Information Sharing and Analysis Organization (ISAO) Standards Organization

Online Public Forum

18 NOVEMBER 2016

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

ISAO
Standards Organization

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

Agenda

- Why We’re Here
- Cyber Information Sharing & Legal Concerns
- ISAO SO Survey
- Future Voluntary Guidelines
- Growing the Community
- Building Capability
- Questions & Answers

Why We’re 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.

Presentation to the ISAO Standards Organization: Some Issues Around Information Sharing that General Counsels May Think About

David Turetsky

Partner and Co-leader of the Cybsersecurity, Privacy and Data Protection Practice

Akin Gump Strauss Hauer & Feld LLP

Co-leader ISAO SO Working Group 4, Privacy and Security

dturetsky@akingump.com

Direct: +1 202.887.4074

Information Sharing Can Help to Provide Necessary Security in a Digital World

- The digital technologies that expand our future, economic and otherwise, also create vectors for attack from close and far away.
- While no silver bullet, voluntary cybersecurity information sharing is a tool that has attracted the support of experts, the Congress and the President. Over time, it might become necessary to meet commercial requirements and to demonstrate reasonable care.
- The idea of cybersecurity information sharing is to make actionable information available rapidly so that the same cybersecurity threat can't work again and again.
  - It can raise the cost to adversaries of developing cyberattack tools since their tools can't be used over and over to generate a return.
  - It can potentially lower the cost to companies of defending well and improve their ability to avoid costly harm if they have better information about what needs to be defended against.

Effective Information Sharing Isn’t Easy for All Companies

- Information sharing is much easier spoken about than accomplished: To be most effective, companies need to share cybersecurity threat information in a timely manner, have an effective platform and process for doing so, an ability to use effectively what they receive, and the trust that is necessary to support this environment.
- Companies may need know-how, personnel, technology, policies, systems, etc.
- Effective information sharing can require company resources and commitment that require dialogue across many levels and disciplines to obtain. That can be a real challenge for companies and make it harder to make a choice to share.
  - Not every discipline necessarily understands cybersecurity issues well, but often those disciplines are necessary to support the processes, resources and commitment required to make information sharing happen effectively.
  - Boards don’t necessarily get briefed and provide support for information sharing, which could be a potential way to bridge different disciplines and priorities, and move forward.

Challenges of Voluntary Information Sharing

- Companies aren't necessarily used to sharing with other companies, especially about threats they face, and they are concerned about reputation, competition, liability and many other issues. They also may not have the personnel, expertise, systems and other resources to invest in or benefit from sharing.
- While the theory is strong, the actual benefits of information sharing are not well-documented through metrics and anecdotes. This may reduce the likelihood some corporate constituencies will fairly weigh the benefits to the company of sharing with the risks and costs.
- Interestingly, some general counsels were recently asked to discuss what obstacles remain to more and faster information sharing. They responded that their cybersecurity and IT experts were not pressing this with them, so the lawyers were not focused there.
- At most companies, however, especially of any size, information sharing is going on among security and IT people, perhaps informally, whether general counsels know it or not.

What is Information Sharing?

- Cybersecurity information sharing can take many forms:
  - Between the government and the private sector (directly or through information sharing organizations) and vice versa.
    - The government has resources the private sector doesn't, such as the NSA, CIA, FBI, etc. It also has experience from defending the .gov (dot gov) domain, e.g., from attacks seeking military information from the government not unlike what military contractors face. On the other hand, some parts of the government may have different objectives than private companies, such as catching perpetrators.
    - "…[T]his has to be a shared mission…Government has many capabilities, but it's not appropriate or even possible for government to secure the computer networks of private businesses… but the private sector doesn't always have the capabilities needed during a cyber attack, the situational awareness, or the ability to warn other companies in real time, or the capacity to coordinate a response across companies and sectors. So we're going to have to be smart and efficient and focus on what each sector does best, and then do it together." President Obama, 2/13/2015
  - Between similar or dissimilar businesses or institutions, individually, or through for-profit or non-profit information sharing organizations organized by sector, geography, supply chain, etc. These organizations are usually called ISACs (Information Sharing and Analysis Centers) or ISAOs (Information Sharing and Analysis Organizations).

