ISAO
Standards Organization

ISAO 100-2: Guidelines for Establishing an Information Sharing and Analysis Organization (ISAO)

v1.01

October 14, 2016

ISAO 100-2

Guidelines for Establishing an Information Sharing and Analysis Organization (ISAO)

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

The ISAO SO leadership and authors of this document would like to acknowledge those individuals who contributed significantly to the development of this publication, including:

Kevin Albano of IBM, Scott Algeier of IT-ISAC, Michael Arceneaux of Water-ISAC, Jon Baker of The MITRE Corporation, Adam Buteux of PWC, Roger Callahan of FS-ISAC, Timothy Casey of Intel Corporation, Luke Dembosky of Debevoise & Plimpton LLP, Tim Evans Senior Advisor of John Hopkins University Applied Physics Laboratory, Jeremy Feigelson of Debevoise & Plimpton LLP, Betsi McGrath of The MITRE Corporation, Benjamin R. Pedersen of Debevoise & Plimpton LLP, David Pedraza of BCD Solutions | IT Staffing and Managed Services, Meeta Sidhu of Price Waterhouse Coopers, Rick Simon of Intel Security, Bobbie Stempfley of The MITRE Corporation, and Joseph Viens of Charter Communications and COMMS ISAC.

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 1
2 Introduction 1
3 Key Strategic Planning Factors 1
3.1 Define the Essence of the ISAO 2
3.2 Determine What Information to Share 2
3.3 Identify Role in the ISAO Ecosystem 4
3.4 Partner and Collaborate 4
3.5 Define Services and Capabilities 5
3.6 Define Membership Criteria and Identify Target Members 6
3.7 Measure Effectiveness 7
4 Key Operational Planning Factors 8
4.1 Establish a Governance Model 8
4.1.1 Formal vs. Informal Governance Structures 9
4.1.2 Types of Formal Legal Entities 9
4.2 Develop the Business Model 9
4.2.1 Marketing Plan 10
4.2.2 Communications Strategy 10
4.2.3 Financial Plan 11
4.2.4 Cost Drivers 12
5 Building a Trusted Community 14
5.1 Creating Trust in an ISAO 14
5.2 Building and Maintaining Trust 16
6 Final Considerations 16
Appendix A Service and Capability Matrix 18
Appendix B Glossary 26
Appendix C Acronyms 29

1 EXECUTIVE SUMMARY

The purpose of this document is to provide a set of guidelines for establishing an Information Sharing and Analysis Organization (ISAO). First, a set of key strategic planning factors is provided to help emerging ISAOs consider the most critical questions early in the process. These strategic planning factors will then guide and inform consideration of a series of key operational factors. Finally, a section on building a trusted community offers a set of key considerations for establishing trust. Trust is critical to establishing a successful ISAO with active participation and cybersecurity information sharing among members. As a set of guidelines and key considerations, this document is not prescriptive in nature. Instead, the document guides the reader through the most critical items to consider. Establishing an ISAO that meets the needs of a growing membership is an iterative process, and these guidelines are intended to help organizers establish an ISAO and evolve it to keep in step with its members' changing needs.

2 INTRODUCTION

These guidelines are designed to help emerging ISAOs consider critical questions and are an effective tool for periodically evaluating the health and status of established ISAOs. These guidelines take into consideration the different types of ISAOs that may form and the capabilities each may incorporate. This document, along with the other ISAO SO documents, presents a structured approach to the various topics pertinent to ISAOs while considering the immediate needs of emerging ISAOs.

This document is not prescriptive in nature. It does not tell an organization the best way to do something or even what specifically to do. Instead, the document guides the reader through the most critical items to consider.

This document presents a collection of strategic and operational planning factors for consideration, along with a more thorough discussion of consideration for building a trusted community. Overall, it attempts to focus on what is truly unique to establishing an ISAO.

3 KEY STRATEGIC PLANNING FACTORS

Creating an ISAO requires working with a community of stakeholders to define the ISAO's value proposition, objectives, and capabilities to improve cybersecurity for its constituents and membership partners. These factors assume that an initial representative collection of stakeholders is able to consider each factor.

Considering these strategic planning factors in an iterative fashion is recommended since decisions in one area will impact consideration of other areas. Decisions on each key strategic planning factor will guide and influence the operational planning factors presented later in this document.

Furthermore, an ISAO may evolve over time to meet the changing needs of its members. Accordingly, stakeholders should periodically review these key strategic planning factors to ensure alignment with the ISAO's mission and vision.

3.1 DEFINE THE ESSENCE OF THE ISAO

Defining the essence of the ISAO is the critical first step to establishing a new ISAO. From the onset of its existence, the emerging ISAO needs to identify its mission and its vision. A clear articulation of mission and vision will establish a foundation as the emerging ISAO works through the following key strategic and operational planning factors.

Consider the following guiding questions as the emerging ISAO defines its essence:

- What is the common purpose that brings together the members of this ISAO? What connects the organizations that will become the members of the ISAO to form a community for sharing?
- How will the ISAO improve the cybersecurity position of the sharing partners and members of the ISAO? What information sharing problems will the ISAO solve?
- What goals does the ISAO intend to achieve? Goals may range from raising awareness locally through sharing of basic threat intelligence information among individuals, to high-speed real-time sharing of technical threat intelligence on an automated, global basis across an entire sector. Goals may also evolve over time as the ISAO grows in size and resources.
- What is the ISAO's vision? How do the ISAO stakeholders and members picture the ISAO 1 year after formation, 5 years after, etc.? For each timeline milestone, where will the ISAO be in terms of size, geographic scope, products, services, and activities?
- What is the ISAO planning to do differently from other ISAOs? What unique solution does the ISAO bring to its members through information sharing?

3.2 DETERMINE WHAT INFORMATION TO SHARE

Determining what type of information to share and how to share that information is the next factor to consider. Take a systematic approach to understanding the information sharing requirements of target members as well as those of potential partner ISAOs. The emerging ISAO should consider what sorts of information it has, what sorts of information it needs from its members and partner ISAOs, and what sorts of information those organizations would like to receive.

