ISAO
Standards Organization

ISAO SP 4000: Protecting Consumer Privacy in Cybersecurity Information Sharing

v1.0

July 26, 2017

ISAO SP 4000

Protecting Consumer Privacy in Cybersecurity Information Sharing

v1.0
ISAO Standards Organization
July 26, 2017

Acknowledgments

This publication was developed by the Information Sharing and Analysis Organization Standards Organization (ISAO SO) with representatives from industry, government, civil society, and academia 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 Four—Privacy and Security

David Turetsky
Visiting 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:

Scott Algeier, Executive Director, Information Technology-Information Sharing and Analysis Center (IT-ISAC); Sarah Geffroy, Director, Global Public Policy, AT&T; Robyn Greene, Policy Counsel and Government Affairs Lead, Open Technology Institute, New America Foundation; Joseph Lorenzo Hall, Chief Technologist, Center for Democracy & Technology; Norma Krayem, Holland and Knight LLP; Megan Stifel, Cybersecurity Policy Director at Public Knowledge; David Turetsky, Visiting Professor at the University of Albany, College of Emergency Preparedness, Homeland Security and Cybersecurity.

Special thanks from the authors goes to the ISAO SO Advisors and staff.

This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number, 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	July 26, 2017

Table of Contents

1 PREFACE

In September 2016, the Information Sharing and Analysis Organization Standards Organization published ISAO 300-1, *Introduction to Information Sharing*,[1] to promote sharing of cyber threat indicators and defensive measures. Section 9, "Information Privacy," included core and supporting principles for entities to consider in establishing an ISAO. This document supplements that high-level guidance to further assist entities as they assess the potential privacy implications of cybersecurity information sharing. It builds upon basic principles by outlining actions to promote efficient and effective information sharing while minimizing the impact on privacy interests. The primary target audience for this document is risk managers and those involved within an entity on a cross-disciplinary basis in making decisions about how to approach privacy when sharing cybersecurity information. Nevertheless, this document is maturity agnostic, and reflects actions an organization should consider regardless of its information sharing capabilities.

This document is not intended to create baseline requirements for regulatory or enforcement action. It is consistent with the *Cybersecurity Information Sharing Act of 2015 (CISA)*,[2] it draws upon *Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities*[3] from the Departments of Homeland Security and Justice, and it makes additional suggestions to advance privacy and facilitate robust information sharing.

2 GUIDING PRACTICES

1. Establish and implement written policies that identify the types of cybersecurity information shared within and by an organization; how it will be used, retained, and shared; and with whom it will be shared.

    - Issues for policy consideration may include cybersecurity information collection, use, access, receipt, retention, dissemination, minimization, and disposal.

    - Cybersecurity information may include information necessary to deter or protect against a cybersecurity threat such as indicators of compromise; threat actor tactics, techniques, and procedures; and malicious code. It would not typically include, for example, spear phishing target email addresses or names.

2. Disclose, retain, and use information shared for a cybersecurity purpose only for cybersecurity purposes, as defined by CISA.

[1] See https://www.isao.org/products/isao-300-1-introduction-to-information-sharing/.

[2] See https://www.law.cornell.edu/uscode/text/6/chapter-6/subchapter-I

[3] See https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf.

3. Before sharing cybersecurity information, remove or redact information that is known at the time of sharing to be information of a specific individual or that identifies a specific individual, unless it relates directly to the detection, prevention, or mitigation of a cybersecurity threat.

4. Upon receiving information known at the time of sharing to identify a specific individual or is of a specific individual that is not information directly related to a cybersecurity threat, securely dispose of or anonymize such information as soon as practicable.

5. Upon receiving information not related to cybersecurity, promptly notify the submitter or originator.

6. Update cybersecurity information repositories upon receiving a notice of information erroneously identified as cybersecurity information. Securely return, dispose of, or anonymize any such information.

7. Where appropriate, use tools such as the Traffic Light Protocol[4] or similar approaches to designate the sensitivity of cybersecurity information and govern its sharing within and among organizations.

8. Protect cybersecurity information from unauthorized access or acquisition.

9. Regularly review cybersecurity information to ensure it remains useful for cybersecurity purposes.

10. Regularly review the receipt, retention, dissemination, and use of cybersecurity information for consistency with these practices and associated organizational policies.

11. Consistent with organizational privacy policies, provide appropriate transparency about cybersecurity information sharing practices and potential partners, including notice that information that identifies a specific individual may be shared outside the organization for “cybersecurity purposes,” including with the government, which may result in the government’s use of the information for purposes authorized under CISA.

[4]See https://www.us-cert.gov/tlp