Legislation to Encourage Information Sharing

- There was a widespread belief that legislation could play a role in facilitating voluntary information sharing, especially on closer to a real-time basis.
- There were questions legislation could resolve about what information could be shared and the interaction of existing laws.
- There were questions about how sharing could and should be conducted by the government.
- As part of the effort to remove obstacles and foster more information sharing, industry sought the adoption of certain liability protections for information sharing with support in Congress and the Administration.
  - Providing liability protection was thought to be particularly important to make companies comfortable with the risks of sharing more information very quickly. For example, companies did not want their regulators to use against them information they might voluntarily share; and they wanted protection from liability if they inadvertently included some personal information in what they shared, notwithstanding efforts to ensure that would not happen.
  - In this sense, CISA was aimed at company lawyers; it was intended to make the risk or cost side of the scale lighter when a company considers whether to share.

Cybersecurity Information Sharing Act of 2015 (CISA)

- December 18, 2015, the House and Senate passed an omnibus appropriations package that includes CISA (at Division N, Title I; 6 U.S.C. Subchapter I).
- CISA is intended to foster voluntary cybersecurity information sharing on a real-time or near-real-time basis, both among private companies and between companies and the government.
- Information sharing is intended to help rapidly identify and defend against threats and limit the period of time and number of instances for which a particular attack can be repeated.
- The government cannot compel or coerce companies to participate and cannot condition other benefits or contracts on participation.
- Most provisions sunset after 10 years.
- DOJ and DHS jointly developed policies within 180 days of the law concerning civil liberties, sharing with non-federal entities, etc.

CISA – Key Protections for Participants

- DHS NCCIC (National Cybersecurity and Communication Integration Center) provides the “portal” through which cyber threat information generally is shared with government. DHS maintains personal privacy and civil liberties protections.
  - Use of the portal requires registration, agreements on terms of use, testing, etc. Initially, it has usually taken months rather than weeks to complete the process.
- Gives liability protection and confidentiality protections to businesses for sharing and receiving cybersecurity threat information in conformance with CISA. As noted earlier, this was intended to address legal concerns of companies.
- If private entities perform a privacy scrub before sharing, they are not liable for including personal information they didn’t know at the time of sharing was there.
- Private entities that receive or share threat information are not liable for failing to warn or act based on receiving or providing such information.
- Threat information shared with the government will not be used to regulate lawful activities, nor does it waive any privilege or protection.
- Private entities receive antitrust protections from sharing cyber threat indicators and defensive measures. Other activities such as price fixing are not protected.
- Also exempts cyber threat indicator sharing from FOIA.

Agency Actions Pursuant to CISA

- The automated sharing capability authorized by CISA is operational.
  - Automated Indicator Sharing (AIS) is available for free through the NCCIC.
  - AIS participants connect to a DHS-managed system in NCCIC that allows bidirectional sharing of cyber threat indicators.
- As mandated by CISA, DHS has also released guidance to help non-federal entities share cyber threat indicators (available at https://www.us-cert.gov/ais)
- CISA requires that private entities protect the data they collect, maintain and share from unauthorized access and disclosure. Further, the Act requires the scrubbing of personally identifiable information before a threat indicator is shared
  - DHS has also issued guidelines both for federal entities and the private sector to protect private information and civil liberties, as well as a Privacy Impact Assessment

What can be shared?: “Cyber Threat Indicator” Definition – 6 U.S.C. § 1501(6)

- Malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;
- A method of defeating a security control or exploitation of a security vulnerability;
- A security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;
- A method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;
- Malicious cyber command and control;
- The actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;
- Any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or
- Any combination thereof.

What can be shared?: “Defensive Measure” Definition - 6 U.S.C. § 1501(7)

- An action, device, procedure, signature, technique, or other measure … that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability.
- The term “defensive measure” does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting such information system not owned by the private entity operating the measure; or another entity or Federal entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure.

