ISAO Startup Topics

Draft Document—Request For Comment

SWG G 1—2016 v0.2

ISAO Standards Organization
Standards Working Group 1: ISAO Creation
Frank Grimmelmann, Co-Chair
Deborah Kobza, Co-Chair

May 2, 2016

Table of Contents

Revision Updates

Item	Version	Description	Date
1	0.1.1	Initial Draft ISAO Creation Voluntary Standards	April 29, 2016
2	0.2	Prepared for RFC	May 2, 2016

INTRODUCTION

The importance of information sharing to computer security has been discussed for well over a decade. Early realization of its importance led to the creation of Information Sharing Analysis Centers (ISACs) for the nation's critical infrastructures. In February 2015, the White House issued Executive Order 13691 Promoting Private Sector Cybersecurity Information Sharing (EO 13691) which called for the Secretary of the Department of Homeland Security (DHS) to "strongly encourage the development and formation of Information Sharing and Analysis Organizations (ISAOs)." These new entities could be "organized on the basis of sector, sub-sector, region, or any other affinity" which greatly expanded the number and type of information sharing organizations that will be developed. To help with the establishment of ISAOs, EO 13691 directed DHS to "enter into an agreement with a nongovernmental organization to serve as the ISAO Standards Organization" (ISAO SO).

In developing the standards, guidelines, and other documents that are needed to help entities create and operate ISAOs, the ISAO SO established a number of Standards Working Groups (SWGs). These groups were created to address specific areas pertinent to the creation or operation of ISAOs. When developing the various documents, the SWGs must consider the two overarching efforts important to ISAOs which are 1) the sharing of cybersecurity information, and 2) the analysis of the information that has been shared. The purpose of these efforts is ultimately to improve the nation's ability to "detect, investigate, prevent, and respond to cyber threats" while protecting the privacy and civil liberties of citizens.

To accommodate the expanded list of entities that can form ISAOs described in EO 13691, there will be different types of ISAOs with different objectives and capabilities. There will also be varying levels of organizations within the ISAOs and there may be commercial entities that form to provide services to ISAOs. Some ISAOs may be formed on a very informal basis and may have little or no desire to collect and analyze the information in near real-time for its members. Other ISAOs may be highly interested in near real-time analysis and dissemination of actionable information to better protect its members and may have as an objective the ability to help in the response to security incidents affecting its members. Additionally, an ISAO may initially form with few objectives and target capabilities but then may evolve over time to increase its ability to assist its members by adding additional capabilities and objectives. For example, an ISAO may initially be created to simply share cybersecurity related information among security professionals in its member organizations; then increase the type and frequency of information shared and add the capability to analyze shared information to better detect and prevent cybersecurity attacks; then ultimately add a 24/7 operational capability that can assist its members with ongoing cybersecurity incidents. The goal of the ISAO SO is to be as inclusive as possible in finding a place for any individual or organization that wishes to be part of the nation's overall information sharing program.

This document, and its separate sections, is designed to take into consideration the different types of ISAOs that may be formed and the various levels of capabilities each may incorporate. The document provides an overall organized approach to development of the various documents pertinent to ISAOs while considering the immediate needs of emerging ISAOs. Individual SWGs will develop and refine specific sections of this document in coordination with other SWGs as directed by the ISAO SO, and will consider how each section must fit into the larger picture defining the creation and operation of an ISAO.

PROBLEM STATEMENT

EO 13691 clearly lays out the problem that is being addressed by the creation of a network of ISAOs. It states:

In order to address cyber threats to public health and safety, national security, and economic security of the United States, private companies, nonprofit organizations, executive departments and agencies (agencies), and other entities must be able to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible.

Organizations engaged in the sharing of information related to cybersecurity risks and incidents play an invaluable role in the collective cybersecurity of the United States. The purpose of this [effort] is to encourage the voluntary formation of such organizations, to establish mechanisms to continually improve the capabilities and functions of these organizations, and to better allow these organizations to partner with the Federal Government on a voluntary basis.

Such information sharing must be conducted in a manner that protects the privacy and civil liberties of individuals, that preserves business confidentiality, that safeguards the information being shared, and that protects the ability of the Government to detect, investigate, prevent, and respond to cyber threats to the public health and safety, national security, and economic security of the United States.

To address this problem effectively will require more than just the establishment of a number of disparate information sharing organizations. It will require a coordinated program that effectively identifies and considers the existence and ongoing formation of ISAOs to understand where information sharing is occurring, and the impact said sharing is having. Additionally, the program needs to consider how the efforts of individual ISAOs can be combined into an overarching information sharing program for the nation to improve the cybersecurity resiliency of participants. This program must be as inclusive as possible, appropriately incorporating vetted information from multiple sources. Due consideration must be given to such information to determine the level of trust that can be placed in it which requires that the national program address related issues such as trust, reliability, and overloading of information.