Consider the following guiding questions as the emerging ISAO determines what information to share and how to share that information:

- What information do ISAO members need or what information will support the mission and vision of the ISAO? The answer might range from a narrowly scoped, automated data feed to face-to-face, strategic information sharing, and it may not be limited to a single type of information.
- How will ISAO members use the information received from the ISAO? Members may use information from the ISAO directly in their security operations to mitigate cyber threat or indirectly to inform risk management decisions.
- How will the ISAO acquire the information it shares? In some cases, ISAO members might be the source of the information that the ISAO then reshares to its members. In other cases, the ISAO might offer information received from other sources such as government or industry cybersecurity information providers.
- How does the ISAO intend to share information, at least initially? Examples include informally and on a person-to-person basis, manually through online portals, or automated via information sharing platforms. The ISAO may start with informal sharing and evolve by exploring what technologies exist to allow for rapid sharing of threat indicators.
- Do the ISAO members have the required capabilities to use the types of information that the ISAO provides?
- How will the ISAO ensure that the information shared is actionable or otherwise enriching and enhancing information to meet its members' needs?
- How will the ISAO collect feedback on the information it shares? Collecting feedback will allow the ISAO to evolve its information sharing to ensure that the information supports members' needs and its mission and vision.
- Will information be shared anonymously with the ISAO or will information source attribution be required? Providing source attribution can help to enable collaboration and trust, and may increase the usability of the information. However, attribution may leave some members uneasy to share with the ISAO. Ultimately, a hybrid approach may be required.
- What sort of restrictions or sensitivity levels will the ISAO support in the information that it shares and receives? Look to established methods such as the Traffic Light Protocol (TLP)[1] and others used by mature ISAOs. This decision may impact everything from infrastructure choices to usability of shared information. Clear terms of use will enable more widespread sharing and utilization of the ISAO's information. Similarly, consider whether classified information will be shared.

[1] The Traffic Light Protocol was developed by US-CERT to designate sensitive information and to insure the correct distribution of that information. See https://www.us-cert.gov/tlp.

Review ISAO 300-1, *Introduction to Information Sharing*, for a more in-depth discussion of cybersecurity information sharing, including a discussion of the types of information and the mechanisms for sharing that information.

3.3 IDENTIFY ROLE IN THE ISAO ECOSYSTEM

ISAOs and their members participate in a cybersecurity information sharing ecosystem where information is commonly shared among organizations and across ISAOs. Within this ecosystem there are opportunities to partner for mutual benefit, distribute analytic capability, collaborate on incident response, and more. With this ecosystem in mind, it is highly beneficial for emerging ISAOs to carefully consider their potential role in the ecosystem.

Consider the following guiding questions as the emerging ISAO identifies its role in the cybersecurity information sharing ecosystem (as noted earlier, it will be beneficial for the ISAO to revisit this process, especially as the ecosystem evolves):

- Who is the ISAO's target community?
- Will the ISAO be limited to one industry sector or subsector; include multiple sectors; or support a non-profit community, or geographic region? Will the ISAO be limited to one specific event, such as the Olympics, or perhaps focus on one particular threat, like ransomware?
- Has the ISAO identified target community leaders to champion the ISAO throughout the community, encouraging participation? Is the targeted community already sharing information?
- What will be the ISAO's geographic focus? Consider local, regional, statewide, national, or international. If international, consider whether sharing information with international partners will present challenges from a legal and/or "safe-sharing culture" point of view.
- To what extent will the ISAO interact with various government agencies (including law enforcement)? Review ISAO 600-2, *U.S. Government Relations, Programs, and Services*, for relevant considerations.
- How is this new ISAO similar to or distinct from existing ISAOs or other organizations providing services to the target community (e.g., cyber threat feed providers)?[2]

3.4 PARTNER AND COLLABORATE

Emerging ISAOs need to carefully consider partnering and collaborating with other organizations, including other ISAOs.

[2] For a list of existing information sharing organizations, refer to https://www.isao.org/information-sharing-groups/.

Consider the following guiding questions when evaluating prospective partnerships and collaborations:

- What does the ISAO have to offer the community of sharing partners to enhance the protection of critical infrastructure, industry, business, or government?
- Has the ISAO defined strategic information sharing partners? Have the mutually beneficial objectives of partner strategic alliances been defined?
- What are similar ISAOs currently providing and how can you coordinate, collaborate, and work together?
- Are there other ISAOs that could be partnered with? Consider other ISAOs for mentoring and support to assist with the early defining phases and the transition to operations. Consider other ISAOs for ongoing collaboration.
- Will the ISAO work with other partners to enhance the value of the information received? Will the ISAO openly share with other ISAOs?
- Is internal and external collaboration part of the ISAO's natural workflow?

3.5 DEFINE SERVICES AND CAPABILITIES

This section offers guidelines for ISAOs to consider as they design and implement a collection of services and capabilities to meet the needs of their members.

Appendix A Service and Capability Matrix, provides illustrative examples of services and capabilities that an ISAO can consider. It provides descriptive information for each service or capability, advantages and challenges of each item, and broad recommendations for implementation. ISAOs are encouraged to go beyond the examples provided in this document, and to innovate approaches best suited to delivering member value within their resource environment. As an additional benefit, innovative services will help accelerate capability improvement throughout the information sharing ecosystem.

By reviewing the illustrative list of services and capabilities provided in Appendix A, ISAOs may have a head start in answering important questions in operational planning, such as the following:

- What foundational services will the ISAO offer that provides value for the ISAO's members? For example, will it act as a hub to share cyber threats and defensive measures, analyze data and turn it into "actionable" intelligence, or both?
- Beyond the core set of information sharing services, what additional services will the ISAO provide to add further value for its members?

- What unique services will the ISAO provide to meet distinctive aspects of the ISAO, its members, and its mission? How will the ISAO strategically differentiate itself from other organizations to deliver truly distinctive member value?
- What is the plan for future ISAO service offerings and what capabilities help to provide those?
- Does the ISAO plan to acquire analytic capability to apply to information that is shared for members, and to share analytics with others external to the ISAO?
- Does the ISAO have special expertise in cybersecurity and information sharing?
- How can the ISAO learn from other ISAOs and share innovation with other ISAOs across the community when searching for foundational, additional, and unique services to offer and the capabilities that support them?

3.6 DEFINE MEMBERSHIP CRITERIA AND IDENTIFY TARGET MEMBERS

ISAOs greatly benefit from establishing a clear set of membership criteria. Membership criteria will vary across ISAOs, and an emerging ISAO can benefit from understanding the approaches that other, more mature ISAOs have taken.

Consider the following guiding questions while defining membership criteria:

- What are the foundational membership requirements and how will those requirements be monitored and enforced? Requirements might focus on operational capabilities; how the member would interact with the ISAO; the amount and type of information the member will share; or compliance with industry standards such as NIST SP 800-53 Rev. 4, “Security and Privacy Controls for Federal Information Systems and Organizations”;[3] ISO/IEC 27001, “Information Security Management System Requirements”;[4] or others.
- Are there participation and engagement requirements? Some ISAOs require active participation to ensure sharing and attempt to increase the return on investment. Other ISAOs allow more passive participation.
- Will membership be based upon organizations, individuals, or both? If organizational, will there be limits to organizational participation? If individual and organizational, will there be different requirements for organizations and individuals?
- How will the ISAO identify, engage, and encourage member and stakeholder participation and collaboration? Supporting member participation is critical to

[3] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.
[4] http://www.iso.org/iso/home/standards/management-standards/iso27001.htm.

enabling vibrant sharing within the ISAO. This vibrancy of sharing is often proportional to the support and encouragement given by the senior leaders in member organizations. Without an express "go" signal from management, the ambiguities over whether to share information might lead network defenders and analysts to assume a "no-share" decision out of an abundance of caution.

