ISAO SP-4000

Guiding Practices to Advance Consumer Privacy in Cybersecurity Information Sharing

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

In September 2016, the Information Sharing and Analysis Organization Standards Organization published ISAO 300.1: Introduction to Information Sharing. Section 9, Information Privacy, included core and supporting principles for consideration by entities 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 the core and supporting principles by outlining actions to promote efficient and effective information sharing while minimizing the impact on privacy interests. 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), draws upon the U.S. Departments of Homeland Security and Justice Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities, and 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 could 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.

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

3. 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 before sharing cybersecurity information, unless it relates directly to the detection, prevention, or mitigation of a cybersecurity threat.

4. As soon practicable, securely dispose of, de-identify, or anonymize information that is known at the time of sharing to identify a specific individual

or is of a specific individual obtained through a cybersecurity program when such information is not directly related to a cybersecurity threat.

5. Promptly notify a submitter or originator of information shared for a cybersecurity purpose that is not cybersecurity information.

6. Update cybersecurity information repositories upon receipt of a notice of information erroneously identified as cybersecurity information and securely return, dispose of, de-identify, and/or anonymize any such information.

7. Use tools such as the Traffic Light Protocol or similar approaches to designate sensitive cybersecurity information and govern its sharing within and among organizations.

8. Apply to cybersecurity information appropriate protection 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.