WHAT IS AN ISAO?

Definition: The term “Information Sharing and Analysis Organization,” or ISAO, means any entity or collaboration created or employed by public- or private-sector organizations, for purposes of—

- Gathering and analyzing critical cyber and related information in order to better understand security problems and interdependencies related to cyber systems, so as to ensure their availability, integrity, and reliability;
- Communicating or disclosing critical cyber and related information to help prevent, detect, mitigate, or recover from the effects of an interference, compromise, or incapacitation problem related to cyber systems; and
- Voluntarily disseminating critical cyber and related information to its members; federal, state, and local governments; or any other entities that may be of assistance in carrying out the purposes specified above.

[NOTE: Definition coordinated with SWG chairs in late February 2016, but will be refined in concert with standards development deliberations.]

EXPLANATION AND EXAMPLES

ISAOs consolidate, analyze, and distribute cyber information to their members Overview of ISAO categories and capabilities.

104 ISAO STARTUP TOPICS

105		**ISAO SUPPORT FOR ORGANIZATIONS**
106	SWG 2	While recognizing there is no single description of the capabilities an ISAO will exhibit that will fit all ISAOs that will be formed, it is important to consider a description of the functions that a “fully capable” ISAO will address in support of its members. When describing an ISAO, this discussion of the capabilities exhibited by a fully-capable ISAO will help emerging ISAOs determine the capabilities and objectives they wish to develop – keeping in mind that the initial set of objectives and capabilities will likely evolve as the ISAO matures.
107	SWG 2	A fully capable ISAO will provide a variety of services in support of its members. These services, and the capabilities that are needed to provide them, should be designed to support ISAO members as they manage strategic and tactical cyber-related risks. The type of support can be grouped into three broad categories with some overlap between them.
108	SWG 2	These categories are:
109	SWG 2	Situational Awareness: ISAO members need to understand both the tactical and strategic aspects of the environment in which they are managing risks. This includes activities to collect and share information, analyze it, and formulate recommendations as to what to do with the analyzed information received.
110	SWG 2	Decision-making: ISAOs need to provide actionable information that will enable their members to make decisions related to their current security posture and allocation of security and IT resources. This involves receiving information, establishing its relevancy to the organization, assessing potential impacts, identifying potential actions, and selecting the best course of action for the organization.
111	SWG 2	Actions: ISAO members ultimately will take actions based on information and analysis provided. At this point detailed actions will be developed and responsibilities assigned, the actions implemented and their effectiveness evaluated providing feedback for further consideration.
112	SWG 2	For each of these categories, individual members/organizations will have their own responsibilities addressing the needs of the member/organization and will additionally have responsibilities to the ISAO. The ISAO in turn also has responsibilities for each of these categories that address the ISAO membership as a whole.
113		
114	ISAO SO	**VALUE PROPOSITION**
115		An informative set of cybersecurity threat indicators and best practices provided by ISAOs will make individual members more secure
116		ISAOs implemented in accordance with a consistent yet flexible framework can replicate and extend current trust relationships by establishing a common, shared set of values and expectations
117		Educating and informing members about how to protect, detect, and react to cyber threats
118		By aggregating information from multiple organizations ISAOs present a richer picture of what malicious activity is taking place around the country and the world. Member organizations can then use this enriched information to improve their individual and collective security, blocking attacks they would not have seen otherwise.

