Information Sharing and Analysis Organization (ISAO) Standards Organization

Online Public Meeting

20 OCTOBER 2016

A secure and resilient Nation – connected, informed and empowered.

ISAO
Standards Organization

@ISAO_SO
www.isao.org
lnked.in/ISAO_SO

Agenda

ISAO
Standards Organization

- Why Are We Here?
- Information Sharing with DHS
- Initial Voluntary Guidelines
- What’s Next?
- Growing the Ecosystem
- Resource Library
- ISAO Registry
- National Information Sharing Conference
- Questions & Answers

Why Are We Here?

ISAO
Standards Organization

> “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 and analysis related to cybersecurity risks, incidents and best practices.

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

Information Sharing with DHS

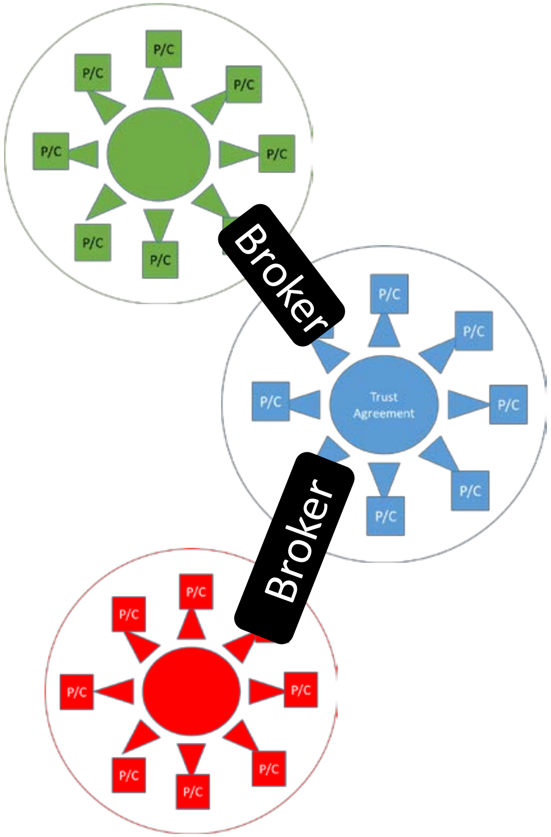
W. Preston Werntz

Chief of Technology Services
National Cybersecurity and Communications
Integration Center (NCCIC)

Automated Indicator Sharing (AIS)

Homeland Security

Trust Brokering Concept



- Brokers work between communities in accordance with the **Trust Models** of the two or more trust communities being brokered

- Brokers may also host automated, machine-speed brokering services allowing communities to work together by filtering, translating, transferring, controlling access, stewarding, consolidating and enriching – in accordance with each brokered community’s Trust Model

Homeland Security

Programs for sharing with the NCCIC

- **Cyber Information Sharing and Collaboration Program (CISCP)** supports broad sharing of cyber threat data (indicators, analytic content, etc.) in multiple formats with direct company analyst to DHS analyst collaboration and access to the NCCIC operations floor. Also includes ability for DHS to sponsor clearances (for classified threat briefs).
- **Automated Indicator Sharing (AIS)** is about sharing machine readable cyber threat indicators near-real-time.

Cybersecurity Information Sharing Act (CISA) of 2015

- The Cybersecurity Information Sharing Act (CISA) of 2015, which is designed to increase cybersecurity information sharing between the private sector and the Federal Government, required DHS to have an automated capability to receive and share cyber threat indicators and defensive measures.
- Non-Federal entity sharing with DHS through AIS or other DHS mechanisms that is conducted in accordance with CISA's requirements (e.g., privacy scrubs) receives liability protection.

Value Proposition
(“What’s in it for me?”)

Why do I want these indicators?

- Receiving cyber threat indicators (and defensive measures) allows organizations to improve their network defense posture faster and forces adversaries to change their infrastructure, tactics, etc.
- If your organization cannot make use of them directly (e.g., outsourced infrastructure), you should make sure your service provider is receiving and using.

Why do I want to share indicators back?

