ISAO
Standards Organization

ISAO SP 8000: FAQs for ISAO General Counsels

v1.0

September 21, 2017

ISAO SP 8000

Frequently Asked Questions for ISAO General Counsels

V1.0
ISAO Standards Organization
September 21, 2017

Acknowledgments

This publication was developed by the Information Sharing and Analysis Organization Standards Organization (ISAO SO) with representatives from the private, professional, and government communities in an ongoing effort to produce a unified, voluntary set of guidelines and guidance for information sharing. The ISAO SO and the Working Group leadership are listed below.

ISAO Standards Organization
Gregory B. White, Ph.D.
ISAO SO—Executive Director
Director, Center for Infrastructure Assurance and Security, UTSA

Richard Lipsey,
ISAO SO—Deputy Director
Senior Strategic Cyber Lead, LMI

Suzie Squier
Executive Director
Retail Cyber Intelligence Sharing Center

Working Group 4—Privacy and Security

David Turetsky
Visiting Assistant Professor at the University of Albany College of Emergency Preparedness, Homeland Security and Cybersecurity

Carl Anderson
Vice President
Van Scoyoc Associates

Norma Krayem
Senior Policy Advisor
Holland and Knight LLP

The ISAO SO leadership would also like to acknowledge those individuals who contributed significantly in the development of these guidelines:

Carl Anderson, Vice President, Van Scoyoc Associates; Hon. Stuart M. Gerson, Epstein Becker & Green, P.C.; Norma Krayem, Holland and Knight LLP; and David Turetsky, Visiting Assistant Professor at the University of Albany, College of Emergency Preparedness, Homeland Security and Cybersecurity.

Special thanks from the authors goes to Marlis Cook, ISAO SO Advisor, Allen Shreffler, ISAO SO Chief of Lifecycle Development, and ISAO SO staff.

This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award No. 2015-PD-128-000001. Disclaimer: “The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security.”

Revision Updates

Item	Version	Description	Date
1	1.0	Initial publication	September 21, 2017

Table of Contents

1 PREFACE

Broadening participation in voluntary information sharing is an important goal, the success of which will fuel the creation of an increasing number of Information Sharing and Analysis Organizations (ISAOs) across a wide range of corporate, institutional, and governmental sectors. While information sharing has been occurring for many years, the Cybersecurity Information Sharing Act of 2015[1] (CISA) was intended to encourage public- and private-sector entities to share cyber-threat information by removing legal barriers and adding certain express liability protections that apply in several certain circumstances. Broadly, as explained in the legislative history, CISA provides "positive legal authorities for private companies to (1) monitor their networks, or those of their customers upon authorization and written consent, for cybersecurity purposes; (2) take defensive measures to stop cyber-attacks; and (3) share cyber threat information with each other and with the government to further collective cybersecurity."[2] CISA therefore provides an environment, and potentially serves as a catalyst, for increasing private-sector information sharing. As such proliferation continues, an organizational general counsel likely will be called upon to recommend whether to participate in such an effort.

To aid in that decision making, we have set forth a compilation of frequently asked questions and related guidance that might shed light on evaluating the potential risks and rewards of information sharing and the development of policies and procedures to succeed in it. We do not pretend that the listing of either is exhaustive, and nothing contained herein should be considered to provide legal advice—that is the ultimate prerogative of the in-house and outside counsel of each organization. And while this memorandum is targeted at general counsels, we also hope that it might be useful to others who contribute to decisions about cyber-threat information sharing and participation in ISAOs.

[1] See Pub. L. No. 114-113, div. N., 129 Stat. 2242, 29362956, at https://www.congress.gov/114/plaws/publ113/PLAW-114publ113.pdf

[2] See S. Rept. No. 114-32, at 2 (2015) at https://www.congress.gov/congressional-report/114th-congress/senate-report/32/1

2 FREQUENTLY ASKED QUESTIONS

2.1 THE BENEFITS OF INFORMATION SHARING

The first question: “What benefit can information sharing about cyber-threat vectors, hacking efforts, company response plans, and outcomes produce for my organization?”

