



Information Sharing and Analysis Organization (ISAO) Standards Organization

Online Meeting

10 March 2016



Agenda



- Why Are We Here?
- Standards Working Group Model
- Initial Deliverables
- Timeline
- ISAO SO Public Website
- Upcoming Events
- Working Group Updates
- Standards Working Group Participation
- Questions & Answers

Why Are We Here?



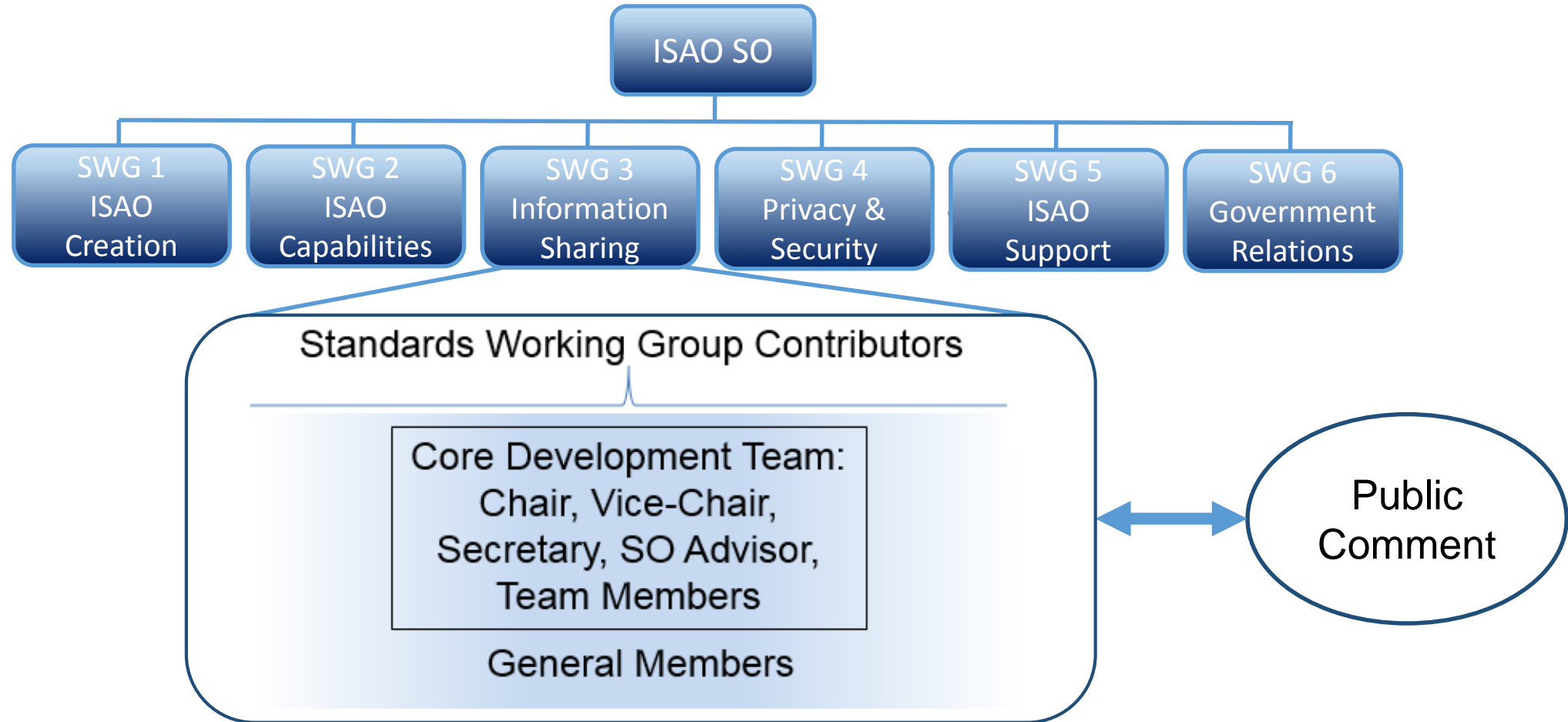
“The cyber threat is one of the most serious economic and national security challenges we face as a Nation.”