- Will all members be considered equal or will levels or tiers of membership be defined? If tiers are established, consider whether or how services and data access may also be tiered to meet the needs of each membership group.

Consider the following guiding questions while identifying target members:

- What is the member identification, nomination, and recruiting strategy? Consider who is responsible and what role the ISAO membership plays in this ongoing process.
- If a diverse set of members is expected, how will the ISAO manage this diversity? Consider diversity in terms of both member organization size (small business vs. large enterprises) and cyber preparedness level (basic cyber defense capabilities vs. advanced capabilities).
- How will new members be brought into the ISAO? Consider the impact on trust among ISAO members and how these new members are introduced to the existing membership.
- What sort of new member vetting is required to enable the ISAO's mission and vision?
- What new member communication and training will be provided?

3.7 MEASURE EFFECTIVENESS

Early in the process of establishing a new ISAO, consider developing a set of measures to help assess the overall effectiveness of the services, capabilities, and information sharing supported by the ISAO.

Consider the following guiding questions while identifying target members and seeking to retain existing members:

- What measures are needed to demonstrate membership return on investment? Tracking aggregate data about the type of cybersecurity information received by the ISAO and then the information that is made available to the members can help members understand their return on investment. Similarly, offering more detailed examples that demonstrate the value of the analysis conducted by the ISAO can also help demonstrate return on investment. Perhaps most importantly the ISAO should consider also collecting "success stories" from its members to allow individual member successes to help the general membership better understand how the ISAO can benefit its members.

- What measures are needed to help the ISAO refine the effectiveness of its services, capabilities, and information sharing? A defined feedback process that enables members to offer feedback on cyber threat intelligence received from the ISAO is one example that can assist the ISAO in refining its offerings.
- Are there measures that could help identify service, capability, or information sharing needs? Consider periodically assessing member needs with a structured survey or direct member interviews.
- How can these factors be measured over time to support the management of the ISAO? How often will these factors be measured?

4 KEY OPERATIONAL PLANNING FACTORS

Successful establishment of an ISAO is dependent not only on effective strategic planning, but also on key elements of operational planning. Setting up the organizational model for effective execution and evolution of products and services should be considered as the ISAO is established. Key operational planning elements include decisions on the type or form of legal entity that may be necessary to support the functions, governance models, and business planning.

4.1 ESTABLISH A GOVERNANCE MODEL

Individuals and small groups can function with informal decision models, but an effective ISAO benefits greatly by considering how decisions will be made that affect a diverse and potentially large group of members. The need for a defined governance model that articulates how the ISAO will be directed and overseen is an important initial requirement for an emerging ISAO. The questions raised for consideration throughout these guidelines demonstrate the need for a defined governance model to help reconcile competing priorities, differing needs, and disparate approaches for reaching the ISAO's objectives. A governing body authorized to make decisions and formulate the ISAO's organizational policies should be established when the ISAO is first forming.

Although there are many legal and other considerations that may seem complicated, keep in mind that governance choices can flow easily from the vision and goals for the ISAO. Depending on its vision and goals, the ISAO may choose to establish itself as an informal group with a looser set of operating rules, or it may choose at the outset to establish itself as a formal operating entity. It is important to recognize that the vision, goals, and membership of the ISAO may change considerably over time, which may support consideration of starting an ISAO with a smaller, less formal organization and making changes to the governance structure as the ISAO evolves and matures.

4.1.1 FORMAL VS. INFORMAL GOVERNANCE STRUCTURES

Consider the following questions to support the decision of establishing the ISAO with an informal or formal governance structure:

- **Membership requirements**. Will the ISAO require members to agree formally to written requirements of membership? If so, one way to accomplish this is to create a formal legal entity to which members can agree through a membership agreement, memorandum of understanding, information sharing agreement, or similar document.
- **Membership fees/payments**. If the ISAO will receive and make payments, how will those be treated from a tax standpoint and according to applicable law and regulatory requirements? A formal legal entity, including not-for-profit status if applicable under local and federal law, may be the best approach.
- **Third parties**. Do you expect the ISAO to engage in activities that require contracting with a third party? If not, a separate legal governance structure may not be necessary, at least until the ISAO begins to encounter such needs.

4.1.2 TYPES OF FORMAL LEGAL ENTITIES

What type of legal entity will best address the needs and requirements of the ISAO? For example, a very large ISAO with significant resources may consider incorporating under local or state law, providing the most formal governance structure and clearest protection from liability. In contrast, a smaller ISAO that simply needs the ability to conduct business as a separately recognized legal entity may require a less formal structure, or one with greater governance flexibility, such as a Limited Liability Company (LLC).

Additionally, the ISAO should consider whether benefactors, regulators, and other third parties with whom the ISAO may desire to interact and contract may have greater comfort with corporations, as compared to LLCs, as a result of the larger and more developed body of statutory and case law relating to corporations.

If the ISAO has concluded, based on the preceding questions, that establishing the ISAO as a formal legal entity is necessary to serve the ISAO members' needs, the ISAO and its stakeholders should consider consulting legal counsel to assist in choosing the most appropriate type of legal structure to meet the ISAO's needs. Decisions on governance structures such as incorporation, boards, and not-for-profit status require knowledge of local, state, and federal laws.

4.2 DEVELOP THE BUSINESS MODEL

ISAOs should spend time considering their business model and how they will identify and sustain funding, maintain membership participation, establish and sustain necessary information technology to support collaboration and analytic

activities, and monitor execution of ISAO functions to meet member expectations. Key elements of the business model to be considered are listed below.

4.2.1 MARKETING PLAN

A marketing plan is typically a document that captures a company's plan for advertising and marketing. Marketing objectives are identified and the plan describes the activities required to achieve those objectives.

A marketing plan will support the continued definition of the ISAO, encourage membership, and enable overall operations. Marketing plans can be detailed formal documents or informal activities performed by ISAO staff and members. These considerations are part of defining the vision for the ISAO. Consider the following items to help inform the marketing plan for the ISAO:

- Essential marketing policies and processes: Who will define, develop, and maintain the plan?
- What will be the ISAO's foundational positioning statement, including goals and objectives, envisioned capabilities, value and benefits it intends to deliver, and how it differs from other ISAOs?
- How will the positioning statement be used in recruiting, external communication, and member communication?
- Reaching the ISAO's audiences
    - Marketing communications policy: What will be the rules, responsibilities, and authorities for marketing communications?
    - What tactical marketing tools will the ISAO use to communicate to its audiences (e.g., events, online and documentary materials, public relations, advertising, private recruitment, and the like)?
    - If the ISAO plans to accept revenue-generating advertising opportunities, what will be the policies around and the process for advertising on ISAO properties?