- Effectively done, sharing can provide information, otherwise unavailable to a given entity, that might prevent or at least identify compromises, reveal vulnerabilities—potentially before exploitation—and promote useful system modifications, threat reduction, and cost savings.
- It also can be a material contribution to protecting the nation’s vital assets, including its critical infrastructure.
- Sharing can occur without including personal information, removing many of the concerns that organizations have with sharing information.

2.2 THE GENERAL RISKS

“What general risks will information sharing present, and how can they be best anticipated and avoided if my organization participates?”

- While there always is some possibility of an increase in risk when an organization no longer has direct control over a piece of sensitive information that has been shared outside its walls, that quantum of risk should be weighed against the benefits that sharing can provide to your organization, especially when you have taken steps to mitigate compromise. Furthermore, federal laws such as CISA provide protections that lower the risk by providing clear authority for sharing and other protections for sharing information. Operating in a trusted environment, maximizing automated sharing where possible, and providing coordinated privacy and security training to reduce the possibility of human error are all mitigating factors that counsels should carefully consider in conjunction with sharing efforts. Additionally, there are many privacy protections built into CISA. For example, CISA limits the definition of “cyber-threat indicator” to information necessary to describe or identify an attribute of a cybersecurity threat. Also, information that is not directly related to a cybersecurity threat that the non-federal entity knows at the time of sharing to be personal information of a specific individual, or that identifies a specific individual, should be removed before sharing—for liability protection.
- To the extent that a counsel is concerned with potential reputation risk in the context of sharing, note that ISAO protocols such as the Traffic Light Protocol generally allow information providers to affect or control the extent of distribution, identification, and so forth. Some also provide tiers based upon levels of trust that can limit sharing due to knowledge and experience with recipients.

- General or outside counsels should analyze any existing insurance policies to determine any positive or negative effect on coverage and whether threat sharing might be considered useful in, or otherwise affect, policy underwriting. Organizations must answer whether entering a sharing arrangement may mitigate existing risks or present new risks.

2.3 ADVANTAGES OF SHARING WITH OTHER NON-GOVERNMENTAL ENTITIES OR THE GOVERNMENT

"If we participate, what are the advantages of sharing with other non-governmental entities (including with an ISAO) or with the government?"

- The answer to this question is situational. Broader sharing could increase the benefits to your organization because of the advantages that multiple sources of information, defense mechanisms, and other things provide. Sharing cyber-threat indicators and defensive measures helps ensure that one entity's detection of a threat allows other entities to quickly defend against that threat, which helps mitigate attacks quickly and protects the entire ecosystem.
- Sharing with an ISAO might help your organization leverage resources, such as threat analytics, to which you are unable to dedicate resources on your own. Executive Order (EO) 13691, "Promoting Private Sector Cybersecurity Information Sharing," was signed on February 13, 2015. EO 13691 encourages the development of ISAOs to serve as focal points for cybersecurity collaboration within the private sector and between the private sector and government. ISAOs provide a central resource for their members to gather information on cyber threats to critical infrastructure and for two-way sharing of cyber-threat information between the private and public sectors.
- Private entities receive liability protection and other protections and exemptions for sharing cyber-threat indicators and defensive measures with other private entities, including ISAOs, in accordance with CISA.[3] Such sharing is authorized "notwithstanding any other provision of law," meaning that any conflicting law is overridden when conducted in accordance with CISA. To receive liability protection or to benefit from CISA's other protections, an entity must share cyber-threat indicators or defensive measures for a cyber-security purpose. Before sharing, the entity must remove information not directly related to a cybersecurity threat that it knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual, and the entity should implement and use a security control

[3] See 6 U.S.C. § 1503 at http://uscode.house.gov/view.xhtml?path=/prelim@title6/chapter6/subchapter1&edition=prelim and 6 U.S.C. 1505(b)(1) at http://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title6-section1505&num=0&edition=prelim

to protect against unauthorized access to or acquisition of the information. Finally, when receiving such information, the entity must observe lawful restrictions placed by the sharing entity.[4]

