Cybersecurity-Related Information Sharing Guidelines

Draft Document—Request For Comment

SWG G 3—2016 v0.2

ISAO Standards Organization
Standards Working Group 3: Information Sharing
Kent Landfield, Chair
Michael Darling, Co-Chair

May 2, 2016

Table of Contents

Figures

Tables

EXECUTIVE SUMMARY

Standards Working Group (SWG) 3, Information Sharing, produced this draft for discussion purposes at the upcoming workshops and to further encourage private-sector input before the ISAO SO publishes a complete preliminary draft for public comment.

SWG3 is currently focusing on cyber threat information sharing. In the future it is our intent to expand this effort to support cyber-physical threat information as well. In the process of performing our work, we developed a context and conceptual framework to focus the discussion of information sharing capabilities. We have identified some areas where more information is needed.

NOTE TO REVIEWERS

The discussion draft that follows includes a framework overview, a set of information capabilities, and the data aspects that fit together. The three areas are interrelated but distinct. What is not clear is the most effective way to present these: in a NIST CSF format, in some other means? We appreciate your assistance in helping determine the most useful way to depict the overall relationships for someone getting involved in an ISAO for the first time.

The following are additional questions or issues to consider:

- Additional discussions about the Information Sharing Context and conceptual framework being presented
- Further categories of information an ISAO may want to be shared
- The functional decomposition of an ISAO
- The depth of focus on the analytics aspects of an ISAO.

Suggestions in these areas would be particularly useful and will be incorporated into the document in the coming versions. The material is and will remain a work in progress; SWG3 welcomes and actively encourages comments and other input.

OBJECTIVES

As noted in the "Introduction" section of the ISAO SO Product Outline (of which this document will be a part), ISAOs need to be able to share information related to cybersecurity risks and incidents, and to collaborate in as close to real time as possible. Further, the efforts of individual ISAOs can be combined into an overarching effort to improve the cybersecurity resiliency of their members and the nation.

The ISAO SO recognizes that not all new ISAOs may be capable initially of or desire to fully achieve these objectives. The information sharing guideline is structured to provide a new or existing ISAO with a context identifying outcomes to be considered when selecting and implementing information sharing and collaboration efforts for the ISAO. In addition to a context framework and information uses, we also present a functional decomposition of possible ISAO information sharing activities. This guideline also offers a path to consider for maturing an ISAO's information sharing capabilities. Note that the framework is conceptual as opposed to prescriptive, and inclusion is meant to illustrate options rather than mandate. Information sharing may also be supported by other future relevant documents (statements of principle, policy documents, processes, procedures, data standards, etc.).

SUPPORTING CYBERSECURITY RISK AND INCIDENT MANAGEMENT

Companies, enterprises, and organizations manage strategic and tactical cyber-related risks, as a result of the technology they employ or their interaction with others. Managing these risks entails understanding the environment in which they are operating (situational awareness), determining directions to pursue (decision-making), and detailing efforts (actions) to undertake. These are activities an organization executes daily.

Taking a risk-based approach, where defensive actions and practices are aligned to changes in the cybersecurity environment, an ISAO can assist members in the *decision-making* efforts by identifying possible *actions* to help them establish the appropriate practices to prevent, detect, respond to, and recover from relevant threats, vulnerabilities, and incidents.

ISAOs can perform a significant role in assisting their members and others to better understand various cybersecurity-related risks by providing *situational awareness* of the current and emerging environment in which they and others are operating. An ISAO considering the environment and situation can make decisions and inform its members about threats, vulnerabilities, or incidents that may

be of interest or impact. Further, an ISAO may develop and provide recommended measures or actions to address immediate or emerging changes in the cybersecurity environment of interest to its members. In this way, the ISAO itself is executing the same situational awareness, decision-making, and actions framework in its ISAO support role for its members.

With respect to cybersecurity-related information, an organization has a need for various types of information, which we place for discussion purposes into an *context for information sharing* with two major categories.

The first category of information relates to the purpose for which the information is used. While the overall purpose of information sharing is to enable effective risk management, this can be distilled into three groups of information. These different groups build up to a full spectrum of risk management.

