ISAO Standards Organization

ISAO 300-1:
Introduction to Information Sharing

v1.01

October 14, 2016

ISAO 300-1

Introduction to Information Sharing

v1.01
ISAO Standards Organization
October 14, 2016

Acknowledgements

This publication was developed by the Information Sharing and Analysis Organization Standards Organization (ISAO SO) with representatives from industry, government, 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

Brian Engle
Executive Director
Retail Cyber Intelligence Sharing Center

Working Group One—ISAO Creation

Frank Grimmelmann
President & CEO
Arizona Cyber Threat Response Alliance (ACTRA)

Deborah Kobza
President & CEO
Global Institute for Cybersecurity & Research

Working Group Two—ISAO Services and Capabilities

Denise Anderson
President
National Health Information Sharing & Analysis Center
Chair, National Council of ISACs (NCI)

Fred Hintermister
Manager
Electricity Information Sharing and Analysis Center
North American Reliability Corporation
Vice Chair, National Council of ISACs (NCI)

Working Group Three—Information Sharing

Kent Landfield
Director, Standards and Technology Policy
Intel Corporation

Michael Darling
Director, Cybersecurity and Privacy
PwC

Working Group Four—Privacy and Security

Rick Howard
Chief Security Officer
Palo Alto Networks

David Turetsky
Partner
Akin Gump Strauss Hauer & Feld LLP

The ISAO SO leadership and authors of this document would also like to acknowledge those individuals who contributed significantly to the development of this publication, including:

Kevin Albano of IBM, Scott Algeier of IT-ISAC, Carl Anderson of HITRUST, Jon Baker of The MITRE Corporation, Allison Bender of Hogan Lovells, Chris Boyer of AT&T, Adam Buteux of PWC, Roger Callahan of FS-ISAC, Timothy Casey of Intel Corporation, Dan Cashman of FairPoint Communications, Christy Coffey of ThreatConnect, David Eilken of Soltra, Roxanne Everetts of National Defense University, Paul Geraci of OSIsoft, Stuart Gerson of Epstein, Becker & Green, LLP, Steve Hitch of NTTSecurity, Adam Isles of Chertoff Group, LLC, John Johnston of Axiall Corporation, Klara Jordan of FireEye, Akilah Kamaria of Blue Fields Digital, Norma Krayem Holland and Knight LLP, Terry Leach of Astrolytes, Tom Litchford of the National Retail Federation, Alelie Llapitan of Solutionize, Chris Needs of NC4, Betsi McGrath of The MITRE Corporation, Kim Milford of Research and Education Networking Information Sharing and Analysis Center, Bruce Parkman of The Macalan Group, Bobbie Stempfley of The MITRE Corporation, Roy Stephan of PierceMatrix, Megan Stifel of Silicon Harbor Consultants, LLC, Nick Sturgeon of the Indiana Information Sharing and Analysis Center, Shawn Talmadge of Commonwealth of Virginia, Jay Taylor of Schneider Electric, Michael Thibodeaux of BASF SE, Matt Tooley of the National Cable & Telecommunication Association, Michael Vermilye of Johns Hopkins University Applied Physics Laboratory, Joseph Viens of Charter Communications, Jesse Ward of NTCA-The Rural Broadband Association, Douglas T. White of C5T, John Woodso of Baker & McKenzie, LLP, and Brandon Workentin of EnergySec,

Special thanks from the authors goes to the ISAO SO advisors and staff who helped greatly along the way in the development of this document: Chris Rutherford, Daniel Knight, Larry Sjelin and James Navarro.

Revision Updates

Item	Version	Description	Date
1	1.0	Initial Publication	September 30, 2016
2	1.01	Editorial Update/Corrections	October 14, 2016

Table of Contents

Figures

Tables

1 EXECUTIVE SUMMARY

The purpose of this document is to provide an introduction to cybersecurity information sharing. The intent is to provide a foundation for those trying to understand the basics of information sharing as it relates to Information Sharing and Analysis Organizations (ISAOs). This document describes a conceptual framework for information sharing, information sharing concepts, the types of cybersecurity information an organization may want to share, ways an organization can facilitate information sharing, as well as privacy and security concerns to be considered.