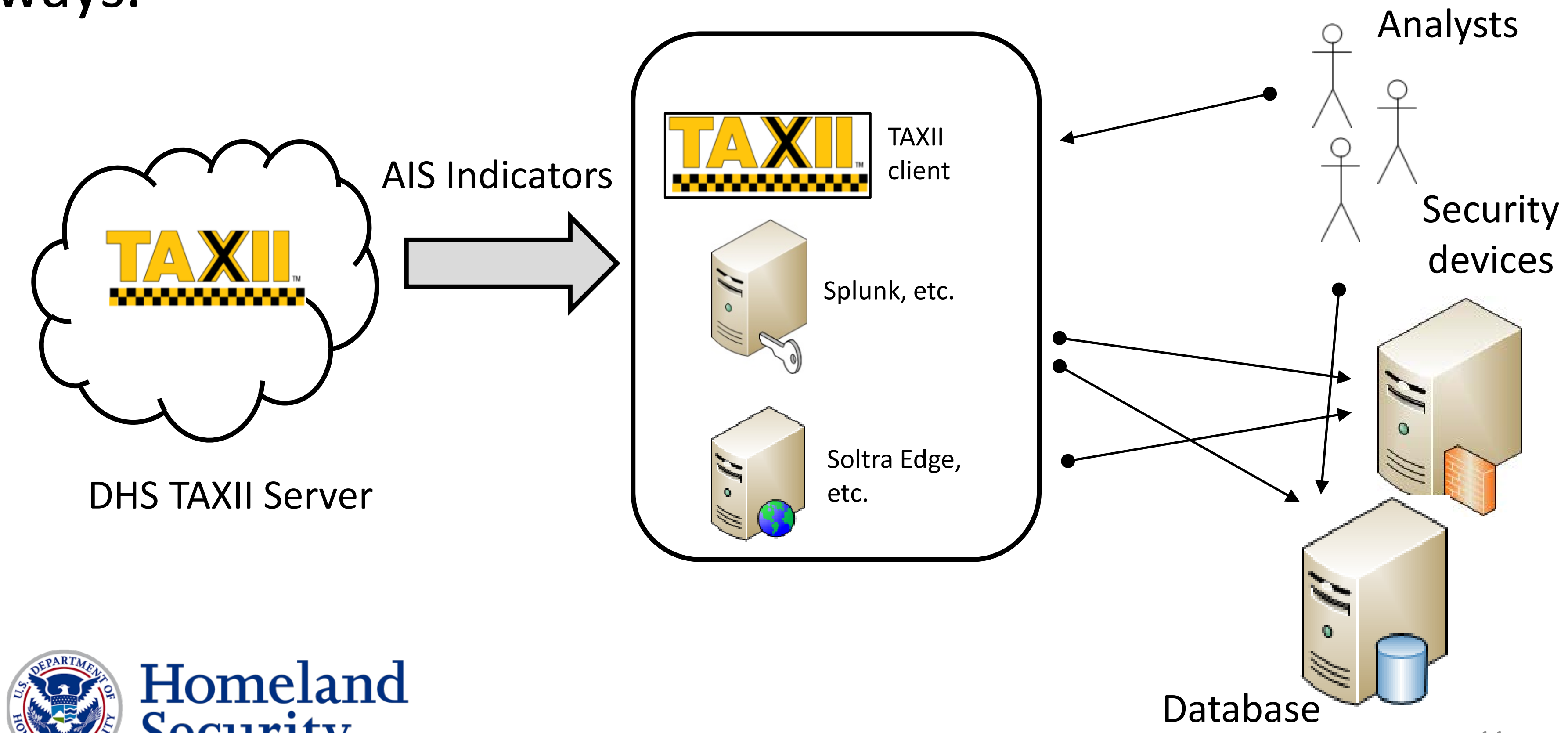
- Your detection becomes someone else’s prevention and makes the entire community stronger (think of animals in a large herd).
- Liability protection.

Plugging into AIS

- Sign the AIS Terms of Use
- Decide on how you’d like to connect
- Ensure you have processes and policies in place for receiving and sharing indicators

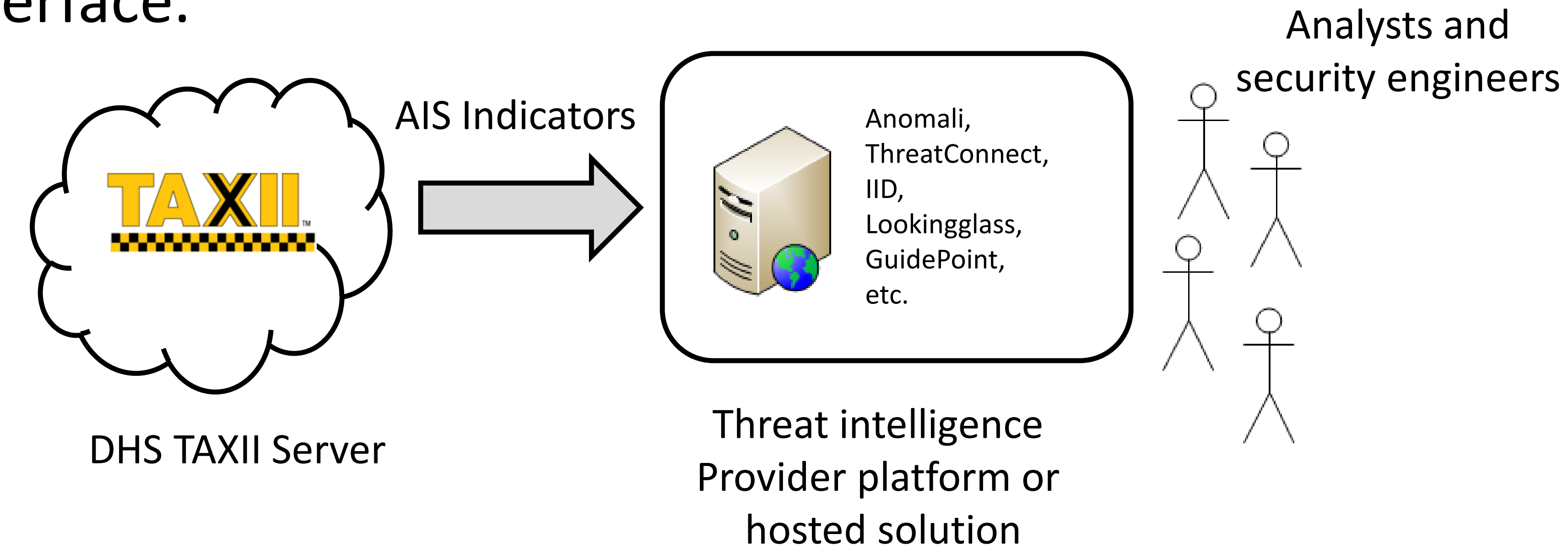
You Host the Connection

Indicators are pulled from the DHS TAXII server via your own TAXII capability where they can be used in multiple ways.



Someone Else Hosts the Connection

Indicators are pulled from the DHS TAXII server into a commercial threat intelligence provider or other hosted solution and accessed by security staff through a user interface.



Receiving from AIS

Activities	Things to Think About
Decide how to use the incoming STIX information.	How will you determine which indicators or defensive measures apply to your organization? Will you take automated action with them, or send to analysts for review?
Getting the STIX information to your security end-points.	Do your security products speak STIX natively, or will you need to transform it before loading it up?
Sharing feedback to DHS.	Can you provide feedback to DHS on quality of indicators? Did you detect potential malicious activity previously unknown?
Further sharing the AIS indicators.	Is that allowable via the TLP marking? Do you have processes or technical controls in place to manage that sharing.