- *Situational awareness* information provides awareness of the broader threat landscape.
- *Decision making* information is customized to a particular organization's needs and enables more effective security management.
- *Action* information directly supports the implementation of a particular measure that improves security.

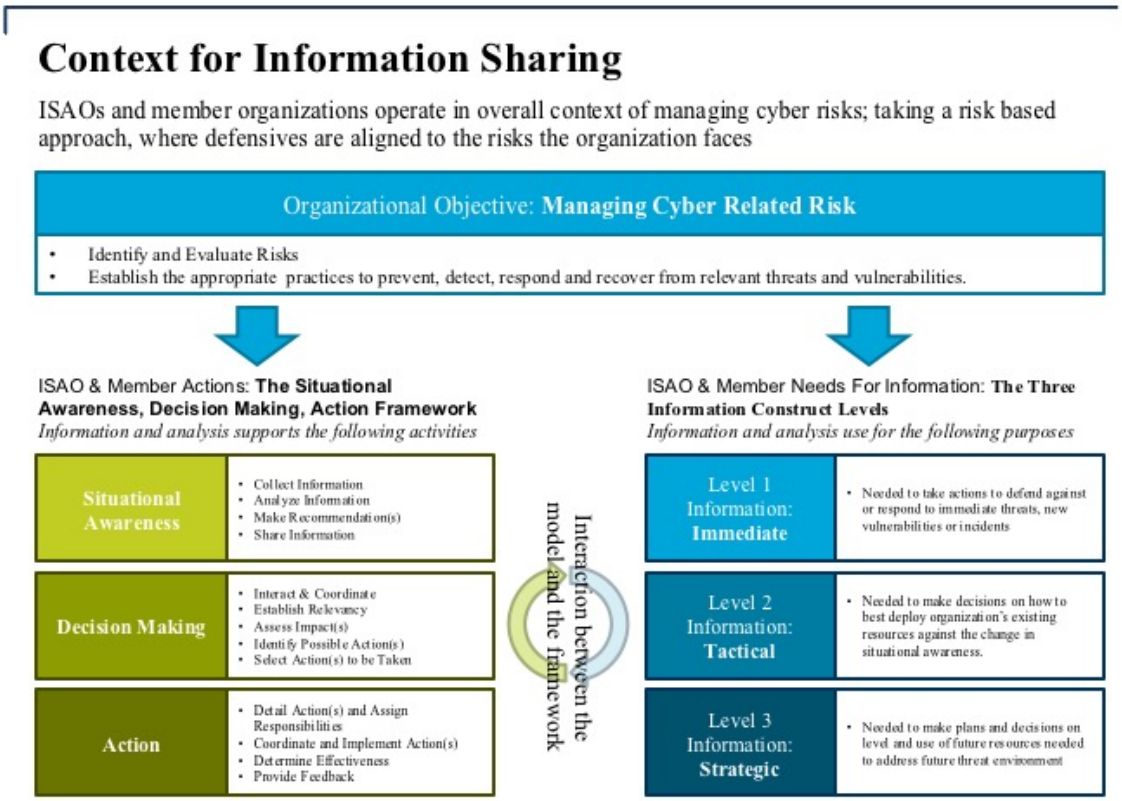
The second category of information revolves around time and the application of resources. This type of information seeks to capture the complementary efforts that need to occur for effective cybersecurity. It begins with information most operationally relevant to security and builds upon it.

- *Immediate* information relates to actions to defend against or respond to new threats, vulnerabilities, or incidents.
- *Tactical* information relates to decisions on how to best deploy organization's existing resources against the change in situational awareness.
- *Strategic* information relates to making plans and decisions on efforts and resources needed to address emerging or future threat environments.

The situational awareness, decision-making, and action framework and the information construct levels are depicted in Figure 1. Conceptually, a mature ISAO will have a close and interactive relationship between the framework an organization is executing and the information sharing construct levels an ISAO is performing.