119		The ISAO members are also able to make effective and timely responses if they find they’ve had unauthorized intrusions.
120		
121		**GOVERNANCE**
122	SWG 1	**Legal Construct and Governance**
123	SWG 1	**Articles of Incorporation / Charter - To formally establish the existence of the ISAO**
124	SWG 1	**State-Specific Articles of Incorporation Requirements**
125	SWG 1	What are the specific requirements to form a non-profit, for-profit or other structure that the ISAO may determine for the state or states they plan to operate in? What will be the principal point of operations (including physical location?
126	SWG 1	Who will serve as the Registered Agent and the Incorporator?
127	SWG 1	**Articles of Incorporation / Charter**
128	SWG 1	Basic information will be needed including what is the name of the organization? Effective dates of the Articles?
129	SWG 1	Is it required to register or reserve the name of the organization?
130	SWG 1	Is the organization "For-Profit", "Non-Profit?" Will the ISAO have just domestic members? International members? Both?
131	SWG 1	**Vision and Mission**
132	SWG 1	Have the members defined the core purpose of the organization? What do the members want to accomplish with the creation of the ISAO?
133	SWG 1	**Board of Directors or Governing Leadership**
134	SWG 1	Does the ISAO want to have a Board of Directors and formal leadership positions in the ISAO? If so, what process do the members want to use to establish this? Formal elections? Define process in by-laws?
135	SWG 1	**Bylaws**
136	SWG 1	**Bylaws Definition and Authorization**
137	SWG 1	Have the Bylaws been defined by the Executive Director and the Board of Directors?
138	SWG 1	Have the Bylaws been adopted by the Board of Directors?
139	SWG 1	Do the Bylaws give the Board of Directors the power to alter, amend or repeat the Bylaws?
140	SWG 1	**Emergency Bylaws**
141	SWG 1	What are your Emergency Bylaws requirements?
142	SWG 1	**Bylaws - Change Management**
143	SWG 1	How are your Bylaws amended and voted on?
144	SWG 1	**Name and Legal Construct**
145	SWG 1	What is the name of the ISAO?
146	SWG 1	What is the legal construct?
147	SWG 1	What IRS non-profit certification?
148	SWG 1	**Purpose, Vision and Mission**
149	SWG 1	Have the members defined the purpose of the ISAO? Is it clear what the ISAO plans to achieve? Has the vision and mission of the ISAO been articulated?

150	SWG 1	**Recognition / Certification**
151	SWG 1	Does the government require any certifications from the ISAO to share and receive information? If so, what are those processes?
152	SWG 1	**Offices and Registered Agent**
153	SWG 1	Offices - Where does the ISAO maintain a registered office and how is it designated?
154	SWG 1	Agent - Who or what organization is serving as the Registered Agent? How is this documented?
155	SWG 1	**Membership**
156	SWG 1	Membership
157	SWG 1	What public- or private-sector organizations, institutions, or individuals can be members?
158	SWG 1	Will members institute controls and checks over who can join, including reviewing the U.S. sanctions list prior to allowing new members in? What is the process to constantly monitor and check these lists?
159	SWG 1	Member Information Sharing
160	SWG 1	Do you have formal Member Information Sharing Agreements?
161	SWG 1	Have you defined a process for how these agreements will be defined and/or changed over time?
162	SWG 1	Have you defined what your information sharing protocols, standards, and guidelines will be?
163	SWG 1	How do you enforce governance of your Member Information Sharing Agreement?
164	SWG 1	How do you encourage or require member information sharing?
165	SWG 1	Classes (Categories of Members)
166	SWG 1	Have you defined classes or categories of membership?
167	SWG 1	Do these classes or categories of membership receive different levels of services?
168	SWG 1	New Member - Membership Criteria
169	SWG 1	What is required of an public- or private-sector organization, institution or individual to join as a member?
170	SWG 1	Do you have a Member "Code of Conduct" Policy?
171	SWG 1	Do you require Members to sign a Membership Agreement?
172	SWG 1	Member Fees (Dues)
173	SWG 1	What are the membership fees (dues) and how are they collected and managed? Are these annual or bi-annual dues?
174	SWG 1	Membership Termination, Expulsion and Suspension
175	SWG 1	What is the process for members to work out disagreements or issues?
176	SWG 1	What are the conditions and what is the process under which a membership can be terminated, expelled or suspended?
177	SWG 1	Is the termination, expulsion or suspension process against a specific individual representing the member organization, or the member organization?
178	SWG 1	Have you defined processes for Members to work out disagreements? What Member Conflict Resolution Policies and Procedures do your have in place? Have all of the members agreed to these procedures?