Sharing to AIS

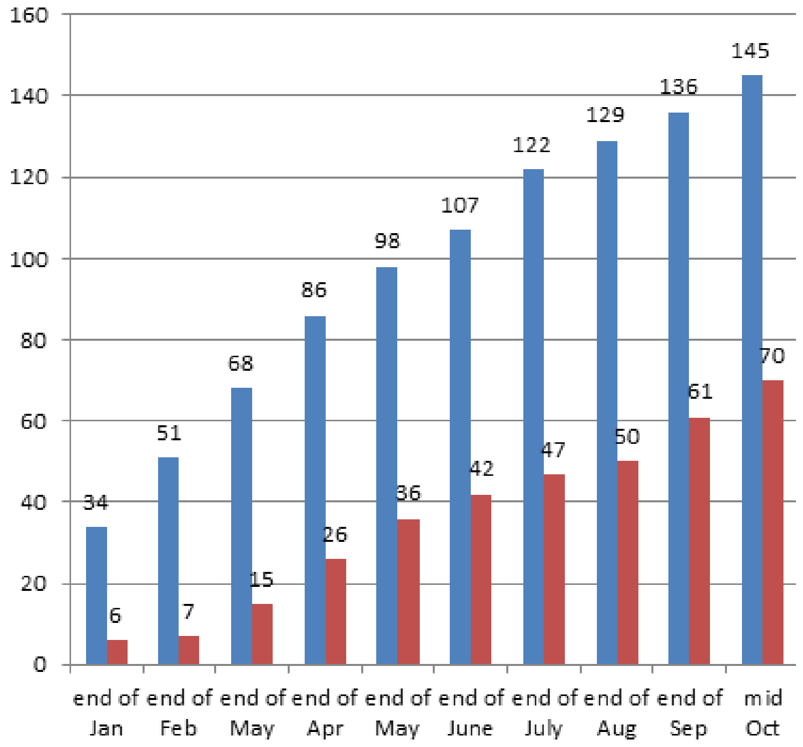
Activities	Things to Think About
Decide what information you want to share.	Who owns the information? What restrictions are there on sharing it? Do you want to remain anonymous to the broader community when you share it? Do you have processes in place to perform a privacy review before sharing it?
Format the information into STIX.	If not already in STIX, do you need to manually transform it? Do you own any security products that speak STIX natively?
Getting the STIX content into your TAXII client.	Do you need to build or buy a TAXII client? Do one of your security products already speak TAXII natively?

Privacy Scrub

- The Cybersecurity Information Sharing Act (CISA) of 2015 requires entities to conduct a privacy review before sharing to DHS in order to receive liability protection.
- DHS always performs another privacy review upon receipt of indicators.
  - All indicators go through an automated or manual privacy review.
  - Any part of an indicator that fails an automated review goes to a DHS analyst for review.

AIS Snapshot

- 145 Terms of Use signed, 56 non-Federal entities connected to server
- 12 Federal entities connected
  - DOE, NCIJTF, TREAS, NTOC, DOC, HHS, DOI, GSA, EPA, DHS SOC, FBI SOC, USAID and EDU
- ~36,100 total unique indicators shared (since March)



Questions?