98 *Figure 1. Context for Information Sharing*

DRAFT FOR REVIEW



99

100 ISAO INFORMATION SHARING VALUE 101 PROPOSITION AND POLICIES

102 Fundamental to the establishment of an ISAO will be the "value proposition" to be
103 offered its participants, partners, and collaborators and the specific categories of
104 information to be collected, disseminated, and shared. The following guidance
105 can assist ISAOs as they develop their information sharing policy considerations.

106 Using the activities and categories of information discussed previously, an ISAO
107 can consider and respond to the questions below to begin establishing an infor-
108 mation sharing policy.

109 • Which categories of information does the ISAO want to provide members to
110 give them *situational awareness* relevant to their affinity group?

111 • Will the ISAO provide raw data, analysis, or both to assist members in their
112 *tactical decision-making* efforts?

- Will members expect information related to *action* recommendations, including defensive measures, best practices, and/or procedures for incident coordination?
- Will the ISAO provide analysis of a *strategic* nature related to trending analysis and threat actor targeting and motivation?

In the context of the framework and information construct levels, Figure 2 presents various interactions to consider as an ISAO develops its information sharing objectives and policies.

Figure 2. Levels of Information Related to Activity Framework

DRAFT FOR REVIEW

The ISAO Framework

	Situational Awareness	Decision Making	Action
Level 1 Information: Immediate Response *(taking actions against immediate threats/new vulnerabilities/ incidents)*	**ISAO Action:** •Collect information on threats, vulnerabilities, and incidents. •Analyze information and make recommendations •Share information with members **Member Org. Action:** •Collect information and share with ISAO •Receive information from ISAO	**ISAO Action:** •Assess potential impact for all members •Response to member queries •Coordination between members •Propose/assess possible actions **Member Org. Action:** •Establish relevancy •Assess impact •Review potential actions •Select actions to take	**ISAO Action:** •Support response to threats •Coordinate joint response •Assess impact of actions **Member Org. Action:** •Respond to shared information
Level 2 Information: Tactical *(using existing resources to protect against changes in situational awareness)*	**ISAO Action:** •Create overall view of current situational awareness and defensive measure practices •Consolidate, enrich, analyze information and make recommendations •Share information with members **Member Org. Action:** •Receive information from ISAO •Interact with other members •Share defensive measures	**ISAO Action:** •Assess potential impact for all or specific members •Response to member queries •Coordination between members •Propose/assess possible actions **Member Org. Action:** •Establish relevancy •Assess impact of existing defensive measures against threat updates and situational awareness changes. Review potential actions •Select actions to take	**ISAO Action:** •Support implementation •Coordinate joint actions •Assess impact of actions **Member Org. Action:** •Implement decided course of action •Review and adjust
Level 3 Information: Strategic *(changing resources based on future threat environment)*	**ISAO Action:** •Trend analysis on information •Publish in-depth analysis •Share information with members **Member Org. Action:** •Receive information from ISAO •Interact with other members •Share strategies and plans	**ISAO Action:** •Response to member queries •Coordination between members •Propose/assess possible actions **Member Org. Action:** •Assess existing resources against future threat environment •Benchmark against peers •Set strategy/plans	**ISAO Action:** •Support implementations •Coordinate joint strategies •Assess impact of actions **Member Org. Action:** •Implement selected strategy •Review and adjust decisions and actions.

CATEGORIES OF INFORMATION AN ISAO MAY WANT TO SHARE

ISAOs can support the interactions shown above in Figure 2 by providing their members information needing immediate action, information of a tactical nature, and/or information of a strategic nature.

This information can be described in categories, namely:

- Threats
- Vulnerabilities
- Targets
- Impacts
- Analysis
- Indicators of compromise
- Tactics, techniques, and procedures
- Incident information
- Campaigns
- Defensive measures and courses of action
- Best practices
- Trending and strategic analysis
- Threat actor targeting and motivations
- Existing industry practices.