179	SWG 1	Transfer of Membership
180	SWG 1	Is membership transferrable to another organization? To another individual within an organization that is a member?
181	SWG 1	Member Meetings
182	SWG 1	Have the Members decided how often they want to meet? Where they are held?
183	SWG 1	How are Member Meetings attended (i.e. in-person, virtual, or both?)
184	SWG 1	How are Member Meeting Notices delivered?
185	SWG 1	How are Emergency Member Meetings handled?
186	SWG 1	Quorum
187	SWG 1	What constitutes a Quorum for Member Meetings?
188	SWG 1	Voting Privileges and Manager of Voting
189	SWG 1	Do different level of paying members have different voting privileges?
190	SWG 1	What are Member voting privileges?
191	SWG 1	What is the voting process?
192	SWG 1	Government Members / Liaison
193	SWG 1	Do you want state, local or Federal agencies to join as members?
194	SWG 1	Does the organization understand the various requirements for sharing with all levels of government?
195	SWG 1	Have you reviewed the legal or regulatory compliance implications for sharing with the government? And differences in sharing with state, local and Federal law enforcement?
196	SWG 1	Is information shared with the private sector and government shared separately?
197	SWG 1	What are the Information Sharing Protocols required? (Traffic-Light Protocols, etc.)
198	SWG 1	**Directors**
199	SWG 1	Board Roles, General Powers and Duties
200	SWG 1	Do you have a Board of Directors Roles and Responsibilities Agreement Board Members are required to sign?
201	SWG 1	What are the roles and responsibilities of the Board of Directors?
202	SWG 1	Do you have the role and responsibilities of the CEO, Executive Director or President defined, documented, and communicated to the Board in writing to ensure the Board is not involved in day-to-day operations and activities?
203	SWG 1	Do you have a Board of Directors "Code of Conduct" Policy?
204	SWG 1	Do you have a Board of Directors "Conflict of Interest Policy”?
205	SWG 1	To ensure the ISAO meets member's desired issues, challenges, and requirements; how do you ensure that the ISAO is Member-driven and Board-governed, not vice-versa?
206	SWG 1	Do you have protocols and policies in place to manage Board conflicts (i.e. with their roles and responsibilities, between Board Members, or with Officers, Executive Management or staff?
207	SWG 1	Voting Directors
208	SWG 1	How many Directors are on the Board (minimum required and maximum)?
209	SWG 1	Do you ensure that the Board always have an odd number of members to ensure effective voting results?

210	SWG 1	How is the number of Directors determined?
211	SWG 1	Do all Directors have Voting Privileges?
212	SWG 1	If voting on particular initiative, project, ISAO protocols, processes, etc. indicates a conflict of interest involving one or more Members of the Board, what is the process to mitigate the conflict of interest and ensure the applicable Board Member(s) do not have voting privileges?
213	SWG 1	Qualification of Directors
214	SWG 1	What are the qualification requirements to serve on the ISAO Board of Directors?
215	SWG 1	Appointment or Initial and Election of Directors
216	SWG 1	How are Directors either initially appointed or elected to the Board?
217	SWG 1	What is the Board of Director's Nomination Process?
218	SWG 1	Term of Directors
219	SWG 1	What are the term limits for Directors (i.e., two-years, etc.)?
220	SWG 1	Are Directors eligible to be re-elected to the Board at the conclusion of their initial term? How many times can they be eligible for re-election?
221	SWG 1	How do you ensure term limits are adhered to?
222	SWG 1	If Directors currently in office desire to change the By-Laws to increase Director term limits or the number of times a Board Member can be re-elected to the Board, will the ISAO require all Members to approve this change before it can be adopted?
223	SWG 1	Election of Voting Directors
224	SWG 1	How are Directors elected? Annually? Bi-annually?
225	SWG 1	Are Director elections staggered?
226	SWG 1	Vacancies and Resignations
227	SWG 1	What happens when a vacancy occurs on the Board?
228	SWG 1	What is the process to fill vacancies?
229	SWG 1	Decreasing the Board of Directors
230	SWG 1	What is the process of the number of Directors is to be decreased?
231	SWG 1	Quorum and Voting
232	SWG 1	What are the requirements to reach a Quorum for the Board of Director's Meetings and for voting?
233	SWG 1	Chairperson and Vice-Chairperson of the Board of Directors
234	SWG 1	Do you plan to have a Chairperson and Vice-Chairperson
235	SWG 1	How are they elected?
236	SWG 1	What are their term limits?
237	SWG 1	Committees and/or Working Groups
238	SWG 1	How are Committees and/or Working Groups approved, formed and managed?
239	SWG 1	Meetings
240	SWG 1	When are meetings of the Board of Directors held?
241	SWG 1	Action without Meeting
242	SWG 1	What actions can be taken without a Board of Directors meeting?
243	SWG 1	Attendance by Virtual Meeting or Telephone