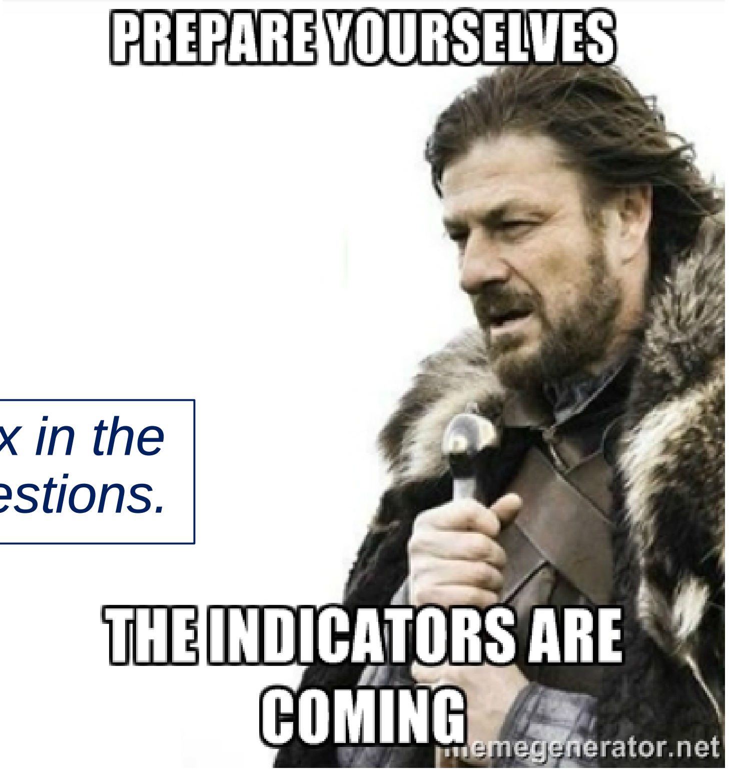
https://www.us-cert.gov/ais

https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti

http://www.us-cert.gov/tlp

preston.werntz@hq.dhs.gov

ncciccustomerservice@hq.dhs.gov

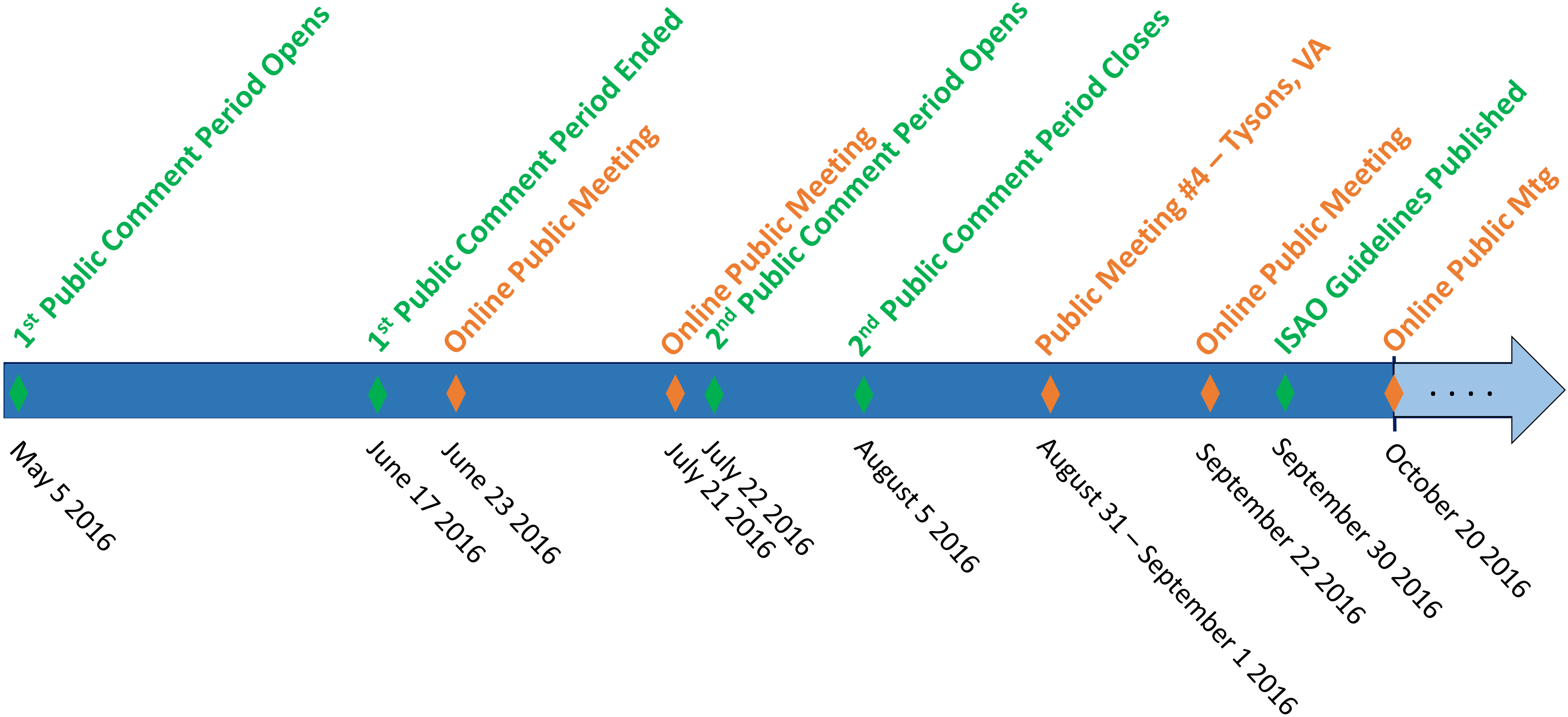


Please use the Question and Answers box in the GoToWebinar Control Panel to submit questions.

Homeland Security

Meeting the Urgent Need

ISAO
Standards Organization



1st Public Comment Period Opens
May 5 2016

1st Public Comment Period Ended
June 17 2016

Online Public Meeting
June 23 2016

Online Public Meeting
July 21 2016

2nd Public Comment Period Opens
July 22 2016

2nd Public Comment Period Closes
August 5 2016

Public Meeting #4 – Tysons, VA
August 31 – September 1 2016

Online Public Meeting
September 22 2016

ISAO Guidelines Published
September 30 2016

Online Public Mtg
October 20 2016

. . . .

Hot off the Press

ISAO Standards Organization

- Evolving Community Body of Knowledge
- Initial voluntary guidelines published 30 Sep 2016
  - **ISAO 100-1, *Introduction to ISAOs***
  - **ISAO 100-2, *Guidelines for Establishing an ISAO***
  - **ISAO 300-1, *Introduction to Information Sharing***
  - **ISAO 600-2, *U.S. Government Relations, Programs, and Services***
- Minor corrections addressed in v1.01
- Now, spread the word and implement!

ISAO 100-1: Introduction to Information Sharing and Analysis Organizations (ISAOs) v1.01

October 14, 20

ISAO 100-2: Guidelines for Establishing an Information Sharing and Analysis Organization (ISAO) v1.01

October 14, 2016

ISAO 300-1: Introduction to Information Sharing v1.01

October 14, 20

ISAO 600-2: U.S. Government Relations, Programs, and Services v1.01

October 14, 2016

Give us your feedback: Contact@isao.org

What's Next? (1 of 3)

ISAO

Standards Organization

- ISAO SO solicited inputs for follow-on docs beginning 1 Sep
- Currently <u>considering</u> the following:
  - ISAO 400-1: INTRODUCTION TO PRIVACY AND SECURITY
    - An intro – midlevel discussion of privacy and security issues
    - Incorporates WG4 Needs Assessment "*Best Practices to Advance Privacy and Security in Private Sector Information Sharing*"
  - ISAO 500-1: INTRODUCTION TO ANALYSIS
    - An intro – midlevel discussion of that other part of information sharing…the A in ISAO
  - ISAO 800-1: INTRODUCTION TO LEGAL ISSUES FOR ISAOs
    - An intro – midlevel discussion of the legal questions and considerations that arise in forming an ISAO
  - ISAO 300-2: INFORMATION SHARING METHODS (ARCHITECTURE)
    - A midlevel look at the subject of Information Sharing and the various methods that can be used – goes beyond the descriptions in ISAO 300-1 to provide "How To" info for new ISAOs

What’s Next? (2 of 3)

