



ISAO SP-8000

Frequently Asked Questions for ISAO General Counsels

Draft Document—Request For Comment

ISAO SO—2017 v0.02

ISAO Standards Organization

May 30, 2017

Copyright © 2017, ISAO SO (Information Sharing and Analysis Organization Standards Organization). Any part of this publication may be distributed, posted, reproduced, stored in a retrieval system, or transmitted in any form or by any means without the prior written permission of the copyright owner.

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:

(Names Under Consideration)



Table of Contents

1	Preface	2
2	Frequently Asked Questions:	2
2.1	What benefit can information sharing about cyber-threat vectors, hacking efforts, company response plans and outcomes produce for my organization?	2
2.2	What general risks will information sharing present and how can they be best anticipated and avoided if my organization participates?	3
2.3	If we participate, what are the advantages of sharing with other non-governmental entities (including with an ISAO), or with the government?	4
2.4	What policies and procedures should my organization have in place to comply with the Cybersecurity Information Sharing Act of 2015 (“CISA”)?	6
2.5	Does CISA provide complete liability protection for information shared through an ISAO?	7
2.6	What privacy and security policies should my organization have in place before it begins to share information with an ISAO?	8
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)?	9
2.8	Are all ISAOs the same?	10

1 Revision Updates

Item	Version	Description	Date

2

3

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 Information Sharing Act of 2015 (Pub. L. No. 114-113, div. N., 129 Stat. 2242, 2936 – 2956 (2015)) (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.” S.Rep. No. 114-32, at 2 (2015). CISA therefore provides an environment and potentially serves as a catalyst for increasing private sector information sharing. As such proliferation continues, it likely will be organizational general counsel who 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 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 cyberthreat 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?

- 39
- 40
- 41
- 42
- 43
- 44
- 45
- 46
- 47
- 48
- 49
- 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 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 organizations may have with sharing information.

50

51

52

53

2.2 WHAT GENERAL RISKS WILL INFORMATION SHARING PRESENT AND HOW CAN THEY BE BEST ANTICIPATED AND AVOIDED IF MY ORGANIZATION PARTICIPATES?

- 54
- 55
- 56
- 57
- 58
- 59
- 60
- 61
- 62
- 63
- 64
- 65
- 66
- 67
- 68
- 69
- 70
- 71
- 72
- 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 counsels should carefully consider in conjunction with sharing efforts.¹ 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 liability protection attaches only if information 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 information that identifies a specific individual is removed prior to sharing.

73 • To the extent that counsel is concerned with potential reputation risk in the
74 context of sharing, note that ISAO protocols such as the Traffic Light Proto-
75 col generally allow information providers to affect or control the extent of
76 distribution, identification, etc. Some also provide tiers based upon levels of
77 trust that can limit sharing based upon knowledge and experience with re-
78 cipients.

79

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

85

86 **2.3 IF WE PARTICIPATE, WHAT ARE THE ADVANTAGES OF**
87 **SHARING WITH OTHER NON-GOVERNMENTAL ENTITIES**
88 **(INCLUDING WITH AN ISAO), OR WITH THE**
89 **GOVERNMENT?**

90

91 • The answer to this question is situational. Broader sharing could increase
92 the benefits to your organization because of the advantages that multiple
93 sources of information, defense mechanisms, etc., provide. Sharing cyber
94 threat indicators and defensive measures helps ensure that one entity's de-
95 tection of a threat allows other entities to quickly defend against that threat,
96 which helps quickly mitigate attacks and protects the entire ecosystem.

97 • Sharing with an ISAO might help your organization leverage resources, such
98 as threat analytics, to which you are unable to dedicate resources on you
99 own. On February 13 2015, Executive Order 13691, Promoting Private Sec-
100 tor Cybersecurity Information Sharing was signed. EO 13691 encourages the
101 development of ISAOs to serve as focal points for cybersecurity collaboration
102 within the private sector and between the private sector and government.

103 ISAOs provide a central resource for gathering information on cyber threats
104 to critical infrastructure and two-way sharing of cyber threat information be-
105 tween the private and public sector.