Information sharing is intended to help those managing and operationally mitigating cybersecurity risks. The nature of cybersecurity has and will continue to evolve over time. Information sharing efforts should also evolve to keep pace with changes in the cybersecurity landscape. This document provides the reader with basic information on topics and capabilities involved in cybersecurity information sharing. Additionally, it offers elements of a cybersecurity information sharing program for those considering forming a new ISAO as well as for existing ISAOs that are reviewing how to further align with their member needs.

Throughout the document, the terms *cybersecurity information sharing, cyber threat sharing, and information sharing* are used interchangeably.

2 INTRODUCTION

Organizations addressing cybersecurity risks can find value by participating in what has generally been characterized as *information sharing*. A benefit of information sharing is the opportunity to leverage knowledge, awareness, understanding and experiences across a broader community.

Participation in information sharing efforts is primarily driven by interest in improving cybersecurity, either personal, organizational, or both. Those responsible for managing cybersecurity risks and taking actions to deal with them may wish to participate in ad hoc, defined, or institutionalized information sharing activities to better understand the environment in which they are operating and to contribute to collective interests.

Information sharing does not solve all cybersecurity challenges an organization faces but can prepare an organization to better understand the threat environment affecting it and others. Learning from others' experiences and understanding what others have found to be effective cybersecurity measures can be an additional benefit as organizations build situational awareness, make decisions, take actions and allocate resources in similar situations.

This document is structured to provide an introduction to information sharing with respect to cybersecurity. It can help those thinking of joining an existing ISAO, starting a new organization or evaluating their current ISAO membership.

While there are many challenges ISAOs will face, providing good 'value' to participants is essential to success. The *Introduction to Information Sharing* is structured to provide ISAOs with outcomes to be considered when selecting and implementing information sharing and collaboration efforts. In addition to presenting a conceptual framework and information uses, this document presents a set of functional components depicting possible ISAO cybersecurity information sharing activities. It provides items to consider for evolving an ISAO's cybersecurity information sharing capabilities. Not all new ISAOs may be capable of or desire to fully achieve what is depicted in this document. The following material is conceptual as opposed to prescriptive and inclusion of considerations is meant to illustrate options rather than mandate them.

3 INFORMATION SHARING CONCEPTS

Companies, enterprises and organizations manage cyber-related risks based on the technology they employ, how the business and customers use that technology, and their interactions with others. Managing these risks entails understanding their own internal environment and the environment in which they are operating (situational awareness), determining directions to pursue (decision-making), and detailing efforts (actions) to undertake. These are activities an organization executes daily.

An ISAO can provide a variety of information to its members in order to help them manage their cyber-related risk. This information can be logically grouped into two dimensions: **Purpose**, & **Time and Application** of resources.

Purpose covers three areas, namely;