President Barack Obama, March 2010

Mission: Improve the Nation’s cybersecurity posture by identifying standards and guidelines for robust and effective information sharing related to cybersecurity risks/incidents and cybersecurity best practices.

Vision: A more secure and resilient Nation that is connected, informed and empowered.

Standards Working Group Model

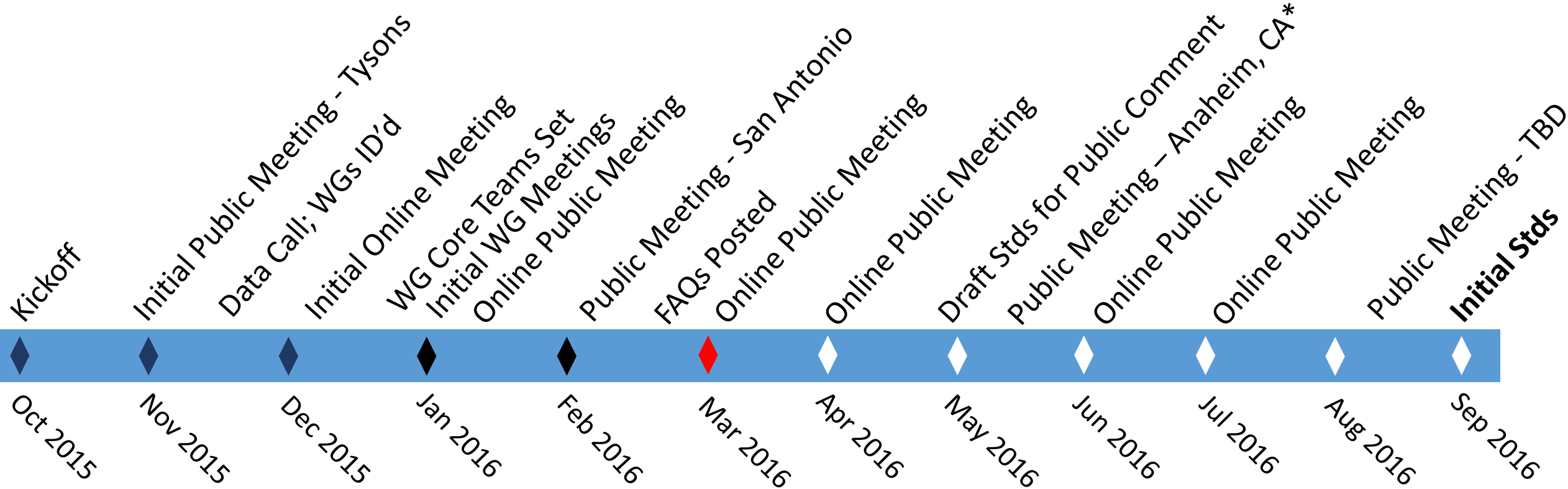


Initial Deliverables



- FAQs and Initial ISAO Definition Posted February 26th
- Draft ISAO Categories to be Posted by March 31st
- Standards Working Group Draft Products Due May 3rd
 - SWG 1: What needs to be considered by a newly forming ISAO?
What are the first steps?
 - SWG 2: What capabilities might an ISAO provide?
 - SWG 3: What types of information will be shared and what are some mechanisms for doing so?
 - SWG 4: What security and privacy is needed for a newly forming ISAO?
 - SWG 5: What mentoring support is available for newly forming ISAOs?
 - SWG 6: What government programs and services are available to assist ISAOs?