244	SWG 1	Can Board Meetings be attended virtually or only in-person?
245	SWG 1	Director Compensation
246	SWG 1	Are Directors compensated? If so, is the Compensation Policy documented?
247	SWG 1	Director Alternate
248	SWG 1	Do you allow alternate individuals from an organization to serve on the Board when the original Board member can not serve?
249	SWG 1	Director Removal
250	SWG 1	How are Directors removed from the Board?
251	SWG 1	What would cause a Director to be removed from the Board?
252	SWG 1	Has the Director Removal Process been documented?
253	SWG 1	Conflicts of Interest
254	SWG 1	Do you have a Board of Directors Conflict of Interest Statement in the Bylaws and an Agreement that the Board Members are required to sign?
255	SWG 1	**Officers**
256	SWG 1	Officer - Definition
257	SWG 1	What Officer positions (roles and responsibilities) have been identified, defined and approved by the Board of Directors?
258	SWG 1	Can an Officer hold more than one Office?
259	SWG 1	Duties of Officers
260	SWG 1	What are the authorities, roles and responsibilities of each Officer?
261	SWG 1	Term of Office
262	SWG 1	What are Terms of Office for each Officer position?
263	SWG 1	Executive Director/CEO/President
264	SWG 1	How is the Officer identified?
265	SWG 1	What are the roles and responsibilities?
266	SWG 1	What authorities?
267	SWG 1	Vice-President
268	SWG 1	How is the Officer identified?
269	SWG 1	What are the roles and responsibilities?
270	SWG 1	What authorities?
271	SWG 1	Secretary
272	SWG 1	How is the Officer identified?
273	SWG 1	What are the roles and responsibilities?
274	SWG 1	What authorities?
275	SWG 1	Treasurer
276	SWG 1	How is the Officer identified?
277	SWG 1	What are the roles and responsibilities?
278	SWG 1	What authorities?
279	SWG 1	Other Officers - CIO, CTO, COO, etc.
280	SWG 1	How is the Officer identified?

281	SWG 1	What are the roles and responsibilities?
282	SWG 1	What authorities?
283	SWG 1	Resignation and/or Removal of Officers
284	SWG 1	What is the process to handle Officer resignations?
285	SWG 1	What is the process to remove an Officer?
286	SWG 1	**Financial Management**
287	SWG 1	Financial Policies and Procedures
288	SWG 1	Do you have formal Financial and Internal Controls Policy and Procedures?
289	SWG 1	Who manages adherence to financial policies and procedures?
290	SWG 1	Where are financial records kept?
291	SWG 1	Does the organization need to hire an accountant or other staff to manage the finances of overall entity?
292	SWG 1	Do you have a formal accounting "Chart of Accounts"
293	SWG 1	Budget Process
294	SWG 1	What is the documented process for the Board to adopt an annual Budget?
295	SWG 1	Who defines the Budget for Board review and approval?
296	SWG 1	Who manages the Budget and Reports to the Board?
297	SWG 1	Fiscal Year and Audit
298	SWG 1	What is the fiscal year of the ISAO?
299	SWG 1	How are annual audits conducted?
300	SWG 1	Do you have a CPA to file required government reports and returns?
301	SWG 1	Have you created independent audit structures of the ISAO's financials annually?
302	SWG 1	Contracts, Loans and Deposit of Funds
303	SWG 1	Contracts
304	SWG 1	Who is authorized to develop, sign, administer and manage contracts on behalf of the ISAO?
305	SWG 1	Loans and Deposits
306	SWG 1	Who is authorized to initiative loans on behalf of the ISAO?
307	SWG 1	Do expenses over a certain amount need to have more than one approver?
308	SWG 1	Who is authorized to deposit funds in an authorized banking facility on behalf of the ISAO?
309	SWG 1	Checks, Drafts, etc.
310	SWG 1	Who is authorized to execute and sign checks on behalf of the ISAO?
311	SWG 1	Who is authorized to endorse checks for deposit on behalf of the ISAO?
312	SWG 1	**Intellectual Property (IP)**
313	SWG 1	**Does the organization plan to create policies, programs etc. that will have Intellectual Property unique to the ISAO?**
314	SWG 1	Do you have Intellectual Property (IP) policies and procedures?
315	SWG 1	**Employees**
316	SWG 1	**Does the organization plan to hire employees? Are there appropriate structures in place to support all of the associate requirements for that?**