Cyber Threat Indicators and Defensive Measures

- What can and cannot be shared as a cyber threat indicator:
  - Effectively, the only information that can be shared is information that is **directly** related to and necessary to identify or describe a cybersecurity threat.
  - Information is not directly related to a cybersecurity threat if it is not necessary to detect, prevent, or mitigate the cybersecurity threat.
  - Example: a spear phishing email.
    - For a phishing email, personal information about the sender, malicious URL in the e-mail, malware files attached to the e-mail, the content of the e-mail, and additional email information related to the malicious email or potential cybersecurity threat actor, such as Subject Line, Message ID, and X-Mailer, could be considered directly related to a cybersecurity threat.
    - The name and e-mail address of the targets of the email (i.e., the “To” address), however, would usually be personal information not directly related to a cybersecurity threat and therefore should not be included as part of the cyber threat indicator.
- Federal agencies and private entities may share and operate defensive measures as defined by CISA as well.

DHS Guidance on Information Sharing

- There are three methods for private entities to share information with the NCCIC, each of which permits a non-federal entity to be eligible for the fullest liability protection available under CISA:

  1) AIS - Non-federal entities may share cyber threat indicators and defensive measures with federal entities using DHS's AIS initiative

     - AIS leverages a technical specification for the format and exchange of cyber threat indicators and defensive measures using the Structured Threat Information eXchange (STIX) and Trusted Automated eXchange of Indicator Information (TAXII). By using standardized fields (STIX) and communication (TAXII), AIS enables organizations to share structured cyber threat information in a secure and automated manner.
     - Participants must acquire their own TAXII client server that will communicate with the DHS TAXII server. AIS participants also execute the AIS Terms of Use (https://www.us-cert.gov/sites/default/files/ais_files/AIS_Terms_of_Use.pdf), and follow submission guidance that outlines the type of information that should and should not be provided when submitting cyber threat indicators and defensive measures through AIS

DHS Guidance on Information Sharing (cont'd)

2) Web Form - Non-federal entities may share cyber threat indicators and defensive measures with DHS's NCCIC by filling out a web form on a DHS website (https://www.us-cert.gov/ais)

3) E-Mail - Non-federal entities may share cyber threat indicators and defensive measures with DHS's NCCIC by sending an email to DHS (see https://www.us-cert.gov/ais)

- Although the non-federal entity must perform a privacy scrub before sharing with the NCCIC, the NCCIC also does a privacy scrub (at least partially automated). Once a cyber threat indicator or defensive measure is received, analyzed and sanitized, the NCCIC will promptly share the indicator or defensive measure. If a portion of a threat indicator requires further review and possibly sanitizing activity, it will share with its federal partners the sanitized portions of a threat indicator and supplement it later with the additional sanitized information.

ISAC / ISAOs

- Non-federal entities may also share cyber threat indicators and defensive measures with federal entities through ISACs or ISAOs, which, if authorized, may share them with federal entities through DHS on their members' behalf.
- Private entities that share a cyber threat indicator or defensive measure with an ISAC or ISAO in accordance with the Act receive liability protection and other protections and exemptions for such sharing. Similarly, ISACs and ISAOs that share information with other private entities in accordance with the Act also receive liability protection if they take the required steps under the statute.
- ISACs have tiers of membership: relatively few current ISAC members are engaged in fully automated information sharing; and most ISACs have protocols allowing information providers to designate the security and confidentiality with which specific information must be handled.

Examples of Issues CISA Does Not Resolve

- Lawyers may understand the legal liability and reputational risks-- the cost and risk side of the equation-- better than the practical benefits of information sharing to the company, especially given the poor documentation of the real-world benefits. They may think their bosses do too, e.g., CEO, Board, etc. Lightening the cost side of the scale doesn't mean the benefits win out.
- Cost, resource, expertise, platform and other issues remain.
- CISA doesn't apply to all information sharing interactions, just what CISA enumerates, e.g., sharing of threat indicators, defensive measures, etc. CISA protections may not apply to all valuable communication available through an ISAO or ISAC, such as information and experiences relating to incident response, exercises, analysis of threats, etc. To the extent this is of concern, and it may not be, the risk of liability might remain a consideration.
- Government regulators are sending mixed messages. For example, the FCC recently approved rules that encourage more voluntary information sharing but at the same time seemed to require broadband internet access providers to notify the FCC of any unauthorized access to personal information, even in circumstances where CISA provides liability protection.