- Similarly, private entities, including ISAOs, that share cyber-threat indicators or defensive measures with the federal government in accordance with CISA receive liability protection and other protections and exemptions.[5] Again, such sharing is authorized "notwithstanding any other provision of law," meaning that any conflicting law is overridden when conducted in accordance with CISA. To obtain liability protection when sharing with the federal government, private entities must share through the Department of Homeland Security (DHS)–operated capability and process for receiving cyber-threat indicators or under one of the exceptions to the use of that capability concerning previously shared cyber-threat indicators and sharing with federal regulatory authorities.[6] Non-federal entities sharing with the federal government also receive additional protections, including exemption from state and federal disclosure laws, exemption from certain state and federal regulatory use, no waiver of privilege for shared material, waiver from ex parte communications, and a limitation on permitted uses the government can make with the information that is shared.

2.4 POLICIES AND PROCEDURES

"What policies and procedures should my organization have in place to comply with the Cybersecurity Information Sharing Act of 2015?"

- Compliance with CISA[7] is a legal matter that should be carefully analyzed by an organization's counsel. CISA contains various protections designed to encourage entities to voluntarily share "cyber-threat indicators" and "defensive measures" with the federal government, state and local governments, and other private entities. Protections include exemption from liability as to sharing, non-waiver of privilege, and protections from Freedom of Information Act disclosure. CISA contemplates removal before sharing information not directly related to a cybersecurity threat that the sharing entity knows at the time of sharing to be personal information of a specific individual or information that

[4] For further information, see U.S. Department of Homeland Security and U.S. Department of Justice, Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015 (June 2015), at https://us-cert.gov/ais

[5] See 6 U.S.C. § 1503(c) at http://uscode.house.gov/view.xhtml?path=/prelim@title6/chapter6/subchapter1&edition=prelim and 6 U.S.C. § 1504(c)(1)(B) at http://uscode.house.gov/view.xhtml?path=/prelim@title6/chapter6&edition=prelim

[6] See 6 U.S.C. § 1504(c)(1)(B)(i) and (ii) at http://uscode.house.gov/view.xhtml?path=/prelim@title6/chapter6&edition=prelim

[7] For specific guidance on the legal requirements under CISA, please refer to the Cybersecurity Information Sharing Act of 2015 at https://www.gpo.gov/fdsys/pkg/FR-2016-06-15/pdf/2016-13742.pdf and https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf

identifies a specific individual.[8] If intending to share under CISA, organizational counsels should analyze and make a legal determination about their own information-handling policies and procedures to ensure they contemplate and appropriately handle such identifying information before sharing under CISA. One must do the removal before sharing occurs to benefit from liability protection.

- Before sharing cyber-threat indicators and defensive measures under CISA, private entities should have processes in place to ensure the removal of information not directly related to a cybersecurity threat that the entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual. The entity also should implement and use a security control to protect against unauthorized access to or acquisition of the cyber-threat information or defensive measures. When receiving such information, the entity also should have policies in place that require observing lawful restrictions placed by the sharing federal government or private entity.
- Similarly, a counsel contemplating sharing within an ISAO should consider whether its organization's current information-sharing and handling policies and procedures might affect or restrict sharing.
- It is incumbent upon an entity and its counsel to review the policies and processes of an ISAO before beginning an information-sharing program.

2.5 LIABILITY PROTECTIONS

"Does CISA provide complete liability protection for information shared through an ISAO?"

- The liability protections provided for in CISA for sharing in accordance with the Act are complex and require an independent judgment of organizational (and/or outside) counsel. In evaluating liability risk and protections for sharing through an ISAO, the counsel should consider the following:
  - CISA authorizes non-federal entities to monitor their networks and to share certain types of information—that is, cyber-threat indicators and defensive measures—both with other non-federal entities and with the federal government. It also contains specific liability protection for monitoring and sharing undertaken in accordance with the Act, which includes particularities about how the information must be shared with the government and what types of privacy and security reviews must occur.
  - CISA permits sharing information for a "cybersecurity purpose," as defined in the statute. The counsel should consider the various contexts in which

[8] For additional information, please see ISAO SP 4000 at https://testisao.lmi.org/products/isao-sp-4000-protecting-consumer-privacy-in-cybersecurity-information-sharing-v1-0/

information might be shared—for example, sharing threat indicators, response to threats or breaches, and joint readiness exercises—and the potential risks associated with each.