ISAO
Standards Organization

- Also currently considering the following:
  - ISAO 300-3: AUTOMATED INFORMATION SHARING
    - A midlevel technical discussion of automated information sharing and its impact on the ecosystem
  - ISAO 600-1: INTRODUCTION TO THE ROLE OF GOVERNMENT
    - Introduces the 600 series on the relationship between the private industry and government
  - ISAO 600-3: STATES, LOCAL, TRIBAL & TERRITORIAL ISSUES
    - An intro – midlevel discussion of issues impacting information sharing at subnational levels
  - ISAO 700-1: INTRODUCTION TO GLOBAL SHARING
    - Introduces the 700 series on information sharing on a global scale
  - ISAO 200-1: INTRODUCTION TO ISAO CAPABILITIES AND SERVICES
    - Introduces the 200 series on Capabilities and Services of an ISAO and provides an intro – midlevel discussion of the various capabilities and services an ISAO may consider adopting

What’s Next? (3 of 3)

- The ISAO SO is engaged with working group leaders to discuss priorities and assignments
- Submit suggestions for new documents to Contact@isao.org

Requested Information	Provide Information Here
Document Title	[Enter the proposed document title.]
Purpose of the Document	[Describe the document you propose to develop. Identify the document goals that will be addressed. This information should come from your analysis of need.]
Results of Analysis	[Overview of the results of your analysis and explain why they point to a need for a document in this area.]
Target Audience	[Describe who is the target audience of the document, at what level – management, technical, etc. Be specific about what level of training/education the audience requires. Who are you writing the document for? Who will use this document and what general skills / knowledge this audience needs to have prior to reading the document.]
Duplication of Effort	[Describe the type of literature search conducted to ensure that documents are consistent with other ISAO SO documents. Search other ISAO SO documents for this topic area or related to this topic area. Ensure consistent terminology, definitions and discussions on the topic.]
Ecosystem / National Scope	[Describe how this document has applicability across the ecosystem. What type of capability or capabilities does this document address?]
Additional Comments	[Other pertinent information needed by the ISAO SO in determining approval of the proposed document.]

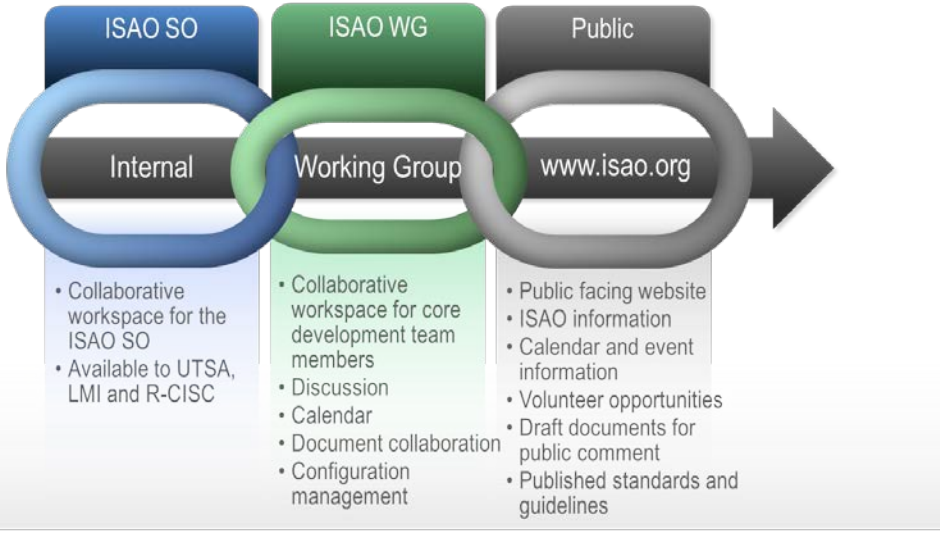
Building the Community

ISAO
Standards Organization

- Working Group Evolution
- Refining Collaboration Infrastructure
- Broadening Outreach by Leveraging Networks
- Creating Venues for Online and Face-to-Face Interaction