317	SWG 1	Do you have an Employee Handbook - Policies and Procedures?
318	SWG 1	Do you conduct background checks on your employees?
319	SWG 1	Do you have Security Policies that Employees are required to sign?
320	SWG 1	**Consultants/Vendors**
321	SWG 1	Do you have Consulting and Vendor Agreements?
322	SWG 1	Do you do background checks on your consultants and vendors?
323	SWG 1	Do you have Security Policies that consultants and vendors are required to sign?
324	SWG 1	**Physical Access Security**
325	SWG 1	Do you have formal physical security access controls -policies, procedures and security facility technology?
326	SWG 1	Information Sharing Protections - Legislative
327	SWG 1	What information sharing protections (legislation) are currently law?
328	SWG 1	Are you communicating these protections to your membership?
329	SWG 1	**Notices**
330	SWG 1	How are Notices delivered to the Board Members of General Members?
331	SWG 1	**Indemnification**
332	SWG 1	Right to Indemnification
333	SWG 1	Does the ISAO indemnify any Director, Officer, Employee or Agent?
334	SWG 1	Is so, what is the process and is it documented?
335	SWG 1	**Amendments**
336	SWG 1	How are Amendments defined and added to the Bylaws?
337	SWG 1	Is the process documented?
338	SWG 1	**Bylaws Certification**
339	SWG 1	Acceptance by the Board of Directors
340	SWG 1	Do you have a statement acknowledging that the Bylaws have been adopted by the Board of Directors?
341		
343	SWG 2	**SERVICE OFFERINGS**
344	SWG 2	Vulnerability Management
345	SWG 2	Best Practice Library
346	SWG 2	Situational Awareness
347	SWG 2	Threat Warning (Actionable Intelligence)
348	SWG 2	Operational support and assistance
349	SWG 2	Support for Incident Response and Recovery
350	SWG 2	Risk Management
351	SWG 2	Information management and analysis
352	SWG 2	Trusted Information Sharing and Collaboration Environment/Services
353		
354	SWG 2	**OPERATING MODELS (TYPES OF ISAOs)**
355	SWG 2	Categories of ISAOs

356	SWG 2	Risk-based (e.g. ecosystem wide vulnerability)
357	SWG 2	Threat-based (general or specific, either methods or individual actors)
358	SWG 2	Individuals and informal group-based
359	SWG 2	Industry- and Sector-based
360	SWG 2	Geographically-based
361	SWG 2	Technology-based
362	SWG 2	Issue-based
363	SWG 2	Limited Time or Special Event Driven
364	SWG 2	Clearing house vs. membership
365	SWG 2	Structuring ISAOs for state, local, sector, etc.
366	SWG 2	Outsourcing analysis considerations
367	SWG 2	Scaling of ISAOs
368	SWG 2	Operational cost of ISAO based on ISAO Maturity/Capability
369		
370	SWG 3	**INFORMATION SHARING POLICY**
371	SWG 3	Use of shared information
372	SWG 3	Prioritization of Information for Exchange
373	SWG 3	Vetting of data and information received
374	SWG 3	Ownership of Information
375	SWG 3	Liability of Sharing Information
376	SWG 3	Minimizing data shared
377	SWG 3	Anonymity of data shared
378	SWG 3	Anonymity of information sources
379	SWG 3	Integrity of Information Shared
380	SWG 3	Framework for sharing between ISAOs
381	SWG 3	One-Way Information Sharing
382	SWG 3	Two-Way Information Sharing
383	SWG 3	Information Sharing Networks
384	SWG 4	Procedures for capability for real/near-real time exchange
385	SWG 4	Handling sensitive information
386	SWG 4	Handling classified information
387	SWG 6	Privacy protections
388	SWG 6	Considerations when sharing to/from the Federal Government
389	SWG 6	International considerations
390		
391	SWG 3	**INFORMATION COLLECTION AND DISSEMINATION**
392	SWG 3	Define a process to identify what's important to members
393	SWG 3	Define data model for sharing information
394	SWG 3	Determine level of analysis to be provided

395	SWG 3	How to get companies to share
396	SWG 3	Identify and establish triggers for sharing
397	SWG 3	Establish effective information control policies or principles
398		
399	SWG 3	**SHARING MODELS AND MECHANISMS**
400	SWG 3	Models
401	SWG 3	Mesh Network
402	SWG 3	Hub & Spoke
403	SWG 3	Publish/Subscribe
404	SWG 3	Peer2Peer
405	SWG 3	Flooding
406	SWG 3	Portal
407	SWG 3	Mechanisms
408	SWG 3	Face to Face
409	SWG 3	Telephone
410	SWG 3	E-mail/Listserv
411	SWG 3	Website postings
412	SWG 3	Automated (Primary indicator and defensive measures then follow on info)
413		
414	SWG 1	**START-UP ACTIVITIES / KEY PLANNING FACTORS**
415	SWG 1	**Value Proposition**
416	SWG 1	ISAOs strive to improve cyber security for domestic and international partners.
417	SWG 1	Define the information sharing problem that your ISAO will solve.
418	SWG 1	Does your solution fix a broken information sharing problem that has measurable consequences?
419	SWG 1	What solution can you bring to information sharing that is unique to you?
420	SWG 1	Define in depth, what other similar ISAOs are doing right now, i.e. who is the competition?
421	SWG 1	What does your organization have to offer the ISAO community of sharing partners or your targeted sharing partners that enhances the protection of critical infrastructure?
422	SWG 1	What can your organization do differently or better than other ISAOs?
423	SWG 1	What is your value added content; information, analytics, actionable cyber intelligence?
424	SWG 1	How will your ISAO improve the cybersecurity posture of your sharing partners?
425	SWG 1	Define ISAO Service Offerings
426	SWG 1	Design a core set of services in order to:
427	SWG 1	Act as hub to share cyber threats and defensive measures information; and
428	SWG 1	Analyze data and turning it into usable information that adds value to ISAO members.

