Initial Public Meeting of the Information Sharing and Analysis Organization (ISAO) Standards Organization

November 9, 2015

"The What": An ISAO Framework of Standards
Executive Summary and Minutes of Breakout Sessions

Background: The objective of these sessions was to identify topics for future ISAO standards working groups to address. Participants in each of the three sessions broke into 3 groups. Each group discussed 4 topic areas and captured input in a brainstorming style environment. Each group captured input by documenting comments on the framework input sheets that were taped on the wall. The participants' documented comments for each of the 4 topic areas are provided below following this executive summary.

Each session commenced with a slide presentation which framed the discussion, listed suggested principles the Standards Organization will follow, and provided a framework describing initial topics for the working groups and the products the working groups develop.

The four topics (for initial working groups to work) to brainstorm included ISAO creation & business processes, ISAO capabilities, Information Sharing, and Privacy & Security. An example of a topic, Membership, was presented so the participants could see what was desired to gain from the sessions.

Instructions on the brainstorming session were presented before breaking into three groups to work the four topics. It was underscored that while issues may be captured they would not be adjudicated in the sessions: the adjudication would be performed by the working groups. The three groups for each of the three breakout sessions had approximately 60+ minutes to brainstorm the four topics.

The Moderator and Facilitator were supported by a note-taker to ensure maximum capture of all discussions.

At the end of the 80 minute session the group moved to their next breakout area.

Synopsis: The participants of each breakout session quickly broke into three similarly-sized groups and started brainstorming each of the four topics. The moderator and facilitator moved through the groups offering suggestions when the groups got stuck and providing options to consider for putting up the best practices, challenges, issues, considerations, and all ideas. When a few issues were taking over progress it was directed the issue be captured (and identified as such) and keep moving onto the next thoughts. This was repeated for each session with similar interactions between the moderator/facilitator and participants.

The passion was absolutely evident. People from different organizations, different backgrounds all coming together in a group to work on topics and they worked feverishly, excitedly, throughout the 60-70 minutes and sometimes even beyond. They shared ideas across the board but it was the teamwork of the folks working together to come to contribute those ideas, issues, best practices, ideas. There was a lot of information and material that came out that was above and beyond in the DHS workshops. The one complaint was that the sessions were too short. Folks were really getting into the rhythm of the brainstorming and opportunities that we perhaps lengthen those in the future for more information.

So, some of the items that came up and there were differences in opinion on it: funding was a concern. Some questions were:
How do you start up an ISAO?
How do you maintain an ISAO?
Who certifies an ISAO and how. Self-certification was also discussed and, if so, how is it recognized?
What's the purpose of an ISAO?
What's required to create an ISAO?

At the beginning of each breakout session it was emphasized there were no bad inputs: only missed opportunities.

The information captured has been distilled and will be provided to working groups for each of the four topics worked in the breakout sessions.

Breakout Session Topic 1: ISAO Creation and Business Processes

The ISAO Creation and Business Process sessions returned 48 items of interest. The captured items included several considered to be priorities. These were characterizing the relationship of ISAOs with Regulators, consideration for a National Council of ISAOs, standardized criteria and terminology to create an ISAO, and whether an ISAO should have a for-profit or non-profit structure. The items will be further condensed and likely addressed at the next Forum in February.

Breakout Session Topic 2: ISAO Capabilities

The ISAO Capabilities sessions returned 34 items of interest. The importance of the ability of each ISAO to be "tailored" regarding its capabilities was due to the differences likely to be exhibited by each ISAO. Each ISAO will have different needs, expectations and capabilities. It was suggested that as an ISAO becomes more mature and robust it will become more expensive to operate. The more sophisticated the technical acumen the ISAO has the more it will cost in technology and personnel expertise. Also, it was highly recommended to leverage existing standards found in ANSI and ISACs, as examples, in order to streamline development and reduce overhead of standing up.

Breakout Session Topic 3: Information Sharing

The ISAO Information Sharing session returned 55 items of interest. Everything from how information is characterized to the transport and distribution methodology was captured. The importance for procedure establishment and ownership of the information that is shared was also identified. Questions and concerns were raised regarding sharing with the US Government. Additionally, trust was a recurring topic: how to trust the information if from an anonymous source, trust of any information shared (attribution of the source), transparency of sharing, and "scoring" for the quality and usefulness of the information. Avoiding "paralysis by analysis" was discussed meaning how to refine and distill incoming information so a "fire hose" effect is eliminated.

Breakout Session Topic 4: Privacy and Security

The ISAO Privacy and Security session returned 15 items. The reason the number returned was small was because the capture of the discussions across three breakout session were almost identical. One item was the process needed to redact privacy and personally identifiable information. Procedures are needed to safeguard information received and/or transmitted. How Federal, State, and Local privacy laws are to be followed was another recurring concern. Also, the method the US Government will use to declassify information to be shared while still making it useful and relevant was a question. Most information needed to understand zero-day exploits will likely be very sensitive and classified. It was strongly suggested the Working Group for Privacy develop a policy that is usable by all ISAOs and not have much flexibility.

"The What": An ISAO Framework of Standards Breakout Session Capture of Best Practices/Challenges/Issues/Ideas/Concerns

The information below fully captures the information provided by participants during the ISAO Framework Breakout Sessions at the November 9, 2015 Open Forum. There were four ISAO topics and participants were requested to post their best practices, challenges, issues, concerns on these topics. The information below is for Working Group consideration when principles, policies, procedures, processes, guidelines, and templates are developed. In addition to the breakout sessions input gleaned from two DHS workshops held in 2015 are included as well as additional input from a note-taker in the break-out sessions. Items below with two asterisks were identified by participants as being a priority.

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.


CIAS
CENTER FOR INFRASTRUCTURE ASSURANCE AND SECURITY
U T S A


LMI
Complex Problems. Practical Solutions.


R-CISC
RETAIL CYBER INTELLIGENCE SHARING CENTER