- 106
- 107
- 108
- 109
- 110
- 111
- 112
- 113
- 114
- 115
- 116
- 117
- 118
- 119
- 120
- 121
- 122
- 123
- 124
- 125
- 126
- 127
- 128
- 129
- 130
- 131
- 132
- 133
- 134
- 135
- 136
- 137
- 138
- 139
- 140
- 141
- 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. 6 U.S.C. § 1503, § 1505(b)(1). Such sharing is authorized “notwithstanding any other provision of law,” meaning 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 cybersecurity purpose. Prior to sharing, the entity must remove 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, and implement and use a security control 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. 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), *available at* <https://us-cert.gov/ais>.
 -
 - 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. 6 U.S.C. § 1503(c); 6 U.S.C. § 1504(c)(1)(B). Again, such sharing is authorized “notwithstanding any other provision of law,” meaning 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 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. See 6 U.S.C. § 1504(c)(1)(B)(i) and (ii). 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 of the information that is

142 shared. For further information, see U.S. Department of Homeland Security
143 and U.S. Department of Justice, Guidance to Assist Non-Federal Entities to
144 Share Cyber Threat Indicators and Defensive Measures with Federal Entities
145 under the Cybersecurity Information Sharing Act of 2015 (June 2015), *availa-*
146 *ble at* <https://us-cert.gov/ais>.
147

148 **2.4 WHAT POLICIES AND PROCEDURES SHOULD MY** 149 **ORGANIZATION HAVE IN PLACE TO COMPLY WITH THE** 150 **CYBERSECURITY INFORMATION SHARING ACT OF 2015** 151 **(“CISA”)?**

- 153 • Compliance with CISA is a legal matter that should be carefully analyzed by
154 organization counsel. CISA contains various protections designed to encour-
155 age entities voluntarily to share “cyber threat indicators” and “defensive
156 measures” with the federal government, state and local governments, and
157 other private entities. Protections include exemption from liability as to shar-
158 ing, non-waiver of privilege, and protections from FOIA disclosure. CISA
159 contemplates removal before sharing of information not directly related to a
160 cybersecurity threat that the sharing entity knows at the time of sharing to be
161 personal information of a specific individual or information that identifies a
162 specific individual. If intending to share under CISA, organizational coun-
163 sels should analyze and make a legal determination about their own infor-
164 mation handling policies and procedures to ensure they contemplate and
165 appropriately handle such identifying information prior to sharing under
166 CISA.² Removal must also occur before sharing occurs in order to benefit
167 from liability protection.
- 168 •
- 169 • Prior to sharing cyber threat indicators and defensive measures under CISA,
170 private entities should have processes in place to ensure the removal of in-
171 formation not directly related to a cybersecurity threat that the entity knows

² ² For specific guidance on the legal requirements under CISA, please refer to the Cyberse-
curity Information

Sharing Act of 2015 (CISA) Final Guidance Documents published by the Departments of Jus-
tice 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 .

172 at the time of sharing to be personal information of a specific individual or
173 information that identifies a specific individual. The entity should also im-
174 plement and use a security control to protect against unauthorized access to
175 or acquisition of the cyber threat information or defensive measures. When
176 receiving such information, the entity should also have policies in place that
177 require the observation of lawful restrictions placed by the sharing federal
178 government or private entity.

- 179
- 180 • Similarly, a counsel contemplating sharing within an ISAO should consider
181 whether their organization’s current information sharing and handling poli-
182 cies and procedures might affect or restrict sharing.
- 183
- 184 • It is incumbent upon an entity and its counsel to review the policies and pro-
185 cesses of an ISAO prior to beginning an information sharing program.
- 186