4.2.2 COMMUNICATIONS STRATEGY

A communication strategy is the selection of appropriate communication objectives and the identification of specific ISAO awareness goals. The communications strategy is focused on engagement with members, prospective members and partners. It is not about cybersecurity information sharing, but rather enabling effective communications among all stakeholders.

The ISAO will need a communications strategy that's appropriate for the scale, scope, complexity, formality, goals, missions, and resources of the ISAO. Decisions about ISAO communications should include basic operating guidelines for roles, responsibilities, and rules for members and ISAO staff. Scope and tactics

detailed in the strategy can affect operating costs for the ISAO. Consider the following questions:

- **External communications** (not including cybersecurity information sharing)
  - External communications policy: What will be the rules, responsibilities, and authorities for external communications?
  - External communications governance methods and approaches: What methods and approaches will the ISAO use to communicate governance matters with other ISAOs, the ISAO governing body, strategic alliances, and government organizations?
  - External communications tactical tools: What tactical tools will the ISAO use to communicate externally (e.g., listserv, portal, newsletters, e-mail, news feeds, calendars)?
- **ISAO member communications** (not including cybersecurity information sharing)
  - Member communications policy: What will be the rules, roles, responsibilities, authorities, and activities for member communications?
  - Member communications governance methods and approaches: What will be the methods and approaches used to communicate with ISAO members about matters such as recruitment and onboarding, ongoing policy and capabilities development, strategic planning, and accomplishments?
  - Restricted ISAO member communications policy: What is the defined set of restricted communications between ISAO members? Is it based on or limited by industry or government regulation? If so, what are those restricted communications?
  - Member communication roles: What are the ISAO member roles that send or receive information, and what type(s) of information should each role send or receive?
  - Member communication tactical tools: What tactical tools will the ISAO use to communicate with members (listserv, portals, newsletters, e-mail, news feeds, calendars, etc.)?

4.2.3 FINANCIAL PLAN

ISAOs need to understand their current and future financial state by carefully evaluating their assets, expenditures, and revenue. A financial plan will capture these factors and allow the ISAO to plan for a sustainable future.

ISAOs require a financial plan that addresses startup costs, but sustained revenue is required to support ISAO goals, scope, and services. Even a small ISAO that comes together to address a specific short-term issue has to address basic resourcing. ISAO revenue streams will be dependent upon the type of business model the ISAO chooses, including membership or service fees. Based on the

type of ISAO business model, funding options and potential sources of revenue will need to be considered.

4.2.4 COST DRIVERS

An assessment of the external environment and market may be performed to identify foundational requirements and key inputs into the ISAO's operations and financial plan. Items listed here are provided to guide the discussion in the development of a business plan and operating budget; ISAOs can vary widely in size, scope and resourcing.

Depending upon the services, skills, and technologies needed by the ISAO to deliver its services, certain costs may prove to be a significant portion of the ISAO's operational expenditure. It is worth considering the nature of each type of cost, that is, whether they are fixed or variable costs, and how these costs vary as membership grows. An ISAO may benefit from matching the timing of cost to the timing of revenue streams—for example, hosting technology in a cloud-based solution that charges monthly based on usage, versus buying servers that require an initial capital outlay. Consider the following key cost drivers, expenses, and capital requirements for creating and sustaining an ISAO, and for day-to-day operations:

- **Management and operations**
  - Organization formation: legal services, state/federal regulatory requirements, and tax/accounting services.
  - ISAO staff: Regardless of the size and number of members belonging to the ISAO, careful consideration should be noted about the support staff required for ISAO management and day-to-day operations: executive management, managers, analysts, product developers, member identity managers, risk and compliance staff, membership development staff, finance staff, sales and marketing staff, legal counsel, etc.
  - Professional services (consulting, tax, accounting, legal support, etc.): Will the ISAO engage in activities requiring the advice of outside experts, such as technical experts to assist in setting up sharing mechanisms or legal services to advise on particular activities according to local, state, or federal laws and regulations? Will the ISAO employ any full-time or part-time employees, or will it rely on consultants and contractors to facilitate the sharing and analysis of information?
  - Governance: the board of directors, chief executive officer, and other possibly mandated roles (depending on the ISAO's legal structure). Will these roles be filled by individuals who will be financially compensated?

- **Infrastructure and technology.** Technology plays a key role in the ISAO, and technology solutions vary widely in terms of cost. The ISAO should determine operational and infrastructure requirements to support and sustain the ISAO, including the following:
  - Software: applications and licensing fees for core ISAO services (information capture/distribution/analysis/alerting (build vs. buy decision), tools for handling sensitive data (i.e., anonymization), and applications for supporting ISAO daily operations (finance, security, information technology service management, membership development, collaboration tools, etc.).
  - Analytics: the required analytics processing capabilities and to what degree to support the analysis and enrichment of data (in-house, outsourced, or a hybrid model).
  - Hardware: onsite vs. cloud computing, system security, large storage capacity requirements, disaster recovery, and more.
  - Data feed providers: external vendors providing feeds and products that the ISAO can give to its membership and to help support enhancing data analysis.
- **Promotion costs**: developing in-house marketing and outreach capabilities to generate interest in the ISAO's target market community, grow membership, and manage member relationships.
- **Member needs**: ISAO membership target community, including the number, size, and needs of the members that will impact costs (e.g., anticipated number of threat feeds as well as onboarding and integrating members into the ISAO information sharing infrastructure community).
- **Training and education**: continuous training of management and support staff (security—all hazards, both physical and cyber), ISAO policies and procedures, ISAO infrastructure information exchange/sharing platforms, information sharing policies and protocols, and any additional services offered by the ISAO.
- **Office space:** If the ISAO will be meeting in person periodically, will the ISAO need to lease space to do so, or will a particular member provide space where the ISAO management and members can meet? If the ISAO needs to rent space for meetings and operations, will an individual member step forward and sign the lease, or will the ISAO need to do so? Alternatively, short-term conference or meeting space rentals may be available.
- **Financial management**: Will the ISAO require its own bank account to pay for services or receive funds?
- **Insurance**: Will members require the ISAO to obtain insurance to cover its activities?

- **Accreditation, memberships, or affiliations:** Will the ISAO need to obtain or maintain any accreditations, memberships, or affiliations?

5 BUILDING A TRUSTED COMMUNITY

An ISAO can only function when a certain level of trust exists between its members, between the members and the ISAO, and between the ISAO and its partners. The greater the level of trust, the more effective the ISAO can become. Trust is required for the free flow of information between participants, and it is especially necessary in critical situations in which members may have to take it on faith that their sharing partner(s) will treat them and their shared information fairly. Without a minimal level of trust, members will doubt the accuracy of the data they receive or that data they share will be handled responsibly, reducing the likelihood that meaningful data will be exchanged at all and defeating the very purpose of an ISAO. Trust is the key enabler of value for an ISAO.