Questions and Answers

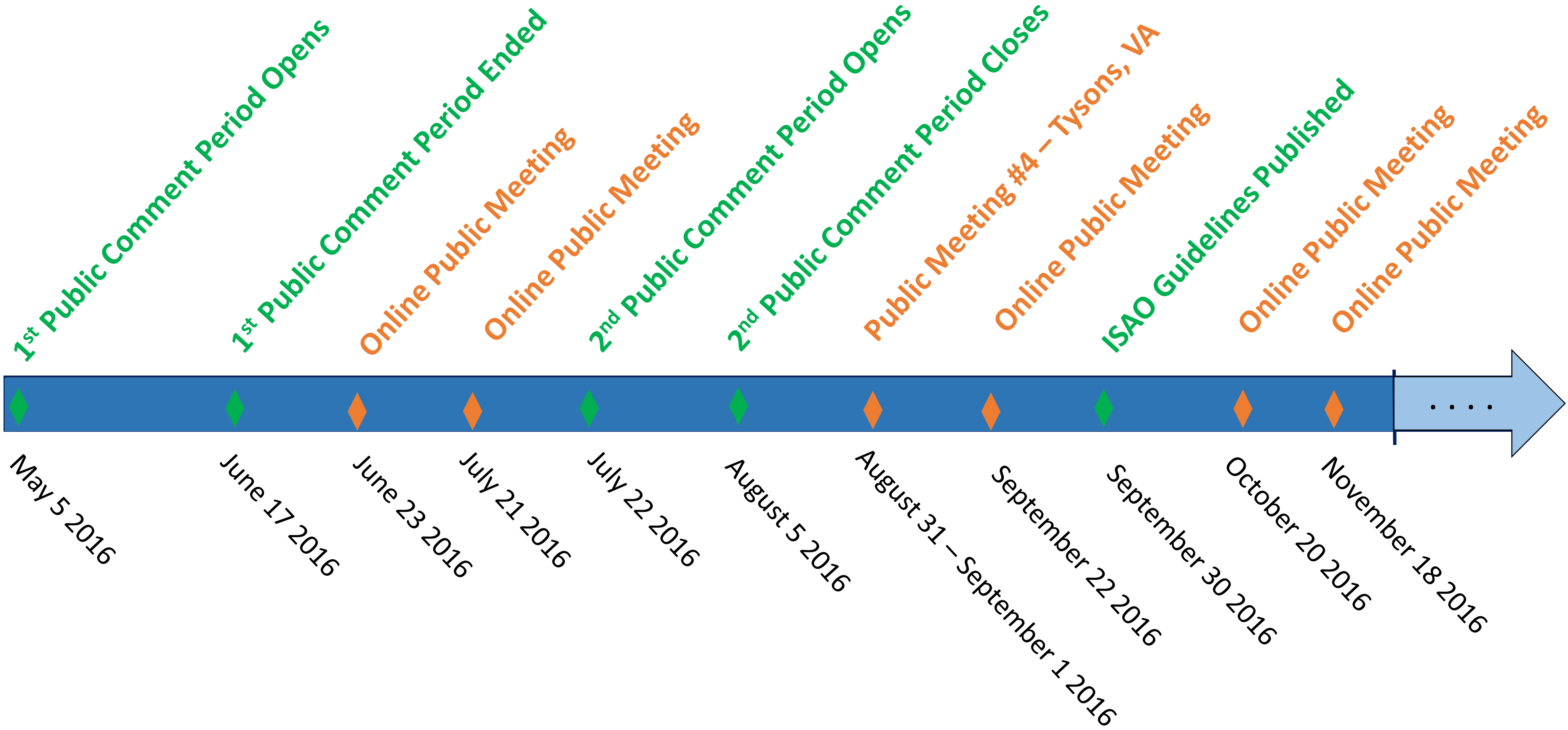
ISAO
Standards Organization

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

Akin Gump
STRAUSS HAUER & FELD LLP

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

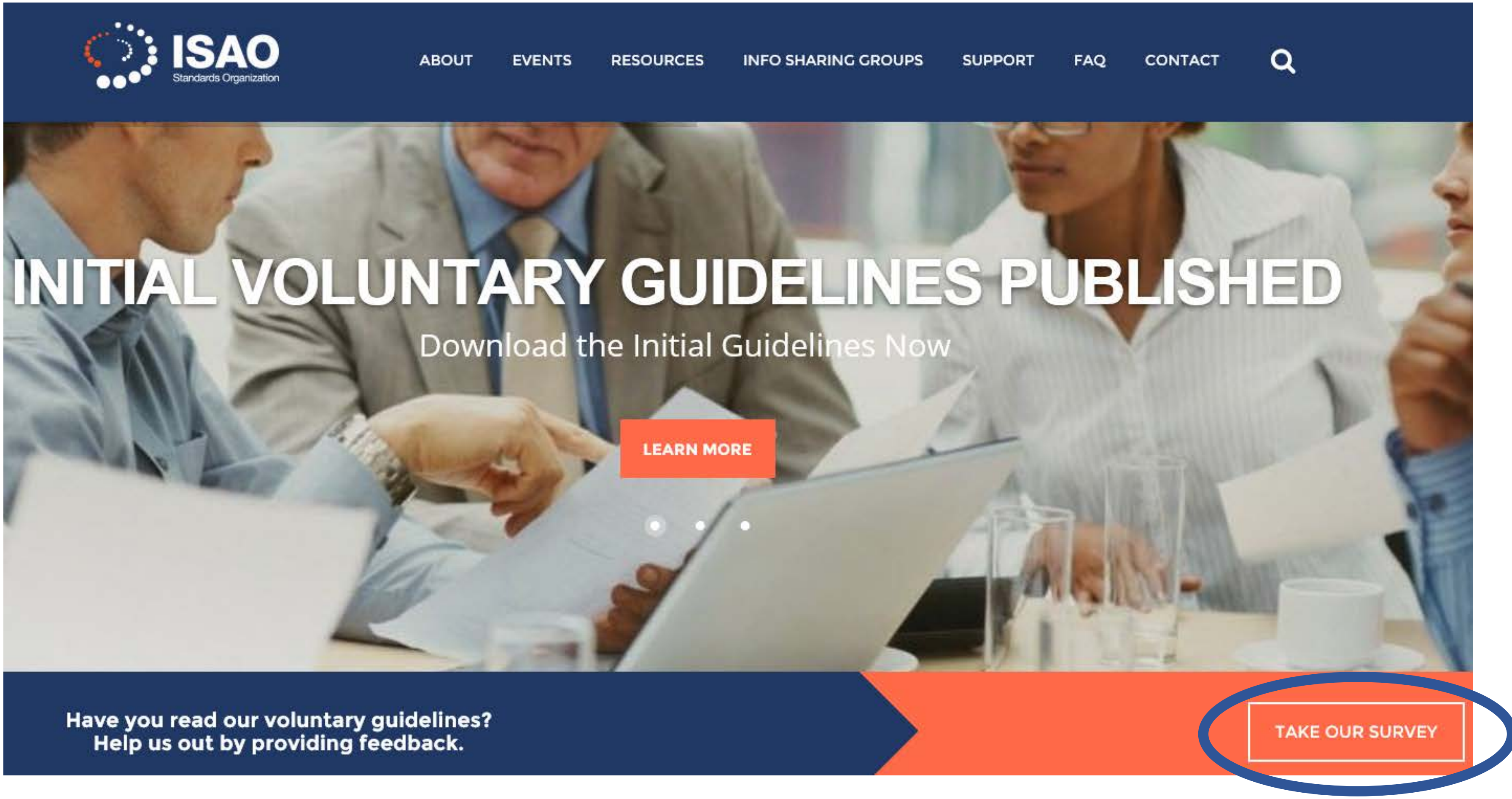
ISAO Guidelines Published
September 30 2016

Online Public Meeting
October 20 2016

Online Public Meeting
November 18 2016

. . . .

ISAO SO Survey



INITIAL VOLUNTARY GUIDELINES PUBLISHED

Download the Initial Guidelines Now

Have you read our voluntary guidelines?
Help us out by providing feedback.

