James McCabe

From: ISAO <ISAO@lmi.org>
Sent: Monday, December 07, 2015 7:51 AM
Cc: Lipsey, Richard
Subject: ISAO SO Data Call and Initial Standards Working Groups
Attachments: Lessons Learned and Best Practices Data Call.docx; Detailed Working Group Topic Inputs.pdf; Working Group Application Form (v1).pdf

Thank you very much for your interest in improving the cybersecurity posture of the Nation through improved cybersecurity information sharing. As discussed during our initial public meeting on November 9th, the Information Sharing and Analysis Organization (ISAO) Standards Organization (SO) is sending out a data call to request specific best practices, documents, and templates that can be used by entities that are forming ISAOs today. In addition, we are announcing the stand up of six initial standards working groups and soliciting volunteers to help develop the principles, policies, processes, standards, guidelines, and templates to promote effective cybersecurity information sharing.

We appreciate your interest and look forward working with you in the weeks and months ahead. If you have any questions, comments, or suggestions, please contact us at ISAO@lmi.org

Regards,

Rick

Richard A. Lipsey

Deputy Director, ISAO Standards Organization

LMI

1777 NE Loop 410, Suite 808
San Antonio, TX 78217
(210) 526-8186

ISAO SO Data Call and Initial Standards Working Groups

Cybersecurity information sharing is not a new concept. For over a decade, the need to share information regarding cybersecurity vulnerabilities and incidents has been recognized by the community and much has been

done (such as the creation of the various ISACs) to address the need. The effort has continued with the issuance of Executive Order 13691, which directed the creation of the Information Sharing and Analysis Organization (ISAO) Standards Organization (SO). The SO seeks to assemble and build upon the many successes already achieved and to identify (or develop where needed) standards, guidelines, best practices and other products that will help build a national program of voluntary cybersecurity information sharing.

Since the announcement of EO 13691, government and industry have begun to identify the issues that must be considered in identifying the guidance that is needed. Several public forums have been held to discuss various aspects of information sharing and many additional comments have been provided on the subject via calls for comments. Coupled with the lessons already learned by existing information sharing organizations, there is a growing body of knowledge addressing various aspects of information sharing. The ISAO SO is aware of this material and is considering all information already provided when launching the various efforts to develop the guidance for new ISAOs. This announcement is one of the first efforts by the Standards Organization to solicit comments on specific aspects of information sharing.

Data Call Follow-Up

The initial ISAO Standards Organization public meeting on November 9, 2015, produced excellent feedback from the participants. (For meeting agenda, briefings, audio files, transcripts, and reports, go to http://www.lmi.org/ISAO-PublicMeeting.) This feedback made references to best practices, processes and other resources. For those who would like to provide additional input or to share templates, best practices, and other documents, please complete the attached "Lessons Learned and Best Practices Data Call" document and send your inputs to ISAO@lmi.org with the subject line: "*Data Call Resources*". The information collected will be used to develop interim solutions for communities of interest wanting to stand up an ISAO quickly while formal standards are being developed.

Initial ISAO Standards Working Groups

There are many issues that need to be considered and we aspire to address all of them at the appropriate time through a voluntary consensus standards process that is open to the public. A list of topics identified to date is included in the document titled, "Detailed Working Group Topic Inputs." Having said this, our initial focus will be on providing the tools needed to allow entities wishing to form an information sharing organization to avail themselves of relevant cybersecurity information to more effectively defend themselves in an increasingly hostile cyber environment.

With the announcement of EO 13691, a number of organizations have come forward expressing a desire to form an ISAO. Accordingly, we plan to collaborate through standards working groups to develop basic guidance that can be provided to entities that want to form ISAOs today. We need to quickly determine what is needed to help them get started on the right path—recognizing that standards, best practices, and other guidance will

follow as our standards working groups do their jobs. These new entities need to be brought into the larger national information sharing infrastructure being created as we work to clarify how information sharing will be accomplished across the various types of existing and emerging ISAOs.