{TBD: These categories will be further defined.}

COLLECTION, DISSEMINATION AND ANALYSIS—FUNCTIONAL DECOMPOSITION

NOTE TO REVIEWERS

At this point the information sharing functional components described below are not intended to be a one-to-one mapping to the context depicted above, as the high-level functional categories are generic and support various aspects of the framework. The high-level categories are decomposed into sub-categories to identify the more specific information capabilities needed to support those categories.

This section describes in more detail the functional components of information sharing an ISAO may want to consider.

Participation in information sharing efforts is mainly driven by interests—either personal, organizational, or both. Those responsible for managing cybersecurity risks and taking actions to deal with them will participate in an ad hoc, defined, or institutionalized information sharing activity to better understand the environment in which they are operating and/or to contribute to collective interests.

Personal or organizational interests generally value the following:

- New knowledge for a better understanding of the threat and vulnerability environment in which they are operating
- Recommendations for dealing with specific threats and vulnerabilities
- Receipt of situational alerts that may affect their security posture
- Validation of their understanding of a current situation or incident
- Additional information that may improve their current understanding of threats, vulnerabilities, and/or incidents
- Knowledge of the actions being taken by others
- Coordination of collective actions
- Feedback on the effectiveness of actions being taken by others individually or collectively.

These personal or organizational interests can be used to describe four functional component categories that together make up the broad tactical and strategic efforts that an ISAO can perform:

- Threat landscape awareness
- Response measures
- Coordination
- Trend and pattern analysis.

These broad categories, as shown below, can be further decomposed to more specific functional elements and information sharing capabilities to support the personal or organizational interests of those participating in or working with an ISAO.

THREAT LANDSCAPE AWARENESS

- Collect information.
- General and community of interest focused.
- Make appropriate information available.
- Analyze collected information.
- Develop “alerts” and “notifications.”

RESPONSE MEASURES

- Distribute “alerts” and “rapid notification.”
- Develop countermeasures.
    - Immediate

191 ▪ Long-term
192 • Identify “best” and “good” practice recommendations.
193 • Determine effectiveness.

194 ## COORDINATION

195 • Establish coordination processes and capabilities.
196 • Activate coordination.
197 • Establish coordination efforts.
198 • Assess coordination efforts.

199 ## TREND AND PATTERN ANALYSIS

200 • Retain historical information.
201 • Perform strategic analysis.
202 ▪ Identify trends, discontinuities, or patterns of activity.
203 ▪ Determine threat actors and motivations.
204 • Publish analysis and recommendations.

205 Table 1 describes these categories and sub-categories and identifies information
206 sharing capabilities that support them.

207 *Table 1. Functional Categories and Information Sharing Capabilities*

Functional Category or Sub-category	Description	Information Sharing Capability
Threat landscape awareness	Know what’s going on related to cybersecurity or other issues of interest to the ISAO.	
◆ Collect information: — General.	◆ Obtain threat, vulnerability, and incident information from ISAO participants and other sources for information of interest.	◆ Anonymous and attributable submissions ◆ Email and listservs ◆ Calls ◆ Meetings ◆ Secure portal submissions ◆ Automation feeds ◆ Direct cybersecurity partner feeds ◆ Traffic Light Protocol (TLP) labelling implementation
◆ Focus on community of interest.	◆ As necessary, encourage community of interest participation to build deeper trust relationships.	◆ Similar capabilities as above that can be segregated and tailored for community of interest participants
— Make appropriate information available.	◆ Distribute or make information available in accordance with TLP procedures and labelling.	◆ Distribution through appropriate communication channels (portal access, email, automation platforms, etc.)

