Privacy

Draft Document—Request For Comment

SWG P 4—2016 v0.2

ISAO Standards Organization
Standards Working Group 4: Information privacy and Security
Rick Howard, Chair
David Turetsky, Co-Chair

May 2, 2016

Copyright © 2016, 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.

Table of Contents

EXECUTIVE SUMMARY

The main goal of any Information Sharing and Analysis Organization (ISAO) is to encourage the sharing of cybersecurity information and to assist entities so they can understand and manage the larger cyber threat ecosystem. ISAOs will engage in activities that include the receipt, retention, use, and dissemination of cyber threat indicators through a voluntary cybersecurity information sharing process. Basic privacy protections will be needed to limit the receipt, retention, use, and dissemination of cyber threat indicators that contain any personal information not directly related to a cybersecurity threat. This following addresses a sample of the type of privacy related issues and questions ISAO’s will need to consider and discuss with its respective membership.

INTRODUCTION

It is important for Information Sharing and Analysis Organizations (ISAOs) that receive, retain, use, and disseminate cyber threat indicators or other information through a voluntary cybersecurity information sharing process to be sensitive to and protective of privacy and civil liberties considerations. This includes the privacy and civil liberties of membership organizations, any individuals concerning whom data may be available or provided, and a full range of other constituencies, customers and individuals. To protect privacy and civil liberties while accomplishing the goals of an ISAO, it will be important to provide guidance to members, participants and ISAO staff on what may be shared and what should not, establish clear responsibilities in that regard, and establish workable and appropriate processes and procedures that provide a reasonable level of assurance regarding the protection of privacy and civil liberties. Before sharing cyber threat indicators or other permitted information, ISAOs should incorporate a review to assess whether information not directly related to cybersecurity threats or the purposes for which the information may be shared is included, whether information is included that the ISAO knows to be personal information about a specific individual or that identifies a specific individual, and the ISAO should make efforts to remove any such impermissible information.

Given the nature of a cyber threat indicator, oftentimes an individual whose personal information is directly related to a cybersecurity threat does not have the ability to consent, be involved in the process used to collect that information, or access or correct that information. But that is a reason to be sensitive and protective of privacy interests, not a reason to avoid sharing cyber threat indicators altogether. However, ISAOs must limit the impact of the data they collect on an individual’s privacy and civil liberties.

Sensitive information such as personally identifiable information (PII), intellectual property, and trade secrets may be encountered when handling cyber threat information. The improper disclosure of such information could cause a variety of harm. Accordingly, organizations should implement the necessary security and privacy controls and handling procedures to protect this information from unauthorized disclosure or modification.

Often —by regulation, law, or contractual obligation— data requires protection. This includes PII and other sensitive information afforded protection under the Sarbanes-Oxley Act, the Payment Card Industry Data Security Standard, the Health Information Portability and Accountability Act, the Federal Information Security Modernization Act of 2014, and the Gramm-Leach-Bliley Act, among others. It is important for ISAOs to identify and appropriately protect such information. ISAOs should consult legal, privacy, and data experts familiar with the various regulatory frameworks when developing procedures for identifying and protecting sensitive information.

As noted above, ISAOs should limit the receipt, retention, use, and dissemination of cyber threat indicators containing personal information about specific individuals or information that identifies specific individuals.

CORE PRINCIPLES

1. ISAO members must identify and contribute indicators that are critical to the threat and make efforts to minimize the PII shared with the ISAO or other members.
2. ISAO members must have clear methods to notify the ISAO if PII is mistakenly contributed.
3. ISAOs must develop responsibilities and operations that provide for the timely destruction or return of cyber threat indicators containing personal information about specific individuals or information that identifies specific individuals.

SUBSIDIARY PRINCIPLES

ISAOs should provide instructions to participants and member companies regarding what to share and what not to share from a privacy standpoint. ISAOs and their participants and member companies should familiarize themselves with applicable privacy law and policy and incorporate appropriate commitments and policy provisions into member rules, foundational documents, and user agreements.

The ISAO SO recommends designating a privacy officer who would ensure compliance with applicable state privacy laws.

Segmentation of sensitive personal information is important to ISAOs when developing cyber threat indicators. Segmentation should include a process for identifying certain data fields that could require some review, either always or by sampling (and the sampling could be by field, by item, a combination, or otherwise); a procedure for returning, deleting, or otherwise minimizing PII; and a way to counsel or advise members who frequently handle PII with less than the necessary care.

ISAOs should adopt and socialize the Department of Homeland Security (DHS) Automated Information Sharing (AIS) Terms of Use if they are sharing with government partners (available at: https://www.us-cert.gov/sites/default/files/ais_files/AIS_Terms_of_Use.pdf). ISAOs should pay particular attention to the following sections of the Terms of Use:

- Section 3.2 states that "An AIS Producer shall use reasonable efforts to ensure that any Indicator or Defensive measure shared is accurate at the time that it is supplied. Further, the AIS Producer will associate any Indicators or Defensive Measures it produces with the appropriate Information Handling Level as defined by the NCCIC [National Cybersecurity and Communications Integration Center]."