As in all other aspects of life, trust is never automatic, even for a formally created ISAO. Trust is earned, and is built through relationships, over time, and often through trial and error. While building trust, members can leverage personal or legal relationships and organizational systems to initiate and support information exchanges. Over time, and with a little experimentation, trust can evolve within the ISAO and enable effective, timely, and beneficial information sharing.

The organizational system by which trusted exchange is achieved is called a "trust construct." There are many trust constructs used in organizations, and each ISAO will benefit from a visible and enduring construct as part of its organization structure. The trust construct may be as simple as only dealing with members the ISAO staff has worked with personally, or it may be as complex as an ongoing process of contractual interactions administered by the legal representatives of the participants. Every trust construct has its advantages and disadvantages, and every ISAO must consider the options and build a construct that best fits the needs of its own participants.

A formal and ratified trust construct, even if a very simple one, is valuable for an ISAO for many reasons. It sets the ground rules for sharing so that all members understand what they have agreed to and what their responsibilities are. When everyone acts according to those expectations, trust is demonstrated and strengthened. The construct also helps potential members decide if this is an organization they want to join, as well as helping other ISAOs identify possible trading partners. Finally, if necessary, it can act as a guide to help resolve conflicts between members.

5.1 CREATING TRUST IN AN ISAO

No single trust model will work for all ISAOs; each ISAO must create its own trust construct as part of its formation activities. It will take time to create an effective construct, as each ISAO must work through the practical details of its own unique

situation. This need to develop trust regardless of the unique situation will require trust to be central to the development of all aspects of planning and operating an ISAO. There is no standard template, so here are some issues to consider when creating or modifying a trust construct:

- Develop a written member agreement that details all the expectations and privileges of membership in the ISAO.
- Decide on the overall type of organization, for example, people-to-people, organization-to-organization, or restricted or open membership.
- Is a legal contract required, such as a nondisclosure agreement (NDA), or are the members comfortable with relying on personal relationships? In either case, it may be helpful to consult a legal representative on this issue.
- If a legal construct such as an NDA is used, ensure it is easy to understand, binding, and enforceable on all members of the organization.
- Know how the information will be used. For example:
  - How is information shared within a member company?
  - Can members share with nonmembers?
  - How will government agencies (state, local, federal, non-U.S.) protect shared information from disclosure under their own transparency laws?
- What size of the ISAO is best? It's easiest to maintain trust in a limited membership, but the sources of information may also be limited.
- Decide how to notify all members when a member joins or leaves so that all members know who is part of the community.
- Have a mechanism to deal with violations of the member agreement. Examples include providing a written warning on the first offense, imposing financial penalties on the offending organization, suspending membership, or removing the offending member from the organization.
- Ensure that members can trust the ISAO itself. Provide clear data handling, protection, and usage terms so that members can safely share information with the ISAO. For additional information on security of data, see ISAO 300-1, *Introduction to Information Sharing*.

As the ISAO evolves, it can gain a better understanding of what factors build and diminish trust among its members. This evolution of trust is addressed in the following section.

5.2 BUILDING AND MAINTAINING TRUST

An ISAO will establish a level of trust among its members at the outset, and this will evolve over time based on the actions of the ISAO and its members. The following are some examples of actions that can help build and maintain levels of trust:

- Initiate trust by getting someone to "go first":
  - Identify and ask specific members to share specific information.
  - Invite members to deliver presentations to the membership on sensitive issues.
- Start with a small number of companies to keep the community small so that members know and have relationships with each other.
- Draw membership from companies or organizations with a common security need or interest.
- Build membership from companies or organizations that already have an element of trust or established business relationships.
- Have a trusted element in the community—such as a Chamber of Commerce, a government agency, a local nonprofit organization or non-governmental organization, an elected official, or a trade association—endorse the organization and encourage others to join.
- Periodically remind members of the trust model mechanism and its rules.
- Actively measure and track levels of trust over time, and assess how levels of trust are influenced by the actions of the ISAO and its members. Trust can be measured directly through engagement with members or indirectly by selecting other measures (such as what, and how much, information is shared) as proxies for trust levels.
- If there is a breach of trust, be transparent about it and correct it. Don't pretend it did not happen; instead address the issue directly and openly.

With respectful and honest interaction over time, an ISAO should be able to build significant trust between members and partners and see tangible benefits in its information sharing.

6 FINAL CONSIDERATIONS

Establishing and evolving an ISAO is an iterative process. The guidelines presented in this document are intended to assist in this process by raising the most critical strategic and operational factors for consideration. ISAOs are encouraged to periodically reevaluate these guidelines as they evolve.

ISAOs participate in an information sharing ecosystem and there are numerous established and evolving ISAOs today. ISAOs should actively establish partnerships to meet shared needs and to learn from the experiences of others.

In addition to this set of guidelines, the ISAO SO has developed a collection of key resources for ISAOs.[5] ISAOs are encouraged to review and leverage these resources.

[5] https://www.isao.org/resources/resource-library/

APPENDIX A SERVICE AND CAPABILITY MATRIX

This appendix provides a listing of common ISAO services and capabilities, along with a discussion of each service's advantages, challenges, and implementation guidelines. The services generally fall into three types:

- **Foundational** services and capabilities are generally considered baseline services for most ISAOs, but are established based on the needs of its members. They might include using a standard method to send and receive cyber threat intelligence, vetting members (a trust capability), and storing cybersecurity information, to name a few.
- **Additional** services further differentiate the ISAO or meet the needs and constraints of its particular operational or business environment. They represent enhanced services beyond those afforded by foundational services, and help ISAOs construct a portfolio of services designed to address the needs of their members. An example might include analysis of incoming cybersecurity information in order to assess its relevance to members' needs.
- **Unique** services are specialized functions or activities developed or adopted by the organization to meet its particular needs or opportunities. Unique services are those that are not otherwise identified as "foundational" or "additional". Unique services are electively created and applied by an ISAO. They might include understanding effective firewall settings, growing mentor-protégé opportunities, or instituting listserv mechanisms. These, along with illustrations in the table below, are representative examples of the potential services or capabilities that could be described as "unique".

ISAO services and capabilities are chosen by the organization and support the needs of its members. Of note, an ISAO does not need to provide all of the foundational services or capabilities enumerated hereafter to be considered an ISAO. Rather, the chart included below is intended to provide information about the advantages and disadvantages of each service for evaluation and use by an interested organization on its path to becoming or evolving its ISAO services and capabilities.