GoToWebinar by citrix

LISTSERV

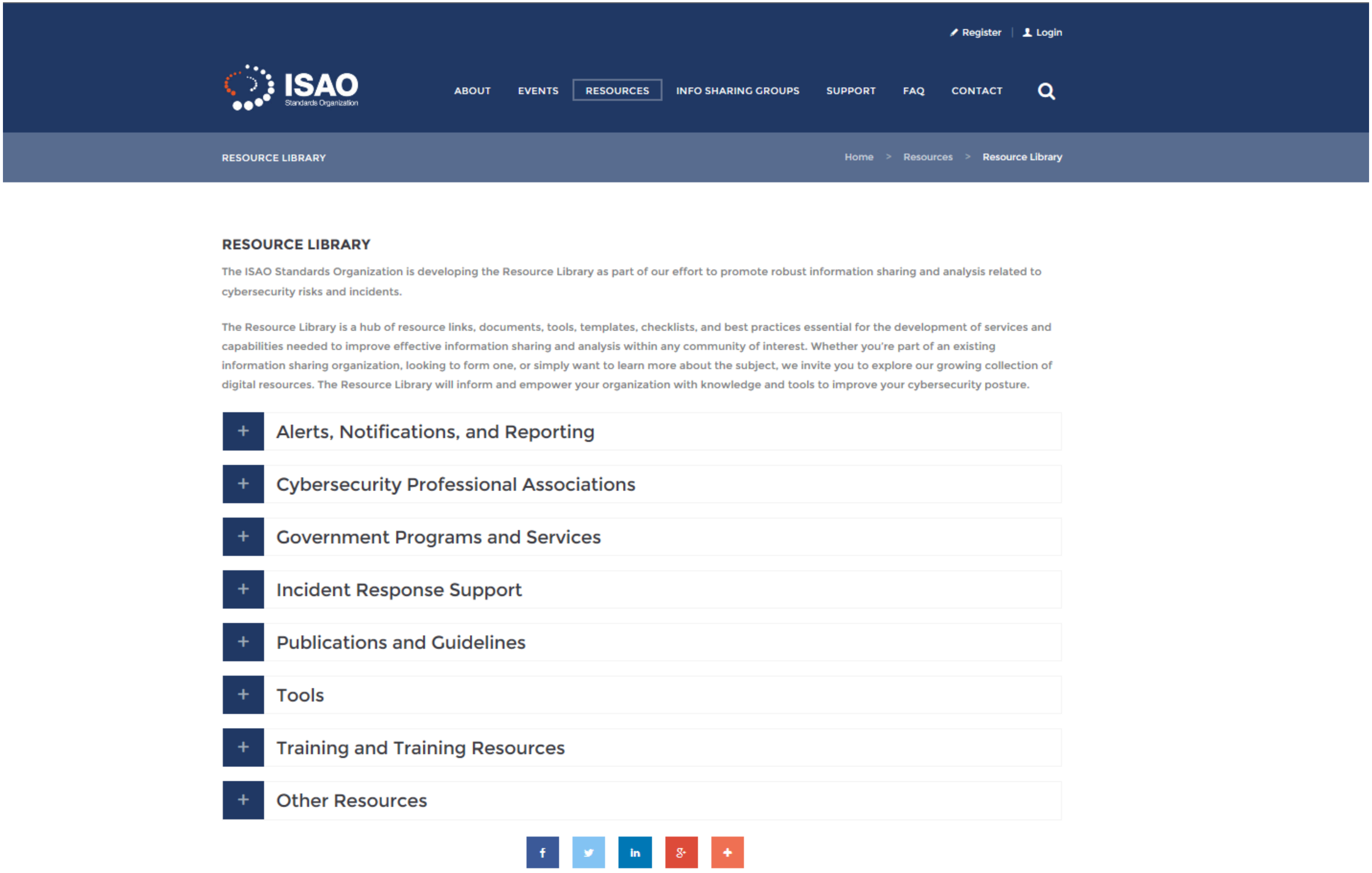


ISAO SO – Internal
- Collaborative workspace for the ISAO SO
- Available to UTSA, LMI and R-CISC

ISAO WG – Working Group
- Collaborative workspace for core development team members
- Discussion
- Calendar
- Document collaboration
- Configuration management

Public – www.isao.org
- Public facing website
- ISAO information
- Calendar and event information
- Volunteer opportunities
- Draft documents for public comment
- Published standards and guidelines

Information Sharing Resource Library



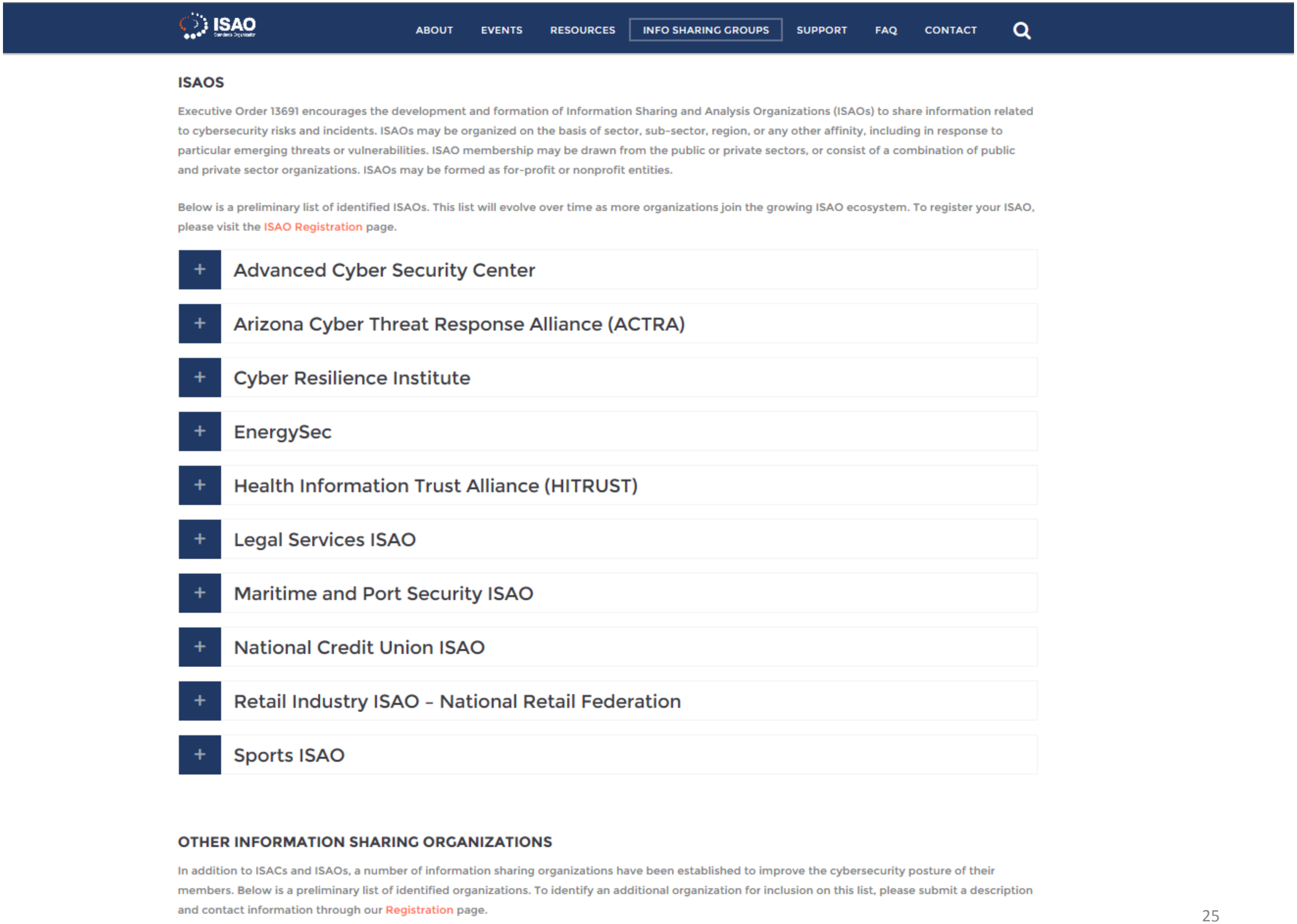
RESOURCE LIBRARY

The ISAO Standards Organization is developing the Resource Library as part of our effort to promote robust information sharing and analysis related to cybersecurity risks and incidents.