Based on our initial focus, we are asking for individuals to identify their interest in participating in one (or more) of six working groups. Although other working groups may be formed later, we believe these are the initial working groups that are essential to meet the immediate needs of emerging ISAOs. We will also be looking to these initial groups to help us develop effective working relationships between the groups and the ISAO SO. As working group processes are established and other topic areas identified, additional working groups will be created and a call for participation in them will be issued.

The working groups will:

· Be open to anybody who wishes to join.

· Be led by a core development team of (ideally) 7 to 10 members, but no more than 20.

- Core development team members will be asked to volunteer the time required to attend periodic meetings and to develop products based on input from the working group membership and the public.

· Develop products which may include statements of principle, policy documents, process flow diagrams, standards, templates, guidelines, best practices, etc., as appropriate.

Working Group 1: ISAO Creation

Objective: Identify and capture the elements necessary for an interested organization to stand up an ISAO. These elements will serve as the basis for creating an ISAO and will have enough flexibility in design to fit the needs of diverse interested organizations.

Working Group 2: ISAO Capabilities

Objective: Identify and capture the capabilities necessary for an interested organization to effectively operate an ISAO. These capabilities will support day-to-day operation of the ISAO and support its main function: to share and receive cyber information in a timely and effective manner. Capabilities must allow for the most basic ISAO and also support more sophisticated organizations.

Working Group 3: ISAO Information Sharing

Objective: Identify and capture items and develop the guidance necessary for an interested organization to effectively share cyber information (threat indicators, vulnerabilities, and best practices) within their ISAO or externally.

Working Group 4: Information Privacy & Security

Objective: Identify and capture the steps to safeguard information (both proprietary and privacy related). Detail the processes and procedures to prevent unauthorized release or access to information not cleared for release. Address how to meet Federal, State, Local, and Tribal laws regarding privacy.

Working Group 5: ISAO Support

Objective: This working group will consist of individuals familiar with the creation and operation of information sharing organizations who will work to support emerging ISAOs as they are created. This working group will work closely with the ISAO SO to provide assistance to emerging ISAOs.

Working Group 6: Government Relations

Objective: This working group will identify and address issues associated with ISAO interactions with the Intelligence Community, Law Enforcement, US Regulators, and Homeland Security.

Call for Participants

Developing effective information sharing standards and processes to bolster the Nation's cybersecurity posture requires the engagement of a variety of subject matter experts with diverse backgrounds and experiences. We are looking both for general members for each of the six initial working groups as well as core development team members for each group. Core development team members must be energetic, experienced and ready to develop comprehensive, workable solutions. Most importantly, core members must be able to work well in groups and to foster collaboration that leads to consensus.

Your participation is welcome and essential. Action is needed and we anticipate a robust activity schedule driven by the urgency of this national issue.

Interested parties are asked to complete the brief Working Group Application Form and e-mail it to ISAO@lmi.org with the subject line: "*Working Group Membership*" expressing their desire to participate, either as a general member or as a core development team member in one or more of the working groups outlined in this document.

MEETING THE URGENT NEED: SHARING LESSONS LEARNED AND BEST PRACTICES

Introduction

On November 9, 2015, the ISAO Standards Organization held its first public meeting. This forum produced excellent feedback from the participants who were able to attend. We are distributing this handout, which is based on similar questions asked at the first public meeting, to gather feedback from those who were not able to attend as well as more detailed information from earlier respondents. In addition, we are seeking existing documents and artifacts that can be used as templates for new ISAOs that are being established (e.g., charters, membership forms, non-disclosure agreements, briefing charts, etc).

The following questionnaire will identify focus areas that have been acknowledged previously by the information sharing community. In addition, there are bullets describing some of the areas of concern that have been communicated. Please answer the questions provided from your perspective (as an information sharing organization or as a potential member of an information sharing organization).

Thank you for engaging in this effort. We look forward to the community's support.