Service/ capability	Description	Advantages	Challenges	Implementation Guidelines
Collect and disseminate data	Data should be based on the needs of the members and could include things like information on threats, vulnerabilities, risks, incidents, and tactics, techniques, or procedures used by threat actors. Types of data could also be actual indicators of compromise (IOCs) including IP addresses, MD5 hashes, and command and control information. Data can	At a very basic level, the collection and dissemination can be as easy and cost-effective as partnering with another organization that already produces a daily report such as the DHS Infrastructure report, or an ISAC daily report, to distribute a daily report to membership via e-mail. Once a process is	Depending on the level of data desired, the format and frequency of dissemination, the process may require talent, time, process, and technology. It will take time to develop a process and cull sources. Finding a format that is easy for members to use and determining what is relevant or desired by membership can also	Foundational: Facilitate a way for members to share data. Pull or partner on an existing daily report and disseminate via e-mail to the membership. Send out an e-mail survey to determine what members want to see and best format for distribution. Create a list of open-source information that is relevant to the membership such as vendor blogs,

Service/ capability	Description	Advantages	Challenges	Implementation Guidelines
	come from a variety of sources, by culling open source reporting from sites such as cybersecurity vendors, media articles, cybersecurity blogs, from white papers, from other ISAO or ISACs, from government sources and reports as well as directly from members. The ISAO can choose to parse relevant data out, add any relevance to the membership, or just distribute the sources with links for more information. Items can be disseminated through an alert, through a daily report, via a portal/database, website, listserver, newsletter or other means. Format can be text, PDF, html or whatever is desired by the membership. Frequency again should be based upon the desires of the membership but could be daily, weekly, or monthly.	developed, the means of pulling information together can be fairly routine. Collecting and disseminating data is a basic activity of an ISAO and can be a very easy way to get relevant and informative data out to the community.	take time and understanding of the constituents. Technology, depending on needs, can also have significant startup and maintenance costs such as in developing a secure portal or creating a platform to share IOCs in a machine-to-machine (automated) fashion. Members may not have the capability to provide or ingest automated data.	news media feeds, other reports from ISAOs or ISACs, and reports from government. Parse out relevant text for effective reading and create links. Disseminate in format and via the means desired by membership. Additional: Develop a secure portal for members to submit data; host relevant documents and indicators for members to access. Unique: Develop a report as outlined in "Foundational" and add a threat intelligence perspective and relevance to the membership commentary to each item.
Facilitate member sharing	The process of enabling members to share information, with or without attribution, with each other and with the ISAO.	If members of the community are familiar with each other, then creating trust is easier. The Traffic Light Protocol is an easy way to get members to agree to sharing protocols. A document like a NDA can also be very simple and can help engender trust. Sharing enhances situational awareness across the constituency and can inform risk-based decision making.	Creating a trust environment is very challenging, especially if the members with the community are unfamiliar with each other. Creating a secure environment (if desired) is expensive. Creating a completely anonymous environment is expensive. Getting members to share is also a challenge. If someone violates trust, that could put a halt on information sharing.	Foundational: Vet members, develop a basic NDA, and establish a type of TLP agreed to by members. Create an e-mail listserver and find a champion within the community to start the sharing. An analyst or staffer can act as a broker for anonymous sharing. Additional: In addition to Foundational steps, establish sharing over a secure means if so desired by members. Develop a portal for submitting anonymous information sharing. The portal environment would include an authentication and identification method to engender trust and a secure environment. Create incentives and rewards for sharing.
Analyze information for relevance and trends	Typically, members of a certain stakeholder group are interested in analysis that pertains to their particular operations/interests.	Trending data can be very informative and can help members understand what is going on within their	Members may prefer to do analysis themselves or may have vendor competitive issues, or they may introduce	Foundational: Providing a forum for members to discuss and identify common issues and trends.

Service/ capability	Description	Advantages	Challenges	Implementation Guidelines
	Analysis can produce actionable information for members by stripping data that are not relevant for membership and can provide information on trends being seen either within the group or in areas of relevance or importance to the group.	respective environments. Supplying relevant analysis makes information and situational awareness more efficient.	additional resource requirements. Finding skilled analytical staff who have a strong understanding of the group and what data are pertinent as well as how to look at and analyze trends can be a challenge and may be expensive. Trending of data could take time, especially if dependent upon data being supplied by the group.	Additional: Finding open-source information that is relevant will require an understanding of the group's membership and its needs. Trending reports from open sources could be disseminated for situational awareness. Additional: Hiring or outsourcing to an analyst staff that will apply analytic methods to collecting and looking at data relevant to the group and then applying an opinion or strategic perspective on that data for the group. Staff or a third party could survey membership to gather data seen within their environments or take the information shared within the process or operation of the ISAO as well as other sources to compile applicable trends and reports.
Disseminate information to members	Have an established and agreed-upon mechanism to share information with members, based upon member needs. May include alerts, advisories, and/or regular publications, such as daily or weekly reports.	Alerts and advisories provide members with time-sensitive awareness of recent and active incidents and threats and freshly reported vulnerabilities. Regular information dissemination provides timely member awareness of information on threats, risks, vulnerabilities, preparedness, recovery and mitigation, and organizational or other activities.	Power, cellular, and Internet outages may prevent members from receiving alerts by e-mail. Members may not see the value of time-sensitive products. Creating actionable products may require an operational background, which can be hard to attract, retain, or fund. Cost, level-of-effort, and resource needs for creation, management, and sustainment may be high, particularly in order to meet urgent deadlines. An unfiltered flow of content could lead to information fatigue and overwhelm members and thus reduce readership and value.	Foundational: Dissemination may be accomplished with the following: 1) Desktop applications or webmail 2) Broadcast e-mail services 3) Electronic mailing list services, such as LISTSERV™ 4) Phone, 5) Website 6) Combination of the above. Additional: via a secure portal, encrypted e-mail channels or other secure means, or via an emergency alert system.
Survey members	Surveys can help learn information about the membership and can also be a quick way to understand member activity or needs.	Can be used to determine members' status or needs.	Surveys take time to construct and analyze. Access to some survey tools are not allowed by some organizations. Getting members to participate in surveys, especially during an	Foundational: Craft a basic e-mail survey, initiate a phone conversation, or host in-person meetings. Additional: Develop a survey committee to accept and cultivate survey requests from members,