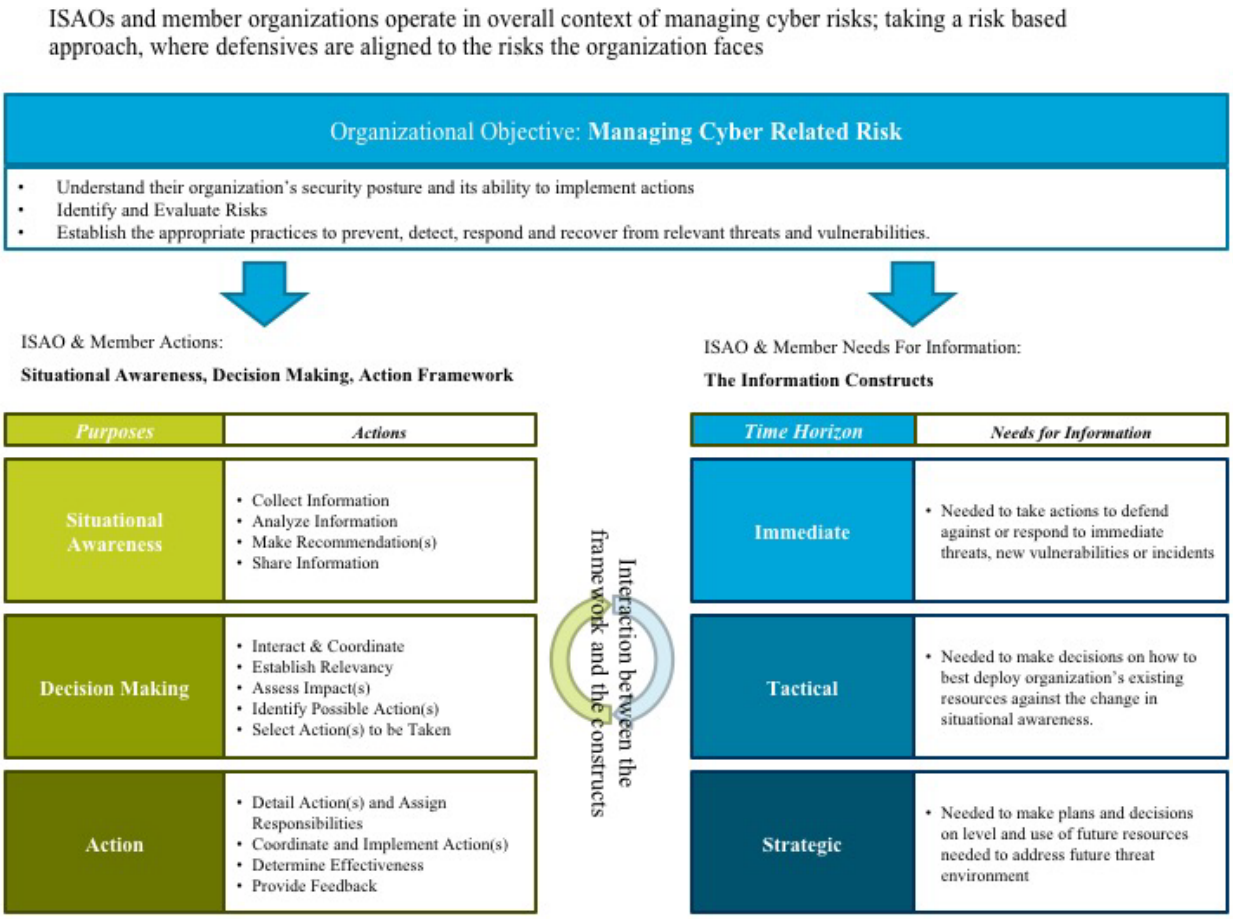
- ***Situational Awareness***—information providing an awareness of the broader threat landscape.
- ***Decision Making***—information relevant to a particular organization's needs and enabling more effective security management.
- ***Action***—information directly supporting the implementation of a particular measure to improve security.

Time and Application of resources begins with information operationally relevant to security and builds upon it. This dimension covers three areas:

- ***Immediate***—information relating to actions to defend against or respond to new threats, vulnerabilities, or incidents.
- ***Tactical***—information relating to decisions on how to best deploy an organization's existing resources against the change in the threat environment.
- ***Strategic***—information relating to making plans and decisions on efforts and resources needed to address emerging or future threat environments.

Figure 1 depicts an information construct and a framework for interacting to align the ISAO and member efforts with the information intended to help organizations manage cyber-related risks.