Functional Category or Sub-category	Description	Information Sharing Capability
— Analyze collected information.	◆ Review, de-conflict, validate, sanitize, and analyze collected information. ◆ Conduct research or intelligence to alert the members of evolving or existing threats, incidents, and vulnerabilities.	◆ Analysts and analysts' tools
— Develop "alerts."	◆ Identify changes in situational awareness that may be of interest to ISAO participants and others.	◆ Communication mechanisms for levels of alert criticality ◆ Multiple mechanisms for highest level of alerts
Response measures	Establish operational or procedural measures to mitigate the utility or deny the effectiveness of vulnerabilities or exploits to infrastructures, operations, or systems.	
◆ Distribute "alerts" and "rapid notification."	◆ Provide developed alerts and notifications to appropriate participants or partners.	◆ Communication mechanisms for levels of alert criticality ◆ Multiple and diverse mechanisms for highest level of alerts
◆ Develop countermeasures: — Immediate — Long-term.	◆ Develop in collaboration with participants and partners, countermeasures to mitigate risks of new threats or vulnerabilities. ◆ Focus on immediate and then longer term measures.	◆ Conferencing and networking collaboration mechanisms for both technical experts and participants ◆ Access to capabilities that provide searchable topic analysis for participants
◆ Identify "best" and "good" practice recommendations.	◆ Based on interests of participants, make recommendations for "best" and "good" practices to mitigate and respond to cybersecurity and other relevant risks and incidents.	◆ Conferencing, networking, and forums for collaboration among technical experts and participants ◆ Surveying capabilities ◆ Publishing and providing references and a repository for availability of recommendations to participants ◆ Access to capabilities that provide searchable topic analysis for participants
◆ Determine effectiveness.	◆ Develop metrics and perform surveys to continually measure the effectiveness and satisfaction of participants with the services being provided.	◆ Participant survey capabilities
Coordination	Synchronize and integrate activities to ensure the pursuit of the shared objectives established by the ISAO.	
◆ Establish coordination processes and capabilities	◆ Policy and procedures established for assessing the need for coordination among members with shared interests to discuss and coordinated	◆ Communication/network mechanism for a leadership group (identified sub-group) to make a decision to activate coordination.
◆ Activate coordination	◆ Issue notification for an "emergency" call for coordination.	◆ Established diverse communication capability to initiate an "Emergency Call"

Functional Category or Sub-category	Description	Information Sharing Capability
◆ Establish coordination actions/efforts	◆ Establish "playbooks" for various situations where coordination among participants is required.	◆ For ongoing incidents of specified severity implement conferencing capabilities to determine the status, countermeasures, and response information related to an ongoing situation.
◆ Assess coordination efforts	◆ During and following coordination events continually assess decisions and actions taken.	◆ Survey capabilities. ◆ Conferencing capabilities
Trend and Pattern Analysis	Collect information and attempt to spot a pattern or trend derived from the information of interest to the ISAO participants.	
◆ Retain historical information.	◆ Maintain history of submissions, analysis and decisions in a secure database.	◆ Secure operational database and software with appropriate access controls to segregate and deal with various sensitivity of information
◆ Perform strategic analysis: — Identify trends, discontinuities, or patterns of activity. — Determine threat actors and motivations.	◆ Analyze the ISAO historical information along with other information to provide value-added insights on trends and new activity of significant to the interest of participants.	◆ Analysts and analysts' tools ◆ External collaboration mechanisms for analysts to engage other experts
◆ Publish analysis and recommendations.	◆ Regularly communicate with ISAO participants and others based on ISAO policy and procedures.	◆ Communication channels and networking events for members to receive analysis ◆ Access to capabilities that provide searchable topic analysis for participants