Service/ capability	Description	Advantages	Challenges	Implementation Guidelines
			incident, can be challenging.	and analyze the results for action and understanding. Unique: Create custom alerting and survey tools during incidents to get a quick status of members and determine any needs or relevant information.
Host a secure online discussion space or other online forums for member-to-member collaboration	Have a means by which member could collaborate and share virtually and securely. This could include a secure listserver, a portal with two-factor or other secure authentication, or a webinar or cloud collaboration tool that restricts access to vetted stakeholders.	Provides opportunities for members to collaborate or seek advice on threats, vulnerabilities and best practices from peers, subject matter experts, and ISAO staff in a secure environment. Providing a secure online space enhances trust and fosters the sharing of more sensitive information.	Cost, level of effort (level-of-effort), and resource needs for creation, maintenance, and sustainment may be high. Members may prefer a streamlined, low-tech, low-touch, automated, or other approach. Adds complexity, which may result in less participation, sharing, and costs—for both the ISAO and the members.	Additional: Use a customizable web-based solution, ideally one that integrates with the ISAO's online portal (should that tool be implemented). There are a number of providers of this service.
Collect and disseminate mitigation information and resources	Mitigation information can come from a variety of sources, including members, and can prevent and defend against attacks.	Contributes to member value proposition and ISAO sustainability if mitigation resources are reliable, are fitted to members' needs, and have positive risk management impact. Increases the resiliency of the community.	May give risk to liability concerns if not properly managed; may require additional talent, time, process, and technology.	Additional: Furnish reports containing mitigation strategies from various sources. Facilitate member-to-member sharing on mitigation strategies, such as code to block malicious activity.
Collect and disseminate response and recovery information and resources	Response and recovery information can come from a variety of sources, including members, and can prevent and defend against attacks.	Contributes to member value proposition and ISAO sustainability if response and recovery are reliable, fitted to members' needs, and have positive risk management impact. Increases the resiliency of the community.	May give risk to liability concerns if not properly managed; may require additional talent, time, process, and technology.	Additional: Furnish reports containing response and recovery strategies from various sources. Facilitate member-to-member sharing on response and recovery strategies.
Develop and maintain relationships with relevant government agencies	Partnership with government and law enforcement can provide additional information and foster collaboration during incidents.	Provides greater awareness about new analytical and other products. May offer access to cyber and intelligence analysts. May lead to opportunities for consultation, collaboration, and partnership.	May require security clearances and/or badging to obtain access, may result in additional requirements to enable collaboration, and sharing may give rise to trust concerns of members. Servicing law enforcement needs, if present in the relationship, could divert resources from other services.	Additional: Identify federal, state, and local agencies that may add value to members. Establish relationships with industry partners that may already have relationships with agencies in place.
Host a secure online document repository for	An online portal provides a secure means for members to access relevant information.	Provides a central clearinghouse of documents for members.	Cost, level of effort, and resource needs for creation, maintenance,	Additional: Develop a password-protected online space where an assortment of articles and

Service/ capability	Description	Advantages	Challenges	Implementation Guidelines
sharing information with members		Provides an alternative to disseminating documents by attaching them to e-mail messages. Provides a restricted-access space to hold material that may be for members only, such as documents marked "For Official Use Only" or TLP Red, Amber, and Green.	and sustainment may be high. Members may prefer a streamlined, low-tech, low-touch, automated, or other approach. Members may not wish to log in to yet another portal.	documents can be posted and made available for viewing and download by members. Possible solutions include proprietary platforms, custom-built platforms and DHS's Homeland Security Information Network platform.
Participate in automated indicator sharing	Machine-to-machine threat indicator sharing.	Provides access to and the ability to share more data in a timely fashion. May accelerate inter-ISAO and other security partner sharing. May speed situational awareness of risks throughout the ISAO ecosystem.	Cost, level-of-effort, and resources may be an issue for creation, maintenance, and sustainment. Increased number of indicators makes analysis more difficult. Trust level in the sources of the indicators can impact the value of the indicators. Members may not have the capability to consume or push automated indicators.	Additional: Consider open-source tools and vendors. For more information, refer to the OASIS working group.
Provide vendor vulnerability notifications	Software and hardware vendors provide notices of vulnerabilities in their products.	Additional situational awareness.	May result in additional costs to disseminate to members. May be duplicative of what members already receive from vendors directly.	Additional: Subscribe to alert feeds or have staff collect and publish alerts. Unique: Provide analysis around the alerts regarding the impact on members.
Support members' efforts to develop their cyber workforce	Training and certification programs for analysts. Education and training via conferences, webinars, workshops, and other mechanisms.	An ISAO providing more offerings and services can meet the need of its membership and produce additional revenue streams. Provides opportunities for ISAO members to learn and interact with each other.	May be outside the scope of desired member value proposition. Depending on level of effort, may require significant resources and costs. May require registration fees, travel costs, and other expenses. May be difficult for members to participate.	Additional: Use ISAO members or staff to develop and present content or leverage third parties. Unique: Leverage the ISAO community to obtain discounts for certification providers. Develop an in-house specialized training program.
Provide a reach-back service, whereby members can consult SMEs	The ability to bring in SMEs, from the membership or outside the membership, to assist other members or organizations.	Leverages SMEs from other member organizations with similar risk models. Could potentially provide for a free or low-cost solution to resolve a problem. Could potentially allow for a repository of solutions.	Can be resource intensive to develop and maintain these relationships. Could lead to unrealistic member expectations.	Additional: After polling membership to better understand needs, create a community or communities of SMEs. Seek volunteers from the member community to provide the SMEs. Facilitate the exchange of information by using a portal, phone bridge, chat, e-mail, webinars, etc.

Service/ capability	Description	Advantages	Challenges	Implementation Guidelines
				Develop and use a nondisclosure or liability release agreement to protect both the member and the SME.
Provide access to Common Vulnerability Enumeration (CVE) publications	CVE publications are compilations of technical information about vulnerabilities.	Additional situational awareness.	May be beyond the scope of member value proposition or interest. May require extensive member education to use and apply or create uptake in perceived value. May be done by others, competitive issues.	Additional: There are several automated feeds (e-mail) for new (or past) CVEs. There is the NCICC CVE feed, which is automated. There is also the National Vulnerability Database, where the ISAO may perform specific searches for CVEs when a member asks about a vulnerability to specific hardware and software platforms. Develop the methods for capture of the CVE announcements and for their distribution. Different methods for distribution may exist due to member needs and means of accepting the alerts. Develop the step-by-step instructions for applying the patches/fixes for members.
Form committees, working groups, or special communities of interest among members	Establish committees, working groups, or forums for member-to-member collaboration. Committees can be formed along subject matter such as big data and can be around functions such as membership, products and services, or other desired groupings.	May be useful if there are threats, vulnerabilities, or other issues that require special attention. Members may find peer input valuable. Easy and inexpensive way to engage membership and focus work on a particular task or project/topic.	Typically, level-of-effort intensive. May create member discord of varying service levels. Member value delivery may be difficult to demonstrate with impact relative to other service options. May result in additional costs to create and maintain. Relies on member participation and engagement to be successful.	Additional: Identify subject matter that may require focused attention. Determine whether in-person or virtual forums are preferred. If virtual is preferred, identify solutions such as listservs, discussion boards, and other collaboration solutions. Determine a charter if needed and a group leader.
Participate in exercises as planners and players	Cyber exercises provide an excellent means to understand current (and past) cyber threats and best practices for improving cybersecurity at the hardware and software level, and they support improved social networking of like-minded professionals.	Can identify shortfalls in operational capabilities. Offers the opportunity to build relationships with potential partners.	Typically, resource intensive. Members may have proprietary or other concerns that limit the availability or desire to exercise. May compete with already heavy member exercise requirements due to oversight and regulatory environment.	Additional: Participate in exercises hosted by public and private entities. Develop and execute internal exercises, developed in-house or by third parties.
Facilitate mutual aid	Mutual aid involves sharing resources or	Provides for like organizations to help	May require resource or time commitments to coordinate.	Unique: Develop a mutual aid agreement through the