- That said, protections and regulatory limitations in CISA apply to actions taken under and in accordance with the Act. CISA's liability protection applies to monitoring information systems and the sharing or receiving of cyber-threat indicators under CISA. CISA makes clear that information shared by an entity to DHS cannot be used for regulatory reach-back and the federal government has limited purposes for using the information outside of cybersecurity. It is important to note that CISA's protections are specific to cyber information sharing, and it does not provide a blanket cover for all potential issues—as such, it should be reviewed with those limitations.

- The SAFETY Act[9] provides certain liability protections for providers of Qualified Anti-Terrorism Technologies if approved by DHS. It can be a tool for certain companies that can be used with CISA as well.

2.6 PRIVACY AND SECURITY POLICIES TO HAVE IN PLACE

"What privacy and security policies should my organization have in place before it begins to share information with an ISAO?"

- To avail oneself of liability protection provided in CISA, sharing must take place in accordance with the Act's specific provisions. Legal reviews before sharing should consider whether an organization has processes in place to ensure that certain personal information is reviewed for its relevance to the cybersecurity threat, and it should be removed before sharing if necessary. Note that most of the value of sharing can be achieved without including personal information. Again, the interpretation of whether an organization's activities are undertaken "in accordance with the Act" is a legal question for consideration and judgment by organizational counsel.

- In a more general sense, every organization participating in an ISAO should have a strong cybersecurity risk management program based on an assessment of its areas of risk and the advice of its counsel. On January 10, 2017, the National Institute of Standards and Technology (NIST) released for comment draft revisions to its landmark voluntary framework of cybersecurity standards. If adopted in current or revised form, the NIST standards would at least be useful points of reference for ISAOs, as are various standards issued by state governments, professional organizations, and the multitude of providers of legal, consulting, and insurance services that have standardized processes.

[9] For more information, consult https://www.safetyact.gov

2.7 METHOD FOR EXCHANGE OF INFORMATION

"If my organization chooses to participate in cyber-threat information sharing, should the exchange of information be done through an automated electronic system or by personal contact (or both)?"

- While automated means of sharing might have distinct advantages in synthesizing data—assuring speed in the process and enhancing privacy and security—the analytic value of human input should not be shortchanged in areas such as seeking innovation on preventing and solving cyber issues, presenting a united front in dealing with counterparts, and dealing effectively with agencies of government. Thus, the council should consider the relative merits of each approach.
- Liability protections come with the sharing of cyber-threat indicators and defensive measures regardless of whether removing information not directly related to a cybersecurity threat occurs through manual or technical means. Similarly, one receives liability protections in sharing cyber-threat indicators and defensive measures with DHS regardless of whether it's through the automated process and capability or through a manual means.
- The DHS Office of Cybersecurity and Communications, National Cybersecurity and Communications Integration Center, and United States Computer Emergency Readiness Team are leading efforts to automate and structure operational cybersecurity information-sharing techniques across the globe. Several community-driven technical specifications that are free for public use have been designed to enable automated information sharing for cybersecurity situational awareness, real-time network defense, and sophisticated threat analysis. These include the following:
  - TAXII™, the Trusted Automated eXchange of Indicator Information
  - STIX™, the Structured Threat Information eXpression
  - CybOX™, the Cyber Observable eXpression.

2.8 THE DIVERSITY OF ISAOS

"Are all ISAOs the same?"

There is an ever-increasing number of ISAOs, and they are not all the same. You should think about how any given ISAO has provided value in its sector or region, whether it has exercised control over the information that is shared within it, and the ability of a given member to influence both ISAO policy and the dissemination of information within the organization.