- Section 3.3 states that "Each AIS Producer will use reasonable efforts to remove from any Indicators or Defensive Measures provided to the NCCIC any information not directly related to a cybersecurity threat that the AIS Producer knows at the time of sharing to be personal information that identifies a specific individual."
- Section 3.4 states that "Each AIS Producer agrees that, in the event it discloses Indicators or Defensive Measures by mistake, in error, or without their appropriate Information Handling Level (through mismarking or a failure to mark), it shall promptly notify the NCCIC and take all reasonable steps to mitigate, including sending a versioning update, as soon as it is able."

ISAOs should understand what raises privacy concerns and educate participants.

Where relevant, ISAOs should follow international privacy law that may differ from U.S. state or federal law. For example, depending on their membership and circumstances, they should seek to understand what information if shared might trigger problems in Germany or elsewhere in the European Union, even if not with all or some U.S. states.

If an ISAO may share threat indicators or defensive measures with the NCCIC or other government partners, and particularly if it intends to secure the legal protections available under CISA, an ISAO must be familiar with the privacy guidance available from the DHS, DoJ and other agencies regarding sharing and should implement that guidance in connection with sharing with the federal government. That guidance is intended to help protect privacy and to provide a path to secure such legal protection for sharing as may be available under CISA.

But even if an ISAO does not intend to share with the federal government, the sharing of appropriate threat information by private parties or other non-federal entities also can raise privacy concerns and, if conducted correctly, with sensitivity to privacy concerns, will also secure liability protection under CISA. Thus, the DHS and DoJ "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," issued on February 16, 2016, ("Guidance to Non-Federal Entities") should be reviewed and considered by an ISAO for implementation, even if does not intend to share information with the federal government. https://www.us-cert.gov/sites/default/files/ais_files/Mom-Federal_Entity_Sharing_Guidance_(Sec%20105(a)).pdf

For example, pages 5 and 6 of the Guidance to Non-Federal Entities provides examples of information containing threat indicators that can be shared, including particular IP addresses in certain circumstances. Therein and from pages 7 and on there is an explanation and examples of what may constitute personal or other information that should not be shared. of health and other information that should be kept private and not be shared, and which also identifies impermissible uses of shared information.

Socialize the processes, procedures, plans, and exercises to make sure ISAO managers know what to do and respond appropriately if the ISAO receives PII.

ISAOs should evaluate the privacy section in the National Institute of Standards and Technology (NIST) framework and determine which of those recommended actions are relevant to their operations.

ISAOs should consider implementing safeguards at all states of PII's lifecycle within the organization and proportionate to the sensitivity of the PII to protect against loss, theft, unauthorized access or acquisition, disclosure, copying, use, or modification.

ISAOs should have processes and procedures to securely dispose of, de-identify, or anonymize PII that is no longer needed. They should regularly audit stored PII and the need for its retention.

ISAOs should develop technology or the ability to audit access to databases containing PII. They should consider whether PII is being logged as part of an independent audit function, and how such PII could be minimized while still implementing the cybersecurity activity effectively.

ISAOs should evaluate the DHS profile for the AIS portal, including any privacy requirements.

ISAOs should design a minimum information exchange mechanism to minimize information shared to only the data necessary to directly address the threats the ISAO is intending to cover.

ISAOs should encrypt all communications with a public key, with the ISAO's public key to be used for encryption, and the member's private keys to be used for signing. If members do not sign communications, include integrity checks in records.

ISAOs should include dates in the data exchange—report date, data expiration date— and control access to data inside the ISAO. They should respect the data expiration date and delete or anonymize the data after that date.

ISAOs should have a clear preventive plan for data protection, including both systems and human elements, and an equally clear remedial plan in the event of a breach. They should also test both periodically and record and adapt to the test outcomes.

ISAOs should formulate an encryption policy that meets the needs and expectations of employees, customers, and counterparts. They should decide the extent to which they will cooperate with law enforcement, absent an enforced subpoena or search warrant.

ISAOs should determine their core membership and audience and build in security and privacy requirements that match the maturity levels commensurate with their membership, recognizing that not all entities or participants receiving information have equal capabilities or equal privacy concerns.

ISAOs should tailor privacy and security controls to the capabilities of their members and the criticality of the information shared. This means, for example, that sharing threats via email or a phone call to specifically identified recipients may have less impact than disseminating information to members broadly through a portal. Therefore, depending upon the tools an ISAO is implementing, the security and privacy requirements will vary.

ISAOs should have clear policy and procedures for data retention and disposition.