Security

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

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 receiving, retaining, using, and disseminating cyber threat indicators through a voluntary cybersecurity information sharing process. Basic security measures will be needed appropriate for the size, complexity, or maturity of an ISAO. This draft document lays out the type of issues and questions ISAOs need to consider and discuss with their members.

BACKGROUND

ISAOs will vary in levels of need, sophistication, and abilities. No matter how mature or new an organization is at creating a cybersecurity information sharing program, basic security requirements will be needed to protect both the dissemination of the information and the information itself.

ISAOs need to discuss and set structures for basic security and privacy policies to protect the criticality of the information shared.

If members choose to share machine-to-machine in an automated fashion or to use email, fax, or phone, then security measures will need to provide matching security and privacy protections, and comply with all related state, local, federal, and international laws and regulations.

An ISAO's membership may also drive the levels of security needed. Whether the organization is for-profit or non-profit, or a large or small company, the security measures also need to match these needs accordingly.

The President recently signed into law the Cybersecurity Information Sharing Act (CISA), which defines procedures for private-sector entities sharing cyber threat indicators and defensive measures with the federal government. CISA also includes basic structures and security requirements that companies must meet to participate in the process with the Department of Homeland Security. It also defines strong privacy protections, which are also addressed in a companion document. Not all ISAOs will participate in the cyber threat indicator sharing program, for a variety of reasons, but it is important to include those requirements in this document for potential ISAOs to consider.

NOTE: The following list of issues is a draft for discussion. It is not intended to be comprehensive but to provide a foundation throughout the ISAO public commenting process. Specific issues—including core privacy issues, the type of information that could be shared, categories of information, and others—would be handled in companion groups in the SO process.

CORE SECURITY SUGGESTIONS FOR ISAOS

BASIC SECURITY COMPONENTS FOR AN ISAO

SECURE WEB PORTAL FOR COMMUNICATIONS

- ISAOs should consider and discuss with their members the levels of security needed to perform the basic functions the members decide they will need.
- ISAOs should also discuss and decide on the vehicle or platform that it may want to use to ensure the security of communications.

- ISAOs should also consider and discuss the level of security that individual members currently have, as it may impact their connectivity to, and the security of, the ISAO structure.

PUBLIC KEY INFRASTRUCTURE (PKI) AND "SECURITY BY DESIGN"

- ISAO members should discuss and decide the basic security design and functions needed to share and disseminate cyber threat information.
- Members should consider incorporating encrypted communications and other basic security measures to be imbedded up front in the design structure.
- An example of such a measure would be: All members will use certificates for signing and authenticating emails in a PKI exchange mechanism. All documents being shared would be encrypted separately from the PKI.

ACCESS CONTROLS

- ISAOs should discuss and decide how to manage access controls for individuals within member entities. Specific criteria should be used to determine levels of access for individuals and members.
- Access controls should be evaluated and individual access removed immediately when individuals leave their respective ISAO member companies, to ensure that no unauthorized access exists. Consider establishing new credentials for replacement individuals that members companies appoint.
- Data should also be federated based upon their criticality, and access controls may vary for different types of data.

CYBERSECURITY ATTACK AND DATA BREACH NOTIFICATION

To maintain a level of trust and dependability between and among members, ISAOs should consider establishing internal reporting plans and communication lines between companies in the event of a cybersecurity attack that may impact the ISAO and its members.

DATA CLASSIFICATION, DISTRIBUTION, AND LABELING

In order for ISAOs to provide security for whatever levels and sophistication of information sharing the members decide, it is important for the ISAOs and their members to consider setting up structures that communicate what that will mean. This could include the following steps:

- Consider the use of best practices like Traffic Light Protocol (TLP) Red/Amber/Green, which can help members understand how to handle information according to data classification standards.
- Discuss and consider establishing internal structures in which commercial entities would not share proprietary information.

- Discuss and consider how ISAO member groups should be structured according to the levels of information classification or sensitivity they can or cannot share or accept, and so on.
- Discuss and consider issues for anonymizing member submissions, as well as establishing parameters for sharing when they want to use anonymization.
- Discuss and consider having clear data retention and disposition policy and procedures. (NOTE: The current DHS AIS program has established data retention policies that are more specific.)
- Discuss and consider a variety of options for sharing information that may include automated intake and dissemination, email, and other methods.

As an example, it would be helpful to consider distribution policies to set up rules for sharing data via email. Policies could cover matters like having a blind copy for all transmissions, deciding who will receive the information, and discussing how to use “reply all” structures.

ISAO MEMBER SECURITY

It is also important to discuss individual member cybersecurity for the sake of the security of the broader ISAO ecosystem.

- ISAOs should discuss and consider using structures like the National Institute of Standards and Technology (NIST) Cybersecurity Framework, which provides a compendium of security standards as a core reference guide.
- If ISAO members already have certain sector, regulatory, or other cybersecurity and information security-related requirements, those should remain in place.
- ISAOs should consider establishing training programs for members on security awareness, as well as for any ISAO internal staff or governing structure.

GLOBAL SECURITY ISSUES

If ISAOs include global corporations, it is important for the ISAO to be aware of and discuss other existing requirements for companies involving information security, cybersecurity, privacy, and overall information sharing.

- If there are cross-border data transfers for information sharing, ISAOs should become familiar with any governing international requirements.

  For example, the United States is in the process of working with the European Union (EU) on Privacy Shield, which includes information security, privacy, and other requirements. Other EU requirements that are important to be aware of include the EU General Data Protection Regulation (GDPR) and the EU Network and Information Security (NIS) Directive.

- ISAOs should be aware of and integrate other regulatory requirements as needed for other countries around the world. In some instances these requirements extend to vendors and third parties, so ISAOs will need to be aware of and comply with these requirements.