429	SWG 1	Beyond the core set of services of information sharing, determine what additional services the ISAO wants to provide to enhance the core ISAO services and add further value to its members.
430	SWG 1	**Information Sharing /Collaboration**
431	SWG 1	ISAOs share timely and accurate cyber threats, indicators, warnings, vulnerabilities, responsive measures and/or defensive measure information with others.
432	SWG 1	What information does your ISAO plan to share with members or customers?
433	SWG 1	1. Threat/Indicator Sharing
434	SWG 1	2. Defensive Measure Sharing
435	SWG 1	Does your organization have special expertise in this particular area of cyber information?
436	SWG 1	What target market of customers or members will your organization focus on to share information with?
437	SWG 1	Have you considered the cost of information sharing in your revenue model?
438	SWG 1	Have you thought about how you will share information with your target market?
439	SWG 1	How do you intend to get your target market involved in telling you what information they want you to share with them? In other words, how will you encourage collaboration?
440	SWG 1	What mechanisms have you considered to engage your sharing partners with to ensure that the information you share is relevant and timely?
441	SWG 1	Have you identified collaborative leaders in your organization and in those of your sharing partners? What organization leads have the most interest in the organizations of your sharing partners?
442	SWG 1	Is there a way to make collaboration with your sharing partners, a part of their natural workflow?
443	SWG 1	How will you ensure that information you share is actionable by your target market?
444	SWG 1	Do you have special analytics that you can apply to information that is shared with you by others that will enhance the value of that raw data?
445	SWG 1	Have you considered working with other partners to enhance the value of the data that you receive?
446	SWG 1	**Strategic Alliances/Organizational Sharing Model**
447	SWG 1	ISAOs have domestic (public- and/or private-sector) and/or International (public- and/or private-sector) partners.
448	SWG 1	Have you mapped out your sharing partner list and your strategic alliance partner list?
449	SWG 1	Consider using a mapping software like Mindnode, Curio, My thoughts, iMindMap, Visio, etc.
450	SWG 1	Do you plan to have domestic (public and/or private) sharing partners?
451	SWG 1	How will you get your domestic sharing partners? Are they already members of customers of your organization?
452	SWG 1	Do your strategic alliance partners have a clearly identifiable mutually beneficial objective?
453	SWG 1	Have you considered finding International sharing partners? If so, how will you connect with them?
454	SWG 1	Would an international strategic alliance improve your information sharing?

455	SWG 1	How would you effectively share information with an international partner?
456	SWG 1	Does your ISAO sharing model help you develop members and/or customer sharing partners?
457	SWG 1	Who will your organization share with specifically and how will you acquire those sharing partners?
458	SWG 1	Will sharing partners be new organizations that you have not done business with or will it be customer-based sharing?
459	SWG 1	Or will it be open sharing with public & private sectors?
460	SWG 1	**Trust Model /Culture**
461	SWG 1	ISAOs typically establish a basis of trust among its sharing partners.
462	SWG 1	How do you plan to create a trust model within your ISAO?
463	SWG 1	What are the risks for you and your sharing partners if trust is broken?
464	SWG 1	How will you create transparency in your ISAO among sharing partners?
465	SWG 1	Do you plan to vet your sharing partners? If so, how?
466	SWG 1	Domestically?
467	SWG 1	Internationally?
468	SWG 1	How will your ISAO use its trust model to promote information sharing and attract more partners to share with?
469	SWG 1	What are your ISAO Member expectations
470	SWG 1	Will you publish ISAO Member rules of behavior
471	SWG 1	What ISAO Member removal approaches will you use; criteria for removal and voting rules
472	SWG 1	**Membership**
473	SWG 1	Membership includes membership models, vetting, onboarding, and removal.
474	SWG 1	Criteria for membership consideration
475	SWG 1	Are there are minimum set of requirements that have to be satisfied and monitored on a regular basis (i.e., annually, etc.) by which each member is re-evaluated from a membership perspective? Who will decide the requirements? Who will be responsible for monitoring members?
476	SWG 1	Member nomination and recruiting
477	SWG 1	What will be the ISAO's member nomination and recruiting strategy?
478	SWG 1	How will the ISAO identify potential organizations for membership?
479	SWG 1	What tactics will the ISAO use to reach potential new members?
480	SWG 1	Membership vetting policy and processes
481	SWG 1	What will be the ISAO's vetting policies including assessment and probation?
482	SWG 1	What will be the voting rules for membership acceptance?
483	SWG 1	What will be the process for vetting, from assessment through voting?
484	SWG 1	New member tactical onboarding considerations
485	SWG 1	What will be the process for signing, recording, and storing membership agreements?
486	SWG 1	How will the new member's systems get linked with the ISAO's systems to begin sharing information?