The Resource Library is a hub of resource links, documents, tools, templates, checklists, and best practices essential for the development of services and capabilities needed to improve effective information sharing and analysis within any community of interest. Whether you're part of an existing information sharing organization, looking to form one, or simply want to learn more about the subject, we invite you to explore our growing collection of digital resources. The Resource Library will inform and empower your organization with knowledge and tools to improve your cybersecurity posture.

- + Alerts, Notifications, and Reporting
- + Cybersecurity Professional Associations
- + Government Programs and Services
- + Incident Response Support
- + Publications and Guidelines
- + Tools
- + Training and Training Resources
- + Other Resources

Information Sharing Groups



ISAOS

Executive Order 13691 encourages the development and formation of Information Sharing and Analysis Organizations (ISAOs) to share information related to cybersecurity risks and incidents. ISAOs may be organized on the basis of sector, sub-sector, region, or any other affinity, including in response to particular emerging threats or vulnerabilities. ISAO membership may be drawn from the public or private sectors, or consist of a combination of public and private sector organizations. ISAOs may be formed as for-profit or nonprofit entities.

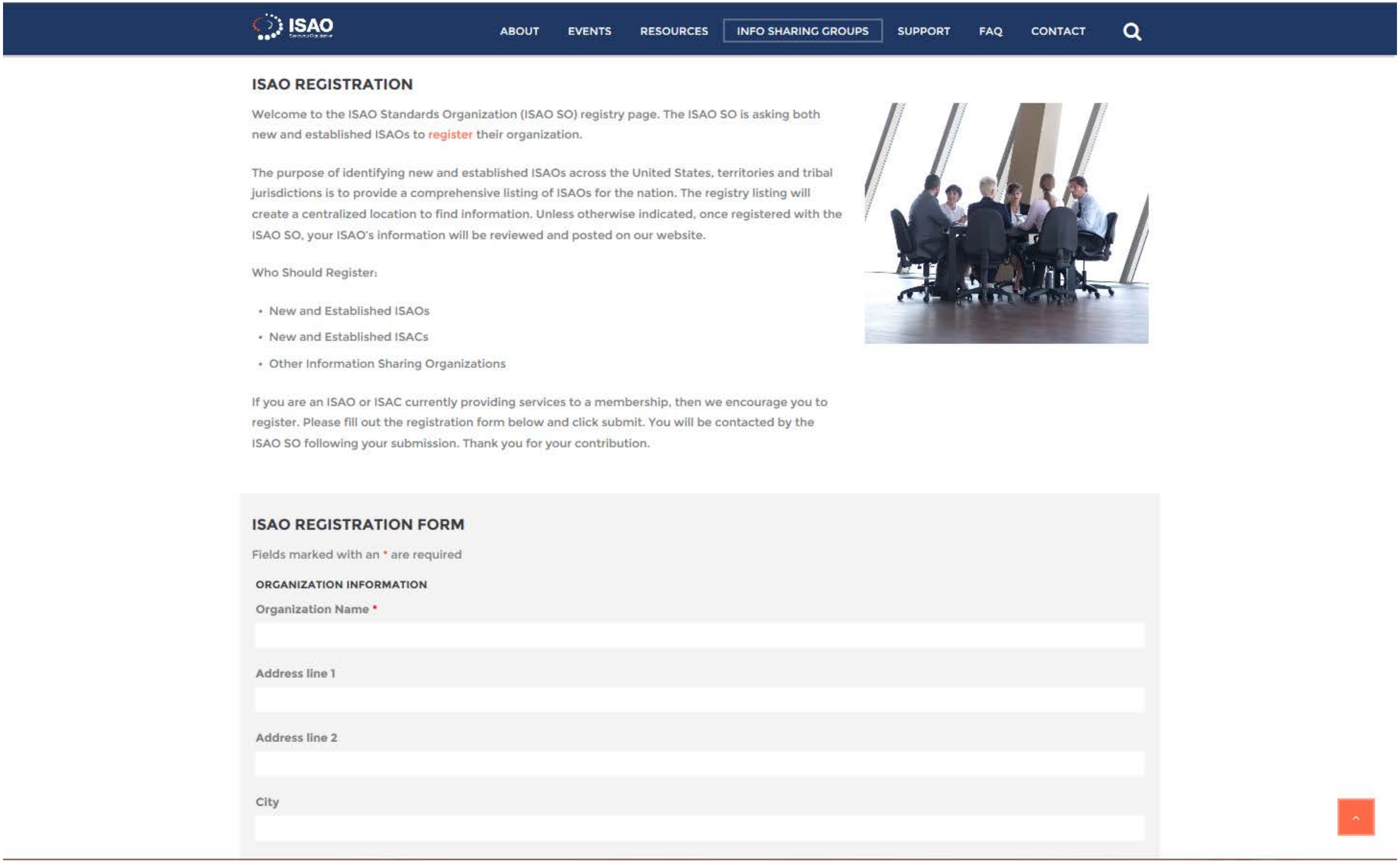
Below is a preliminary list of identified ISAOs. This list will evolve over time as more organizations join the growing ISAO ecosystem. To register your ISAO, please visit the ISAO Registration page.

- + Advanced Cyber Security Center
- + Arizona Cyber Threat Response Alliance (ACTRA)
- + Cyber Resilience Institute
- + EnergySec
- + Health Information Trust Alliance (HITRUST)
- + Legal Services ISAO
- + Maritime and Port Security ISAO
- + National Credit Union ISAO
- + Retail Industry ISAO – National Retail Federation
- + Sports ISAO

OTHER INFORMATION SHARING ORGANIZATIONS

In addition to ISACs and ISAOs, a number of information sharing organizations have been established to improve the cybersecurity posture of their members. Below is a preliminary list of identified organizations. To identify an additional organization for inclusion on this list, please submit a description and contact information through our Registration page.

