This might include binding members to an information sharing policy.
- Disseminating information to members. Possible mechanisms include, but are not limited to, face-to-face meetings, secure portals, mailing lists and other email distribution platforms, online discussions, message boards, webinars and chat applications.

The capabilities represented by the above Basic Voluntary Capability are among the foundational capabilities that new and evolving ISAOs might choose to select, along with other additional and unique capabilities, in any mix they deem appropriate to the needs of their members, the threat and vulnerability environment they face, and the resources and constraints of their particular organization.

This model means that every ISAO can be described in a standard manner that consists of:

- A discrete core capabilities statement summarizing the organization's distinctive blend of descriptive foundational, additional, and unique capabilities, which could be numbered or digitized for reference.
- Basic Voluntary Capability (if chosen by the ISAO) expressed through a recognizable, accepted icon, to promote sharing and inter-ISAO collaboration; and a standard, one-page Basic Voluntary Capability template summary for reference and doctrinal development for operationalized resilience (unity of effort and message).
- Compatibility with measures of effectiveness. All ISAOs can be described in a standard lexicon and format that specifically identifies each capability by type and number. That being the case, research products and resilience plans can benefit from the fact that capabilities application may be further enhanced by digital processing and automated sharing for the benefit of the ISAO community and the nation. The result is a standard lexicon construct that supports continuous improvement in operationalized resilience for the ISAO community as a whole.

CATEGORIES OF ISAOS

Four strategic drivers—information sharing, analytics, member value delivery, and business and IT operations—support the various core capability areas. Additionally, there are three types of capabilities: foundational, additional, and unique. All have been tied together within a comprehensive structure of *voluntary* standards and guidelines that use a common lexicon and a way for prospective trusted collaboration partner organizations to identify a set of capabilities. This section

discusses the types of ISAOs that may emerge; the intent is to *describe, not prescribe,* what ISAOs might look like as they evolve over time.

Although there will be many variations of ISAOs, all will fall into one of the four categories described below, each with different characteristics, attracting different participants, and having different capabilities. A second factor considers degrees of trust, which may be gauged in many ways. Examples may include possession of security clearances, vetting of members, non-disclosure agreements, and other contractual arrangements. When an ISAO is operating within the framework of a larger response organization, the ISAO's host or sponsoring organization might ask for its operation to be aligned with higher level guidance, which promotes unity of effort and message.

Examples include the methods for response used by established ISACs, methodologies and procedures used by the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC), and other proven processes. In these instances an ISAO will be in a category such as "industry or technology" and have capabilities that support its operation.

To restate, this section provides a high-level description of the different categories of ISAOs going forward. The list is non-exhaustive and illustrative only. Our proposed model, which contains numerous capabilities, could identify any specific requirements there as unique that are not already identified within the proposed foundational or additional capabilities. In these instances an ISAO may be in any of the below categories. It is important to remember that some ISAOs, in the individual and/or informal group-based category, may wish to have minimal capabilities and choose to receive cyber threat information by means of email or other less complex means. In the end, what matters is improving the U.S. cybersecurity posture.

CATEGORY 1: INDIVIDUALS AND INFORMAL GROUP-BASED

Characteristics: a single entity, event-driven (such as a new virus or malware requiring a group formed ad hoc to respond); or an informal collection of organizations or individuals with limited sharing in scope or duration and analysis objectives, infrequent sharing of information, information obtained from public sources or other similar ISAOs or between members; generally little or no tailored information analysis or incident response.

Examples: A self-employed security consultant; a localized group of professionals; a rapidly convened or issue-driven ISAO.

CATEGORY 2: INDUSTRY- AND SECTOR-BASED

Characteristics: groups of organizations (public, private, or blended) or a private company sharing a common interest, goal, or purpose. Some members may be

capable of sharing information with federal and law enforcement entities at classified levels. The industry or sector size may vary greatly. Examples might be a small town, an unaffiliated bank, a software consulting firm, or a government contractor. Information received may be from public sources or members. The organization might perform ISAC or other ISAO incident response coordination, perhaps as part of government response frameworks (such as DHS NCCIC) that consist of both public- and private-sector partners. It may analyze shared information as it pertains to the ISAO and its members and other collaborative security partners in coordination efforts.

Examples: Southern U.S. mega churches; U.S. electronic game developers industry; existing ISACs.

CATEGORY 3: GEOGRAPHICALLY-BASED

Characteristics: Members come from a geographic region and cross multiple businesses or sectors. Some members may be able to share information with federal and law enforcement entities at a classified level. Incident response coordination is generally a significant goal of the members. Members regularly analyze government and member-shared information. Entities may provide for a member-supported security operations center (SOC) or similar shared resources or contracted support.

Example: the state of Texas; the city of San Antonio, Bowie County, and so on.

CATEGORY 4: OTHER

Characteristics: Groups of technical individuals who have an active interest in cyber threat indicators due to their engagement of cyber defenses, or other computer technology in their business. These members or groups desire to share information and, in some cases, perform analysis of threat vectors and software. It may be that this group shares directly with the U.S. government in order to collect the most current cyber threat indicator information.

Example: Computer security firms, cyber defense service providers.

CONCLUSION

An ISAO may choose capabilities that will determine its category or, inversely, the category by which an ISAO defines itself may suggest the capabilities it may choose to consider. Either way, ISAO capabilities and categories potentially help inform each other, depending on the approach an ISAO chooses to best serve the needs of its members. The voluntary standards describe possible capabilities for new and developing ISAOs to consider that may help them serve their members, while organizing those capabilities within a comprehensive construct. The construct further accelerates and enables future resilience efforts by offering a standard digital-ready lexicon and a Basic Voluntary Capability, which any ISAO

can aspire to and elect to apply, and which may help accelerate the development of trusted security collaboration for the ISAO that employs it and at ISAO community levels writ large. We have described three types of ISAO capabilities. Although most ISAOs will likely choose to commence operations with primarily foundational capabilities, their evolution over time will probably include relatively greater use of additional and unique capabilities that may potentially broaden and enhance the effectiveness of information sharing and analysis offerings for their members.