487	SWG 1	What will comprise the educational curriculum for new members? Who will receive the training and how will they receive it?
488	SWG 1	What will be the process for new member introductions?
489	SWG 1	**Marketing - For Public and Private ISAOs**
490	SWG 1	Marketing plan
491	SWG 1	Will there be an ISAO marketing plan? If so, who will develop and maintain that plan?
492	SWG 1	What will be the essential marketing processes?
493	SWG 1	Positioning the ISAO through its value proposition
494	SWG 1	What will be the ISAO's foundational positioning statement, including the ISAO's objectives and envisioned capabilities, the value and benefits it intends to deliver, and how it will differ from other ISAOs?
495	SWG 1	How will that positioning statement be used in recruiting, external communication, and member communication?
496	SWG 1	Reaching the ISAO's audiences
497	SWG 1	What tactical marketing tools will the ISAO use to communication externally (e.g. events, online and documentary materials, public relations, advertising, private recruitment, and the like)?
498	SWG 1	If the ISAO accepts revenue-generating advertising, what will be the policies around and process for advertising on ISAO properties.
499	SWG 1	What will be the rules, responsibilities, and authorities for marketing communication?
500	SWG 1	**Communications**
501	SWG 1	Communications outside ISAOs, exclusive of threat intelligence information sharing
502	SWG 1	What will be the methods and approaches used to communicate governance matters bi-directionally with other ISAOs, the ISAO governing organization, strategic alliances, and government organizations?
503	SWG 1	What tactical tools will the ISAO use to communication externally (e.g. listserves, partner portal, newsletters, news feeds, calendars, etc.)?
504	SWG 1	What will be the rules, responsibilities, and authorities for external communication?
505	SWG 1	Communications with ISAO members, exclusive of threat intelligence information sharing
506	SWG 1	What will be the methods and approaches used to communicate bi-directionally with ISAO members about matters such as membership recruitment and onboarding, ongoing policy and capabilities development, strategic planning, accomplishments, etc.?
507	SWG 1	What are the ISAO member roles that should send/receive information and what type of information should each role send/receive?
508	SWG 1	What tactical tools will the ISAO use to communicate bi-directionally with members (e.g. listserves, member-only portal, newsletters, news feeds, calendars, etc.)?
509	SWG 1	What will be the rules, responsibilities, and authorities for ISAO member communication?
510	SWG 1	**Operations and Financial Management**
511	SWG 1	Key Financial Components Impacting the Finances and Operations of an ISAO

512	SWG 1	What are the key cost drivers/expenses/capital requirements that need to be considered for standing up an ISAO and for day to day operations?
513	SWG 1	Based on the type of ISAO business mode, what are the options for funding the ISAO and potential sources of revenue?
514	SWG 1	Membership Models
515	SWG 1	How many different levels of memberships will be offered (i.e., basic, standard, premium)?
516	SWG 1	What will be the different benefits associated to each membership level?
517	SWG 1	What will be the fee structures associated to each membership level?
518		
519	SWG 6	**PARTNERSHIPS AND SUPPORT**
520	SWG 5	Peer relationships and inter-ISAO collaboration
521	ISAO SO	Relationships with national and regional entities, SLTTGs
522	SWG 5	Mentoring
523	SWG 6	ISAO SO support
524	SWG 5	Commercial/industry support
525	SWG 6	Government Programs
526		
527	SWG 6	**GOVERNMENT RELATIONS**
528	SWG 6	Partnership with the government (information exchange and collaboration)
529	SWG 6	Law enforcement liaison
530	SWG 6	Information Sharing and regulator relations
531	SWG 6	Protections when sharing with Regulators
532		
533	**APPENDIX**	
534	ISAO SO	Definitions
535	ISAO SO	References
536	ISAO SO	ISAO SO Standards Development Process