ISAO Registry



ISAO REGISTRATION

Welcome to the ISAO Standards Organization (ISAO SO) registry page. The ISAO SO is asking both new and established ISAOs to register their organization.

The purpose of identifying new and established ISAOs across the United States, territories and tribal jurisdictions is to provide a comprehensive listing of ISAOs for the nation. The registry listing will create a centralized location to find information. Unless otherwise indicated, once registered with the ISAO SO, your ISAO's information will be reviewed and posted on our website.

Who Should Register:

- New and Established ISAOs
- New and Established ISACs
- Other Information Sharing Organizations

If you are an ISAO or ISAC currently providing services to a membership, then we encourage you to register. Please fill out the registration form below and click submit. You will be contacted by the ISAO SO following your submission. Thank you for your contribution.

ISAO REGISTRATION FORM

Fields marked with an * are required

ORGANIZATION INFORMATION

Organization Name *

Address line 1

Address line 2

City

ISAO Roundtable Discussions

ISAO Monthly Online Round Table Discussion

- *A Platform for new and emerging ISAOS*
  - *Peer-discussions and sharing of ideas*
  - *Present challenges or obstacles and discuss solutions*
  - *Highlight resources, tools and training opportunities*
  - *Guest Speakers*

National Information Sharing Conference

ISAO
Standards Organization

- ISAOs
- Service Providers
- Training Sessions
- Call for Papers

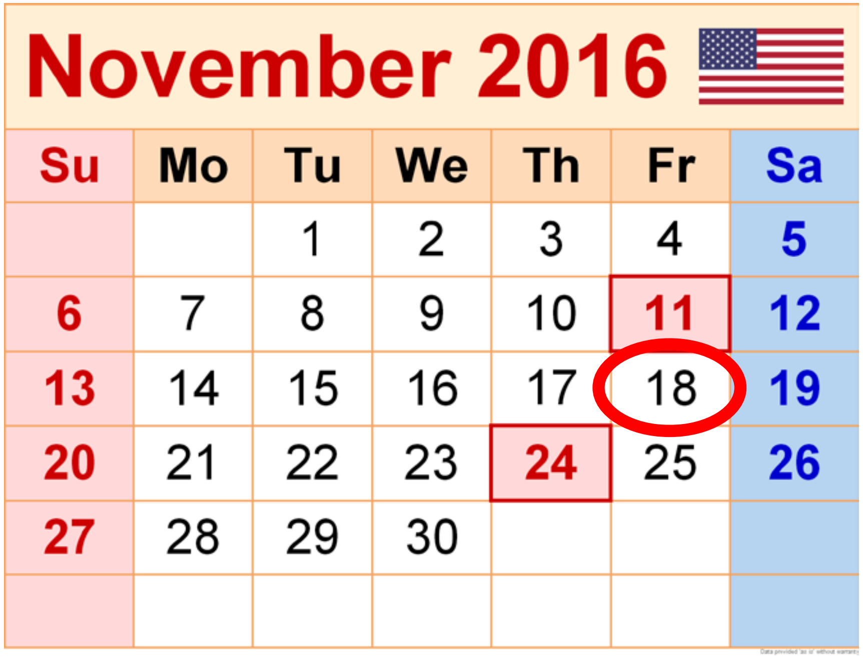
- 2017 Date and Location TBD
  - Considering spring and fall options

Bringing the Community Together

Mark Your Calendars

ISAO
Standards Organization

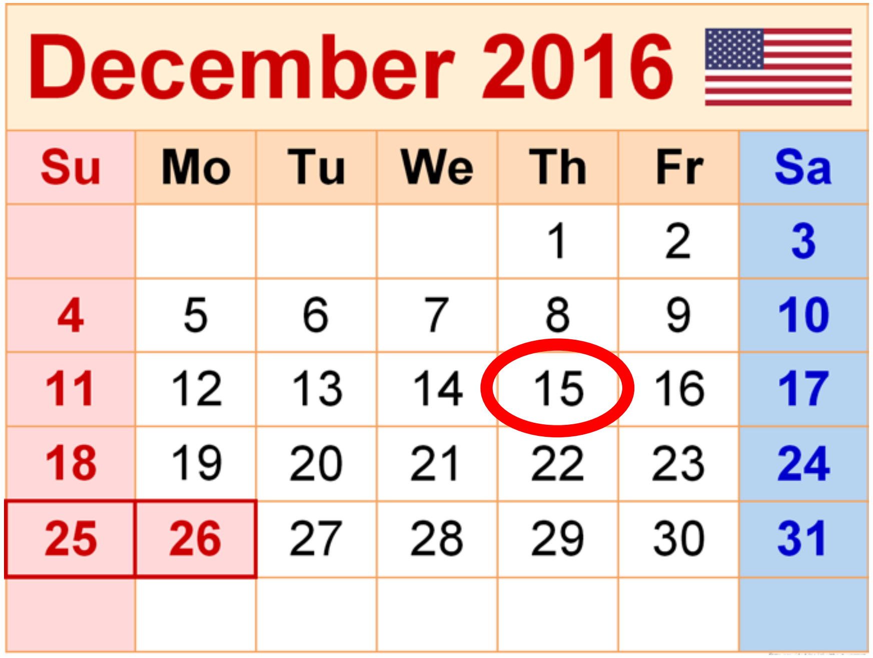
- Online public meetings at 1pm Central time
- Information sharing insights, updates from the ISAO SO, and your chance to engage



November 2016

Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

Data provided 'as is' without warranty



December 2016

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Questions and Answers

ISAO
Standards Organization

Please use the Question and Answers box in your GoToWebinar Control Panel to submit questions to the ISAO SO.

Thanks for joining our online meeting today!