ISAO SP-8000

Frequently Asked Questions for ISAO General Counsels

Draft Document—Request For Comment

ISAO SO—2017 v0.01

ISAO Standards Organization

April 20, 2017

Acknowledgements

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
Dr. Gregory B. White
ISAO SO—Executive Director

Richard Lipsey,
ISAO SO—Deputy Director

Brian Engle
Executive Director
Retail Cyber Intelligence Sharing Center

Working Group Four—Privacy and Security

David Turetsky
Partner
Akin Gump Strauss Hauer & Feld LLP

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:

Table of Contents

Revision Updates

Item	Version	Description	Date

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 had been occurring for many years, the Cybersecurity Act of 2015 (Pub. L. No. 114-113) (CISA) was intended to encourage participation by even more entities by adding certain express liability protections that apply in several certain circumstances. As such proliferation continues, it likely will be organizational general counsel who will be called upon to recommend to their superiors whether to participate in such an effort.

With the growth of the ISAO movement, it is possible that joint private/public information exchange as contemplated under CISA will result in expanded liability protection and government policy that favors cooperation over an enforcement mentality.

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 therein should be considered to contain 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 hope that it also might be useful to others who contribute to decisions about cyber-threat information sharing and participation in ISAOs.

2 FREQUENTLY ASKED QUESTIONS:

2.1 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 prior to exploitation, and help identify victims for notification purposes where information reveals compromised customer

IP addresses, and promote useful system modifications, threat reduction and cost savings.

- It also can be a material contribution to protecting the nation's critical infrastructure.

- It also should be noted that most of the value of sharing can be accomplished without the inclusion of personal information (PII) removing many of the concerns organizations may have with sharing information.

2.2 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. 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 counsels should carefully consider in conjunction with sharing efforts.

- To the extent that counsel is concerned with potential reputation risk in the context of sharing, note that ISAO protocols generally allow information providers to affect or control the extent of distribution, identification, etc. Some also provide tiers based upon levels of trust that can limit sharing based upon 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 risk 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 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, *etc*., provide. Sharing with an ISAO also might help your organization leverage resources, such as threat analytics, to which you are unable to dedicate resources on you own. On February 13 2015, Executive Order 13691, Promoting Private Sector Cybersecurity Information Sharing was signed. 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 gathering information on cyber threats to critical infrastructure and two-way sharing of cyber threat information between the private and public sector.
- If CISA's pre-requisites are met, CISA's liability protections apply both to cyber threat information exchanges between private sector entities including ISAOs and the government and to cyber threat information exchanges between private sector entities alone.

2.4 WHAT POLICIES AND PROCEDURES SHOULD MY ORGANIZATION HAVE IN PLACE TO COMPLY WITH THE CYBERSECURITY INFORMATION SHARING ACT OF 2015 ("CISA")?

- Compliance with CISA is a legal matter that should be carefully analyzed by organization counsel. CISA contains various protections designed to encourage entities voluntarily to 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 FOIA disclosure. CISA also contemplates redaction of certain information (e.g. personally identifiable information or PII) that is not directly related to a cybersecurity threat that the entity knows at the time of sharing that identifies specific individuals or information personal to them. 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 prior to sharing under CISA.[1]

- Similarly, a counsel contemplating sharing within an ISAO should consider whether their organization's current information policies and procedures might affect or restrict sharing.

- It is incumbent upon an entity and their counsel to review the policies and processes of an ISAO prior to beginning an information sharing program.

2.5 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, counsel should consider the following:

  - CISA authorizes non-federal entities to monitor their networks and to share certain types of information-- – *i.e.*, cyber threat indicators and defensive measures – both with other non-federal entities and the federal government. It also contains specific liability protection for monitoring

[1] [1] For specific guidance on the legal requirements under CISA, please refer to the Cybersecurity Information

Sharing Act of 2015 (CISA) Final Guidance Documents published by the Departments of Justice and Department of Homeland Security 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 .

and sharing undertaken in accordance with the Act, which includes particularities about how the information must be shared when sharing with the government, and what types of privacy and security reviews must occur.

- CISA also contemplates sharing information for a "cybersecurity purpose," as defined in the statute. Counsel should consider the various contexts in which information might be shared, *e.g.*, sharing threat indicators, response to threats or breaches, and joint readiness exercises, and the potential risks associated with each.

- Moreover, as a matter of policy, the Federal government has stated that it will not turn over reported CISA information to enforcement agencies, and reported information is not made public.
- CISA also addresses the inadvertent disclosure of personally identifiable information. In any event, counsel must be attentive to have in place measures to protect confidential information that is to be shared.

- That said, protections and regulatory limitations in CISA apply to actions taken under and in accordance with the Act. There currently is no federal law that can insulate an entity from federal enforcement authorities like the FTC or Office of Civil Rights of the Department of Health & Human Services, from State authorities, or from private litigation, in the case of data breaches of sufficient magnitude that they must be publicly reported.

- Whether and in what circumstances an organization may be able to apply for legal liability relief under the antiterrorism law, SAFETY Act. The SAFETY Act provides legal liability protections for providers of anti-terrorism products or services. For more information please consult: https://www.safetyact.gov/

2.6 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 prior to sharing should consider whether an organization has processes in place to ensure certain personally identifying information ("PII") is reviewed for its relevance to the cybersecurity threat, and removed prior to sharing if necessary. This is especially true for PHI (Protected Health Information) covered by HIPAA, which has requirements beyond CISA's. HIPAA also offers certain additional protections if data are encrypted. Note that most of the value of sharing can be achieved without including PII. 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 cyber security 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 published about standards

2.7 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 short-changed in areas like seeking innovation on prevention and solution of cyber issues, presenting a united front in dealing with counterparts and in dealing effectively with

agencies of government. Thus, counsel should consider the relative merits of each approach.

- The DHS Office of Cybersecurity and Communications, National Cybersecurity and Communications Integration Center, and US-CERT 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:
  - TAXII™, the Trusted Automated eXchange of Indicator Information;
  - STIX™, the Structured Threat Information eXpression; and
  - CybOX™, the Cyber Observable eXpression.

2.8 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, how 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 dissemination of information within the organization.