Please send your Data Call document and any available template documents you'd like to share to ISAO@lmi.org with the subject line: "*Data Call Response*".

Threat Information

- Sharing (establishing norms; when to involve law enforcement)
- Receiving (contending with duplicate indicators)
- Verifying (establishing fast and effective methods)
- Analyzing (is this part of something bigger)
- Distributing (sanitizing considerations)
- Timely (establishing a threshold to be timely)
- Actionable (information members can act on)

What is the most significant challenge a new ISAO will face in regard to sharing threat information?

What are your most important best practices in this area?

ISAO membership

- Building membership (identify your core membership)
- Maintaining membership (organize meetings with like-minded organizations to build trust)
- Meeting the needs of the ISAO members
    - Large organizations
    - Small and medium-sized businesses

What will be the greatest hurdle for a new ISAO?

What are the barriers that prevented or discouraged some members from joining and what did you do to overcome it?

What best practices would you suggest?

Products

- Awareness Programs
- Mentoring
- Technical tools/toolkits
- Technical guidance and/or training
- Research and development
- Webcasts/Podcasts/Webinars
- Cyber threat indicators
- Cyber incident response capabilities
- Analytical support
- Threat intelligence information
- Best practices for new threats
- Exercises

For Information sharing organizations:

- **What products are most utilized and/or needed by your members?**

For those *not* in information sharing organizations:

- **What products would you want and why?**

Governance (system of rules, practices, processes)

- Governance structure (keeping it flexible)
- Traffic Light Protocol (sensitive information distribution)
- Insurance needs (liability protection)

In your experience, what governance issues are the most difficult to address and how did you overcome them (if you have)?

What best practices would you suggest?

Formal and/or Legal agreements

- MOUs, MOAs
- NDAs (used in establishing trust)
- Contracts
- Regulatory requirements (if applicable)

Areas to address

- Who owns the information
- How the information is used by members

What are the main formal or legal agreements that are needed in an information sharing organization?

Which agreements are needed first and why?

Trust and Privacy

- Building and maintaining membership trust
  - Secure member portal
  - Anonymization of member reporting
  - Managing perceptions (public/members) when working with the government
- Meeting privacy standards and regulations
  - Encryption methods for information distribution and storage
  - Redacting PII and health information

What practices have you implemented that resolved a trust issue? What was the issue and how did it solve the problem?

Identify a best practice for managing privacy requirements.

Other

What other recommendations would you add?

The information below captures the detailed inputs provided by participants during the ISAO Framework Breakout Sessions at the November 9, 2015 Open Forum held at LMI HQ, together with inputs gleaned from prior DHS workshops. Participants were requested to post their best practices, challenges, issues, concerns on the four topics listed below. Items below with two asterisks were identified by participants as being a priority.

These inputs are provided for working group consideration as principles, policies, procedures, processes, guidelines, and templates are developed. As the working groups are formed, each will be asked to consider a subset of these, and subsequent, issues.

ISAO Creation and Business Processes

1) Will there be a requirement to have articulated bi-laws, membership qualifications, and guideline for participation?

2) Define how protection of intellectual property of members will be accomplished.

3) Define Membership benefits: Include connectivity, access to government, cyber threats, sharing among members/other ISAOs, education, awareness.

4) Articulate the organizing principles of an ISAO.

5) Define the means to scale the size and operation of an ISAO.

6) Explain the vetting process for membership if any.

7) Charter development- include objectives, talent, requirements, acquisition, retention, executive strategy, and oversight mechanism.

8) ISAO Policy Development Process: describe how an ISAO develops its policies.

9) Standard Operating Procedures and/or Tactics/Techniques/Procedures: detail the authority to develop/implement and revise.

10) **Capture ISAC best practices, method of engagement and what metrics are best captured and analyzed.

11) Prescribe how an ISAO advertises itself to attract membership and sharing of information.

12) Certification: Characterize what method of certification to use (i.e. self, third party, or none).