Give us your feedback by November 30th

Future Documents

- Evolving Community Body of Knowledge
- Next voluntary guideline approved for development:
  - ISAO 600-3: State, Local, Tribal & Territorial Issues

    An intro – midlevel discussion of issues impacting information sharing at subnational levels
- Frequently Mentioned Topics:
  - Financial Models of ISAOs
  - Legal Considerations
  - International Considerations

What’s Next? (1 of 2)

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 2)

ISAO
Standards Organization

- Also currently <u>considering</u> 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 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

Give us your feedback by November 30th

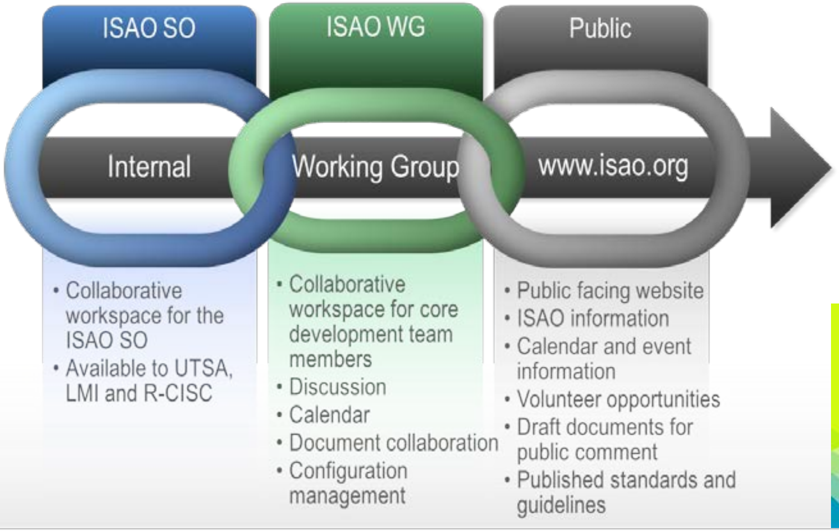
Building the Community

ISAO
Standards Organization

- Spreading the Word to Promote Information Sharing
  - FS-ISAC Fall Summit
  - Cross-Sector Leadership Forum
  - Defense Transportation Fall Conf
  - Midwest Cyber Center
  - MS-ISAC Annual Meeting
  - IT and Comm Sector Annual Meeting
  - San Antonio Cyber Committee
  - Cyber Southwest
- Developing 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

Come see us at RSA!
Booth 4436 in North Expo

RSAConference2017
Moscone Center | San Francisco
February 13 – 17, 2017

National Information Sharing Conference

ISAO
Standards Organization

Announcement Coming Soon!

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

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

Bringing the Community Together

New and Emerging ISAOs Roundtable

ISAO
Standards Organization

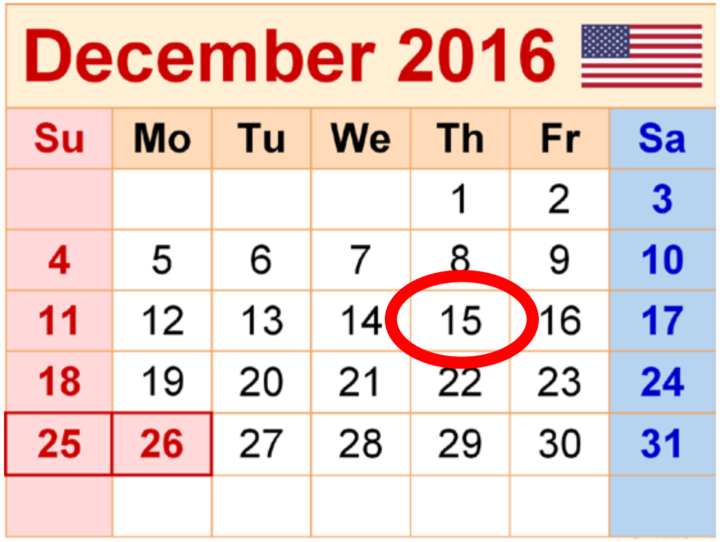
- December 8 at 2pm CT
- Open to new and emerging ISAOs
- Opportunity to share knowledge and ask questions
- December Topic: *An Introduction to Information Sharing*
- Guest Speaker: Kent Landfield, Director of Standards and Technology Policy, Intel Security
- Register your ISAO on ISAO.org to participate in Roundtable discussions

Building Capability and Capacity

Mark Your Calendars

ISAO
Standards Organization

- Online public meeting December 15th at 1pm Central time
- Information sharing insights, updates from the ISAO SO, and your chance to engage



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

Ongoing Engagement

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!