187 **2.5 DOES CISA PROVIDE COMPLETE LIABILITY** 188 **PROTECTION FOR INFORMATION SHARED THROUGH** 189 **AN ISAO?**

- 190
- 191 • The liability protections provided for in CISA for sharing in accordance with
192 the Act are complex and require an independent judgment of organizational
193 (and/or outside) counsel. In evaluating liability risk and protections for shar-
194 ing through an ISAO, counsel should consider the following:
 - 195
 - 196 ○ CISA authorizes non-federal entities to monitor their networks and to
197 share certain types of information – *i.e.*, cyber threat indicators and defen-
198 sive measures – both with other non-federal entities and the federal gov-
199 ernment. It also contains specific liability protection for monitoring and
200 sharing undertaken in accordance with the Act, which includes particular-
201 ities about how the information must be shared when sharing with the
202 government, and what types of privacy and security reviews must occur.
 - 203
 - 204 ○ CISA permits sharing information for a “cybersecurity purpose,” as de-
205 fined in the statute. Counsel should consider the various contexts in

206 which information might be shared, *e.g.*, sharing threat indicators, re-
207 sponse to threats or breaches, and joint readiness exercises, and the poten-
208 tial risks associated with each.

- 209
210
- 211 ○ That said, protections and regulatory limitations in CISA apply to actions
212 taken under and in accordance with the Act. CISA’s liability protection
213 applies to monitoring information systems and the sharing or receiving of
214 cyber threat indicators under CISA. There currently is no federal law that
215 can insulate an entity from federal regulatory authorities like the FTC or
216 Office of Civil Rights of the Department of Health & Human Services,
217 from State authorities, or from private litigation, in the case of data
218 breaches of sufficient magnitude that they must be publicly reported.

- 219
- 220 ● Whether and in what circumstances an organization may be able to apply for
221 legal liability relief under the antiterrorism law, the SAFETY Act. The
222 SAFETY Act provides certain liability protections for providers of Qualified
223 Anti-Terrorism Technologies approved by the Department of Homeland Se-
224 curity. For more information please consult: <https://www.safetyact.gov/>
225

226 **2.6 WHAT PRIVACY AND SECURITY POLICIES SHOULD MY** 227 **ORGANIZATION HAVE IN PLACE BEFORE IT BEGINS TO** 228 **SHARE INFORMATION WITH AN ISAO?**

- 229
- 230 ● To avail oneself of liability protection provided in CISA, sharing must take
231 place in accordance with the Act’s specific provisions. Legal reviews prior to
232 sharing should consider whether an organization has processes in place to
233 ensure certain personal information is reviewed for its relevance to the cy-
234 bersecurity threat, and removed prior to sharing if necessary. Note that
235 most of the value of sharing can be achieved without including personal in-
236 formation. Again, the interpretation of whether an organization’s activities
237 are undertaken “in accordance with the Act” is a legal question for consider-
238 ation and judgment by organizational counsel.
239

- 240
- 241
- 242
- 243
- 244
- 245
- 246
- 247
- 248
- 249
- 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 published about standards.

250

251 **2.7 IF MY ORGANIZATION CHOOSES TO PARTICIPATE IN**

252 **CYBER THREAT INFORMATION SHARING, SHOULD THE**

253 **EXCHANGE OF INFORMATION BE DONE THROUGH AN**

254 **AUTOMATED ELECTRONIC SYSTEM OR BY PERSONAL**

255 **CONTACT (OR BOTH)?**

- 256
- 257
- 258
- 259
- 260
- 261
- 262
- 263
- 264
- 265
- 266
- 267
- 268
- 269
- 270
- 271
- 272
- 273
- 274
- 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 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.
 -
 - Liability protections attach to sharing of cyber threat indicators and defensive measures regardless of whether removal of information not directly related to a cybersecurity threat occurs using a manual or technical means. Similarly, sharing cyber threat indicators and defensive measures with DHS regardless of whether through the automated process and capability or through a manual means receives certain liability protections.
 -
 - 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

275 techniques across the globe. Several community-driven technical specifica-
276 tions that are free for public use have been designed to enable automated in-
277 formation sharing for cybersecurity situational awareness, real-time network
278 defense and sophisticated threat analysis. These include:

- 279 ○ TAXII™, the Trusted Automated eXchange of Indicator Information;
- 280 ○ STIX™, the Structured Threat Information eXpression; and
- 281 ○ CybOX™, the Cyber Observable eXpression.

282

283 **2.8 ARE ALL ISAOS THE SAME?**

284

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