Time is our Enemy



* Pending Signed Hotel Contract



[ABOUT](#)

[EVENTS](#)

[PRODUCTS](#)

[WORKING GROUPS](#)

[FAQ](#)

[CONTACT](#)



CALL FOR PARTICIPATION

Learn How to Get Involved in the Development Process

[LEARN MORE](#)

10
Mar '16

ONLINE MEETING – MARCH 10,
2016



Online Webinar

[READ MORE](#)

Upcoming Events



- Online Public Meeting: April 19th, 1:30-2:30pm Central
(2:30-3:30pm Eastern)
- In-Person Public Meeting: May 19th, Anaheim, CA*

* Pending Signed Hotel Contract

Third Open Public Forum



- Tentative Dates / Location – May 18-19 at the Anaheim Hilton, Anaheim CA*
- Tentative Agenda
 - May 18th (By invitation)
 - AM Leadership Meeting
 - PM SWG Meetings
 - May 19th
 - Public Forum
 - Read Outs from SWGs
 - Public Discussion of SWG Deliverables
 - SWG Breakouts

* Pending Signed Hotel Contract

Working Group 1: ISAO Creation



Frank J. Grimmelmann: President & CEO / Intelligence Liaison Officer,
ACTRA - Arizona Cyber Threat Response Alliance

Deborah Kobza: President & CEO, Global Institute for Cybersecurity + Research

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.

Potential Key Topics

- Organizing principles of the ISAO
- Define membership: types of membership, expectations, rules of behavior
- ISAO leadership and management structure
- Financing the ISAO
- Advertising the ISAO for prospective members and building trust between members
- Identification of agreements: MOU, MOA, NDAs

SO Advisor: Natalie Sjelin

Working Group 2: ISAO Capabilities



Denise Anderson: Chair, National Council of ISACS (NCI), President National Health ISAC
Fred Hintermister: Vice-Chair NCI, Manager, ES-ISAC, North American Electric Reliability Corporation

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.

Potential Key Topics

- Baseline standards for operational, technical, analytical, and personnel capabilities
- Establish capabilities associated with various tiers or categories of ISAOs
- Establish capabilities for business analysis, process and project management, and administration
- Determine certifications (technical and others)

SO Advisor: Brad Howard

Working Group 3: Information Sharing



Kent Landfield: Director, Standards and Technology Policy, Intel Corporation
Michael Darling: Director at PwC

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 an ISAO or externally.

Potential Key Topics

- Vetting data from internal and external sources
- Analysis of threat, vulnerability, and incident data
- Sharing information within an ISAO to its members
- Sharing information with external entities
- Optimize operational architectures and sharing information protocols

SO Advisor: Daniel Knight

Working Group 4: Privacy & Security



Rick Howard: Chief Security Officer, Palo Alto Networks
David Turetsky: Partner, Akin Gump

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

Potential Key Topics

- Anonymization and minimization data
- Redacting privacy information and personally identifiable information
- Intellectual property management and handling
- Authentication process for accessing ISAO information
- Protections for ISAO members and third parties when information is shared with US Government

SO Advisor: Daniel Knight

Working Group 5: Support



Carlos Kizzee: Executive Director, Defense Security Information Exchange
Alex Crowther: National Defense University

Objective: This working group will work closely with the ISAO SO to provide assistance to emerging ISAOs by developing and implementing processes that assist the community of emerging organizations expressing interest in or defining themselves as ISAOs with the identification and proper application of the relevant standards, knowledge, experience, and capabilities available to support their development as an ISAO.

Potential Key Topics

- Develop techniques and strategies to assist in the creation and maturation of ISAOs
- Work with emerging ISAOs and assist with resolution of unforeseen issues
- Develop metrics to gauge the effectiveness of information sharing and analysis efforts
- Address implications of information sharing and analysis
- Provide user feedback to other Standards Working Groups

SO Advisor: Natalie Sjelin

Working Group 6: Government Relations



Mike Echols: Director, DHS Cyber Joint Program Management Office
David Weinstein: Cybersecurity Advisor, State of New Jersey

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

Potential Key Topics

- Legal issues and/or responsibilities when working with Law Enforcement
- Legal issues and/or responsibilities when working with the Intelligence Community
- Managing interactions with Regulators
- Requirements for information sharing between Government and the private sector

SO Advisor: Brad Howard

Standards Working Group Participation



- 110+ experts from various industry sectors, government, and academia already participating in Standards Working Groups
- For those who'd like to join:
 - The Standards Working Group Application Form can be found at the ISAO web page (<https://www.isao.org/standards-working-groups>)
Email completed form to ISAO@lmi.org