13) Describe a standard public-facing web page. Migration to details will be unique to the ISAO.

14) Define what membership is, what the expectations are to be a member, and how membership rules are enforced.

15) Articulate the mechanism for sharing best practices across different ISAOs.

16) Describe the difference between an ISAO and an ISAC in order to advertise the benefit of an ISAO.

17) **Identify how each ISAO may discuss problems that their organizations are solving and communicate that (all hazards, cyber vs physical) to all ISAOs.

18) Define how to structure ISAOs: state, local, regional, sector, and cross-sector.

19) **Establish rules of engagement to create trusting relationships.

20) Specify how to be self-sustaining. Should memberships be free or paid or paid on a sliding scale?

21) Business process: clearly define how info is tracked, used, shared, and what method will be used to protect the data.

22) **Legal issues: define privacy and create/embed strong encryption in order to protect data which resides within an ISAO.

23) **Must share actionable intelligence through an enabling exchange and response of a coalition of ISAOs.

24) **Consider Not-For-Profit legal structure and avoid vendor driven solutions.

25) Allow boards and policy makers to drive finance and legal issues.

26) Members should voluntarily in writing agree to meet framework guidelines which are designed to be flexible in order to meet the differences that will occur in ISAOs.

27) **Develop clear criteria and standard terminology to create an ISAO.

28) **Seed funding: Detail a sustaining financing model.

29) **Membership eligibility: US? International? Government?

30) **What consideration is being given to include foreign companies or U.S. companies based in foreign countries?

31) Who verifies certification compliance?

32) How often are tiers analyzed and validated?

33) **What consideration is being given to develop a national council of ISAOs?

34) Define the business structure of the ISAO: Profit, Not for Profit, Incorporated, etc.?

35) What liability protection is envisioned for ISAOs and members: what will it look like?

36) Is it decided each ISAO will be independent of other ISAOs? Or, is there a model for ISAOs associated with other ISAOs?

37) Will consuming ISAOs be allowed or must it be a give and take relationship in regards to information sharing?

38) **Characterize the relationship of regulators and ISAOs.

39) What applicable contracts, agreements, etc. will the ISAOs be required to have or should have?

40) Will ISAOs be provided business plans, organization structures, roles, and responsibilities when standing up?

41) What methodology will be used to share ISAC best practices with ISAOs?

42) Establish information sharing procedures, process, and standards for ISAOs prior to their operation.

43) To create an ISAO must have a common objective/goal, time, not necessarily dollars.

44) Business process documents should cover common objectives, charter, and standardized components across all ISAOs

45) Establish the leadership and management model for ISAOs.

46) Additional core components besides shared need, trust, requirements, and business build out be identified and captured.

47) Each ISAO must have objectives defined, internal governance framework, decision processes for voting and elections, and should consider mentor/protégé relationships with successful ISAOs.

48) Identify the structuring for enforceable partnering and member agreements.

ISAO Capabilities

49) Define the ability of an ISAO to perform analysis on member information that is shared within the ISAO and on information shared from external sources.

50) Articulate the technical/analytic expertise in cyber security in a baseline.

51) Develop an "easy button" from set up to full capability as a baseline.

52) Delineate the capability required to effectively use STIX and ATXII.

53) Develop a baseline for operational, technical, analytical, and personnel capabilities to operate the ISAO information sharing effectively.

54) Some ISAOs will have strong analytical capabilities but others likely will be limited to sharing and will lack analysis capabilities. Define a process that will accommodate this disparity.

55) Identify certifications (technical/analytical) to be required.

56) Identify what capabilities will be in each tier level.

57) What are the recommended mechanisms for establishing trust? In person? Coordinated? Collaboration?

58) Will there be a requirement for a common operating picture? If so, how will it operate and what will the COP encompass?

59) What is envisioned for an event driven ISAOs?

60) **Leverage existing standards (found in ISACs, ANSI, etc.) as much as possible

61) Avoid trying to be everything to all members

62) Various means of communication are required i.e. push-pull capabilities which includes structured data in an expected format. What capabilities are required to perform this communication?