208

209

APPLYING SHARED INFORMATION

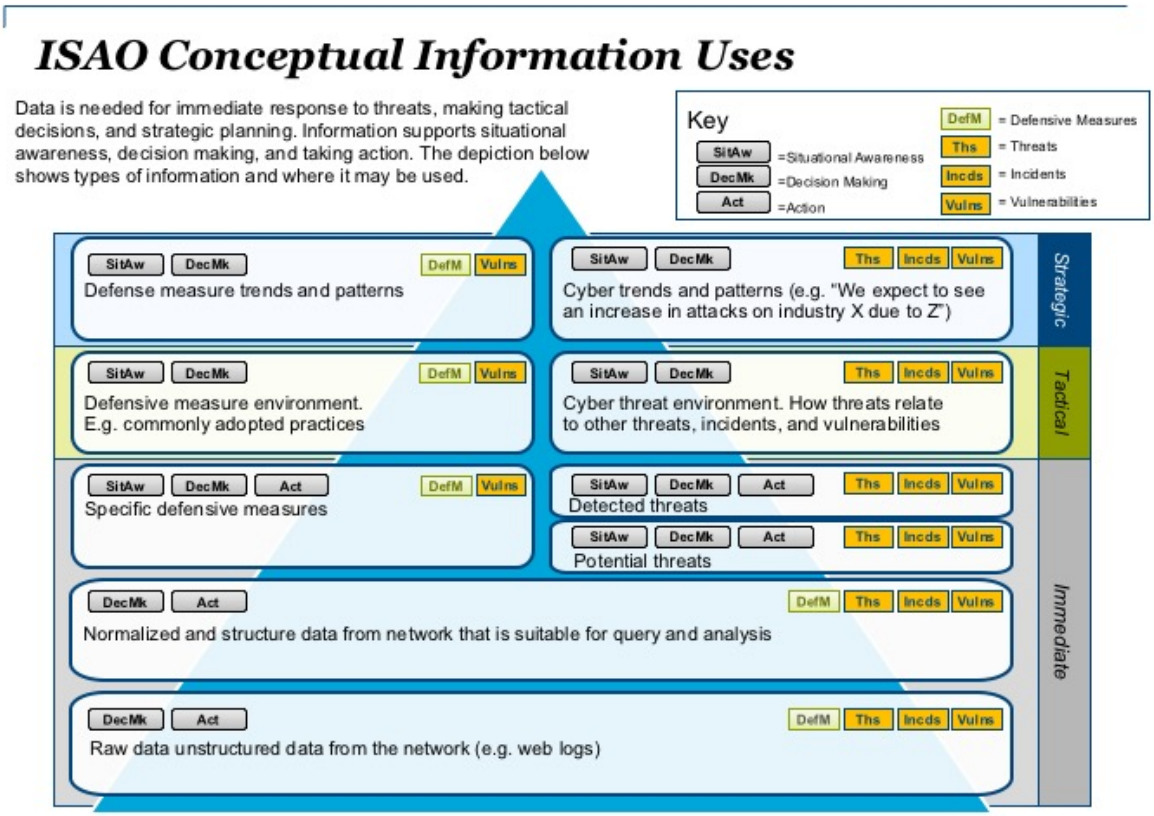
As an example, specific types of information—namely, regarding threats, vulnerabilities, and incidents—can support the framework and an organization's efforts to manage and mitigate its cybersecurity-related risks.

Figure 3 depicts at a high level where specific types of information can be used. The depiction seeks to show the hierarchy of information and how progressive levels of analysis can turn raw unstructured data into valuable knowledge of the environment. Armed with this knowledge, organizations can then prioritize efforts to defend against the most prevalent threats. The categories of information are:

- *Immediate:* Information needs that concern actions to defend against or respond to new threats, vulnerabilities, or incidents
- *Tactical:* Information needs that concern decisions on how to best deploy an organization's existing resources against the change in situational awareness.
- *Strategic:* Information needs that concern making plans and decisions on the efforts and resources needed to address emerging or future threat environments.

Figure 3. Applying Information to Cybersecurity Risks

DRAFT FOR REVIEW



(For future SWG3 development:)

ARCHITECTURAL CONSIDERATIONS

GENERALIZED ARCHITECTURES

- Centralized
- Peer to peer
- Hub and spoke
- Mesh network.

MECHANISMS

(TBD: Level of details and/or references that would be beneficial in this guidance.)

- E-mail/listservs

- Website postings
- Automated (primary indicator and defensive measures, then follow-on information)
- Secure portal
- Direct feeds from threat intelligence firms
- Face-to-face, WebEx meetings, conference calls.

COLLABORATION AMONG ISAOs AND ADVANCED CAPABILITIES

(To be developed:)

- Information sharing capabilities and mechanisms that would help an ISAO achieve the benefits of more active, regular collaboration among ISAOs, partners, and others
- Automated capabilities for information dissemination using a network of standards-based platforms, in addition to advanced capabilities being researched.