Service/ capability	Description	Advantages	Challenges	Implementation Guidelines
among members	knowledge during incidents.	each other during incidents. Increased capability and less down time for members. Fosters further trust among members. Increases the value of the membership in the ISAO.	Could have an adverse effect for the member in need if aid commitments are not fulfilled. Lack of a legal structure could lead to liability and reimbursement challenges.	ISAO or directly between members.
Provide managed security services	A service for members could possibly consist of monitoring their network traffic for anomalies and attacks, pushing application and operating system security patches, managing firewall and router access control lists, and providing a host of other services with the end goal of providing the maximum amount of cybersecurity to the member.	Could provide additional value to members and be a member retention tool. Provides additional member awareness. Could be a revenue stream.	Will require the ISAO to have expert and experienced staff along with documented service agreements. Access to the member's network and systems could give rise to liability issues. Typically, resource and cost-intensive.	Unique: Develop in-house or contract with a third party.
Produce and/or provide threat intelligence	Actionable threat intelligence is insight you can act on—it enables informed decision making that results in better outcomes. ISAOs can develop and provide threat intelligence to help its members understand the threats they are facing and what they can potentially do about it.	Threat intelligence can be very informative and can help members understand what is going on within their respective environment.	May require talent, time, and process; may require additional security measures and information assurance requirements. The same information may be available through other means or sources. Finding skilled threat intelligence staff who have a strong understanding of the group and threat intelligence gathering and production can be a challenge and may be expensive. Developing a threat intelligence program could take time, especially if dependent upon information being supplied by the group or by other sources. May require staff with security clearances and access to classified information.	Unique: Hire or outsource this capability, or form a group within the membership to address threat intelligence.

Service/ capability	Description	Advantages	Challenges	Implementation Guidelines
Provide access to a library of adversary tactics, techniques, and procedures (TTPs)	A library or collection of adversary TTPs is a list of threat actors and their methods and strategies for attack.	Additional situational awareness.	May create security challenges. Inaccurate information could give rise to liability. May require extensive member education to use and apply or create uptake in perceived value. May require extensive resources to create and maintain.	Unique: Create a resource library of links to sites that maintain these TTPs and actionable intelligence on the methods and means employed. Develop and maintain an in-house directory of TTPs based on open-source threat data available from numerous sources, notably the U.S. CERT. The information available includes alerts, vulnerability bulletins, and specifics for the more technically savvy staff (when to share levels of sensitive information, threats to mobile devices, and others). Many sources of threats and indicators are available by subscribing to third-party services. Could also build a directory from automated indicator sharing sources, which may include TTPs.
Offer test-bed access by members for malware analysis	An ISAO test bed is a means by which the ISAO itself and/or members may use, in an isolated environment, a network (usually set up in a virtual manner) that emulates one or more computer network environments. Test beds allow the testing of security configurations, especially changes when attempting to mitigate a vulnerability, and observe what operational impacts may happen.	The ISAO may want to use its test bed to test security configuration settings in support of its membership and offer the settings as a means to improve a member's security posture prior to any implementation that can cause a disruption or unexpected event. Can be used to test the effects of actual malware and see the results of protective measures. Can validate decisions and recommendations to its membership.	Requires additional expenditures to replicate as much as possible its members' networking, greater level of staff expertise regarding virtual environments, and virtual network fabrication. May give rise to ISAO risk due to member activity, may involve costs to create or maintain, may create member access and use disputes with the ISAO, may not deliver value evenly across member groups or which is desired by members, especially relative to other member value opportunities, and may compete with vendors who are ISAO stakeholders alongside members. Members may not be sophisticated enough to handle malware.	Unique: Contract with third parties or develop the capability in-house.

APPENDIX B GLOSSARY

Selected terms used in the publication are defined below.

Alert: Timely information about current security issues, vulnerabilities, and exploits.

Analysis: A detailed examination of the elements or structure of cybersecurity information, in order to identify the applicability to increasing the security of an information system in some way.

Cybersecurity information: Data 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 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.

Cyber threat indicator: Information that is necessary to describe or identify the following:

- Malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability
- A method of defeating a security control or exploitation of a security vulnerability
- A security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability
- A method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability
- Malicious cyber command and control
- The actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat
- Any combination thereof.

Defensive measure: An action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability.

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

Incident response: An organized approach to addressing and managing the aftermath of a security breach or attack (also known as an incident). The goal is to handle the situation in a way that limits damage and reduces recovery time and costs..

Indicator: An artifact or observable evidence that suggests that an adversary is preparing to attack, that an attack is currently underway, or that a compromise may have already occurred.

Malware: A program that is covertly inserted into another program or system with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system.

Malicious cyber command and control: A method for unauthorized remote identification of, access to, or use of an information system or information that is stored on, processed by, or transiting an information system.

Malicious reconnaissance: A method for actively probing or passively monitoring an information system for the purpose of discerning its security vulnerabilities, if such method is associated with a known or suspected cybersecurity threat.

Monitor: To acquire, identify, scan, or possess information that is stored on, processed by, or transiting an information system.

Mitigation: The act of reducing the severity, seriousness, or painfulness of security vulnerability or exposure.

Secure portal: A web-enabled resource that provides controlled secure access to and interactions with relevant information assets (information content, applications, and business processes) to selected audiences using web-based technologies in a personalized manner.

Security control: The management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity, and availability of an information system or its information.

Security vulnerability: Any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

Sharing: See "Cybersecurity information sharing."

Signature: A recognizable, distinguishing pattern associated with an attack, such as a binary string in a virus or a particular set of keystrokes used to gain unauthorized access to a system.

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.

Threat actor: An individual or group involved in malicious cyber activity.

Threat source: The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally exploit a vulnerability.

Vulnerability: A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

APPENDIX C ACRONYMS

DHS	Department of Homeland Security
IP	Internet protocol
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
IT	Information technology
LLC	Limited Liability Company
NDA	Nondisclosure Agreement
NIST	National Institute of Standards and Technology
SO	Standards Organization
TLP	Traffic light protocol
TTP	Tactics, techniques, and procedures