63) Identify the capabilities needed by an ISAO for managing, handling, and sharing classified information.

64) Develop the baseline and procedures for prioritizing/operationalizing information for exchange.

65) Procedures for the capability for real time or near-real time exchange.

66) ISAO workforce development/training opportunities established in ISAO business plan.

67) Core set of capabilities (operational/technical/analytical/personnel) for each tier.

68) Prescribe the level of analysis (e.g. network traffic, malware, mitigation action) to be done by ISAOs.

69) **The more mature/robust the ISAO capabilities the more expensive it becomes to operate. Capture this reality.

70) Analytical capability skills also include aspects of security, intelligence information, and business acumen.

71) **Personnel must have ability to identify requirements (RFI/PIR/IR)

72) Is there a dividing line to determine the best choice between in house analyst and managed surfaces?

73) Limit membership to IT security professionals only?

74) Engagement and outreach for ISAO members is imperative: business analysis, process and project management, admin all support an ISAO.

75) Refine capabilities to meet objectives, member information requirements, communication mechanisms.

76) **A tailored environment is best to meet member requirements. Meaning, each ISAO is likely to have different needs, expectations, and capabilities.

77) External partnerships should include both strategic and tactical.

78) Develop symbiotic process between ISAOs to build on strengths and reduce weaknesses.

79) ISAOs must exist in a collaborative culture to be effective. Develop the procedures and support mechanisms to achieve this culture.

80) An ISAO must have the ability to consume information and not necessarily contribute.

81) Define membership qualifications, if any.

82) Membership experience should be driven by the charter.

Information Sharing

83) Need to establish business vocabulary so everyone is on same sheet of music.

84) What are expected sources of information: Researchers, hackers

85) How does one ISAO tie with another ISAO for info sharing?

86) Need a process for vetting of data and information received

87) Confidentiality of information source is important but how to do?

88) What will be the measures for effectiveness for information that is shared?

89) Develop the processes for one ISAO to be aware of similar ISAOs for best practice and info sharing.

90) Define the expected quality of data that an ISAO will use.

91) Establish the timely and actionable sharing of information definition.

92) Determine if security clearances will be needed to receive classified information from the Gov't or other ISAOs and how the clearances will be issued, maintained, and who holds the clearances.

93) Characterize how confidentiality of information will be managed, how disclosure is handled.

94) Determine how information may be shared with either international ISAOs or US companies who are based in a foreign country

95) Procedures for establishing a global network of ISAOs

96) Develop a consistent and standard method to share cyber threat information (attacks, successful hacks, incidents, vulnerabilities) as well as best practices amongst ISAOs.

97) Define process for scaling information that is shared.

98) Procedures (mechanism) for sharing information in real time or near-real time, daily, weekly). Automated sharing is the only means to inform at speed of thought for maximum awareness and protective measures to be applied.

99) Determine if all information shared will have the same weight or if information, depending on its importance, can be prioritized.

100) Develop principles that address sharing risk, confidentiality, shared interests, recognizing differences.

101) Explain data acceptance, protocols, and options when using automated information sharing systems.

102) Define the vetting process for information sharing regarding source of information, describe how information is to be validated.

103) Maximize use of information sharing techniques and procedures from existing ISACs, to include leveraging existing structures, policies and procedures.

104) Develop procedures for information sharing within the ISAO to its members.

105) Develop the process for the ISAO to share to the US Government its cyber threat information.

106) Establish MOU's, MOA's for sharing information within and outside the ISAO.

107) Utilize existing terminology from the NCCIC, NIST, and other established sources for consistency.

108) Determine if STIX, TAXII, NIEM will be the standard for ISAO information sharing transmission and receipt.

109) Decide if sharing with other organizations such as Carnegie Mellon is possible. Would establishing an MOA with such organizations be within a charter?

110) Address the legal framework amongst members and other ISAOs (and Gov't) for a sharing agreement realizing that legal agreements will not fit all ISAOs.

111) Detail the process and procedures for an ISAO to allow or deny information from an anonymous source.

112) Define what types of information is to be shared: contextual, technical. What does the information look like in order to be helpful?

113) Define the steps needed to handle intellectual property and to safe guard it. Include MOA's or legal documents to be recognized prior to release of IP.

114) Develop the definitions for requiring attribution of the information, either from a fellow ISAO, Gov't or if attribution is to the hacker.

115) Documentation regarding Trust must be for the trust of members and other ISAOs/Gov't, trust of the technology used (its security level) and trust regarding the info sharing process.

116) If anonymous submissions are received (permitted) validation must somehow be available.

117) Transparency must be balanced with issues such as FOIA, and any requesting information not be shared (PII or anything regarding privacy.

118) Key focus is on trust and the ISAO culture and not technology. What features, within principles and policy, add trust?

119) Process must determine who handles the information and further sharing.

120) Policy to identify the limits for which the information may be used.

121) ISAO policy and procedure/process includes the approved secure method for sharing information. Whether it be STIX, TAXII, or other means (e.g. email, portal, website) all must be encrypted in transit and at rest.

122) Develop a standard, yet flexible, Non-Disclosure Agreement that details how info can be used, shared, and stored.

123) Policy covering participation requirements need to be flexible and not rigid in order to attract membership.

124) Policy must address the "free riders": those who only wish to consume and not share. Some ISAOs will be ok with this others not.

125) ** Avoid TLP, does not give quantifiable values, only subjective visuals. However, when possible develop informative TLP for the right situations.

126) Develop policy which address member and ISAO liability protections when sharing information.

127) Vetting of candidate members will be included within the policy document(s).

128) Create procedures which includes the process of developing, maintaining, maturing relationships with members and other ISAOs.

129) Create a "scoring" mechanism for the quality and usefulness of information shared.

130) The biggest identified factor regarding trust is confidentiality of sources and internal personal information. The policy should address this factor and how it is to be implemented and enforced.

131) Policy and procedures include accountability measures for actions taken by members of an ISAO and other ISAOs.

132) Describe what the Gov't will want regarding ISAO information passed up to them.

133) Identify what is to be shared with Members and with other ISAOs.

134) **The owner of the information needs to drive decision on what to share.

135) A mechanism to be developed to also include sharing of vendor cybersecurity information whether it is about cyber threats, best practices, or vulnerabilities.

136) Describe how "triage" information is shared on how to take action on a threat or vulnerability.

137) Detail how data integrity will be maintained when sharing.

Privacy & Security

138) Develop a process to redact privacy information or personally identifiable information.

139) Include in the Procedure and Process documents the way to safeguard information. This includes ALL data: threat information, personally identifiable information found in shared information as well as all member information.

140) Intellectual Property will be addressed in the procedure and process documents and may include the development of NDAs and other legally binding documents.

141) Determine which federal, state and local laws need to be followed and what validates compliance with these laws and regulations.

142) Consider when developing procedures and processes to use best practices already in use by the ISACs.

143) Define Personally Identifiable Information and provide examples.

144) Sensitive information needs definition (with examples) in the procedure and process documents.

145) Regulatory interface with ISAOs captured in procedures and process document as well as the ISAO Charter.

146) Describe the authentication for accessing the ISAO website (for members) and documents/cyber threat info which may be sensitive.

147) Consider a "safe harbor" to provide wanted/needed protections when sharing with regulators.

148) Capture how the US Gov't will declassify information in order to get to ISAOs.

149) Develop a Privacy Policy.

150) Address in Policy, Procedures, and Processes how to work with aggregated data that may become highly sensitive when looked at as a whole.

151) Define information classification levels. That is, sensitive, confidential, four official use by ISAO, etc.

152) Characterize what protections can be offered to Members/ISAOs for privacy if the ISAO shares with the US Government.