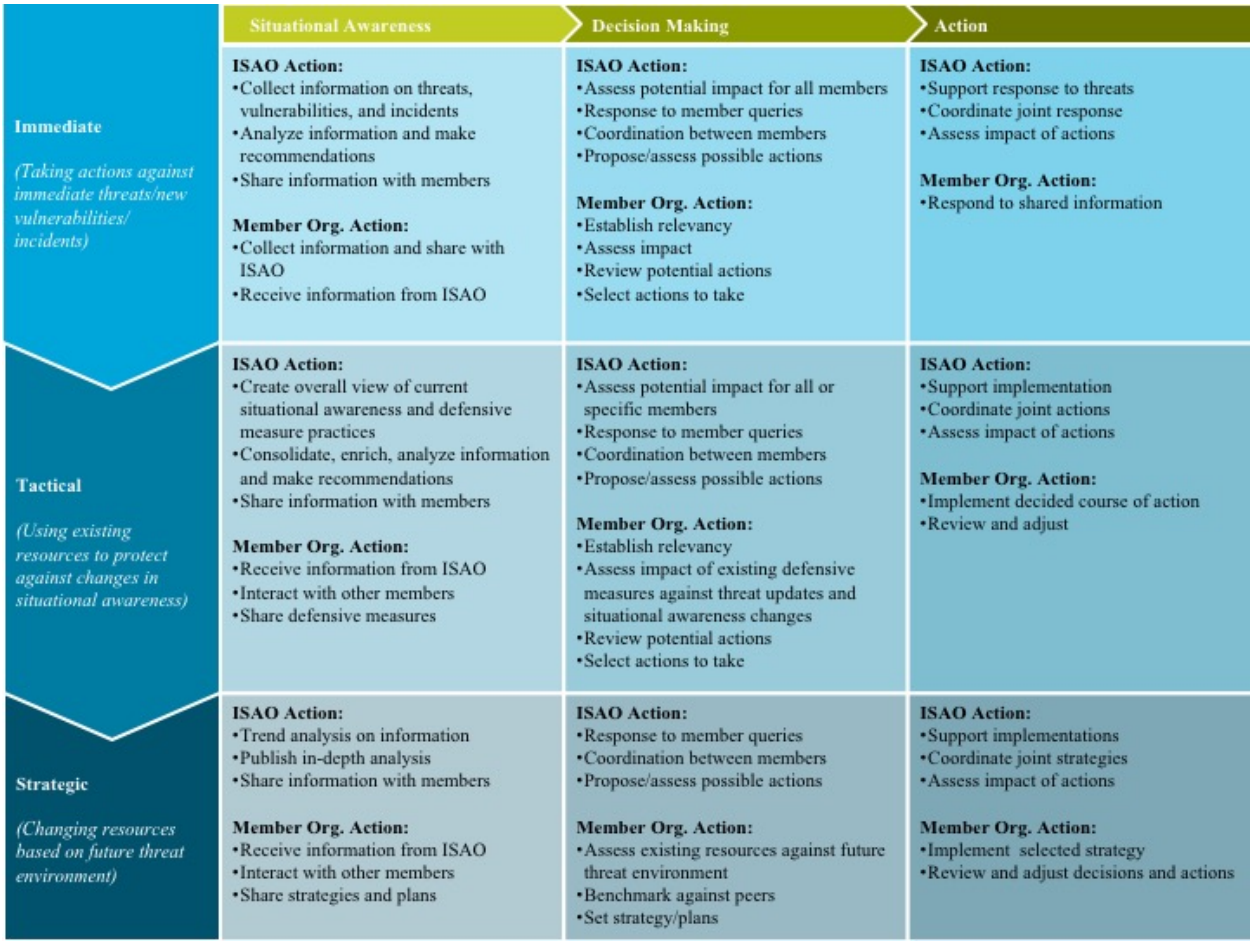
Figure 1. Context for Information Sharing



3.1 INFORMATION SHARING FRAMEWORK

Using the two dimensions previously discussed, the Conceptual Information Sharing Framework depicted in Figure 2 presents a context for the various high-level interactions to consider as an ISAO develops its information sharing objectives. The interactions depict both the conceptual activities of the ISAO and the activities of its members.

Figure 2. Conceptual Information Sharing Framework



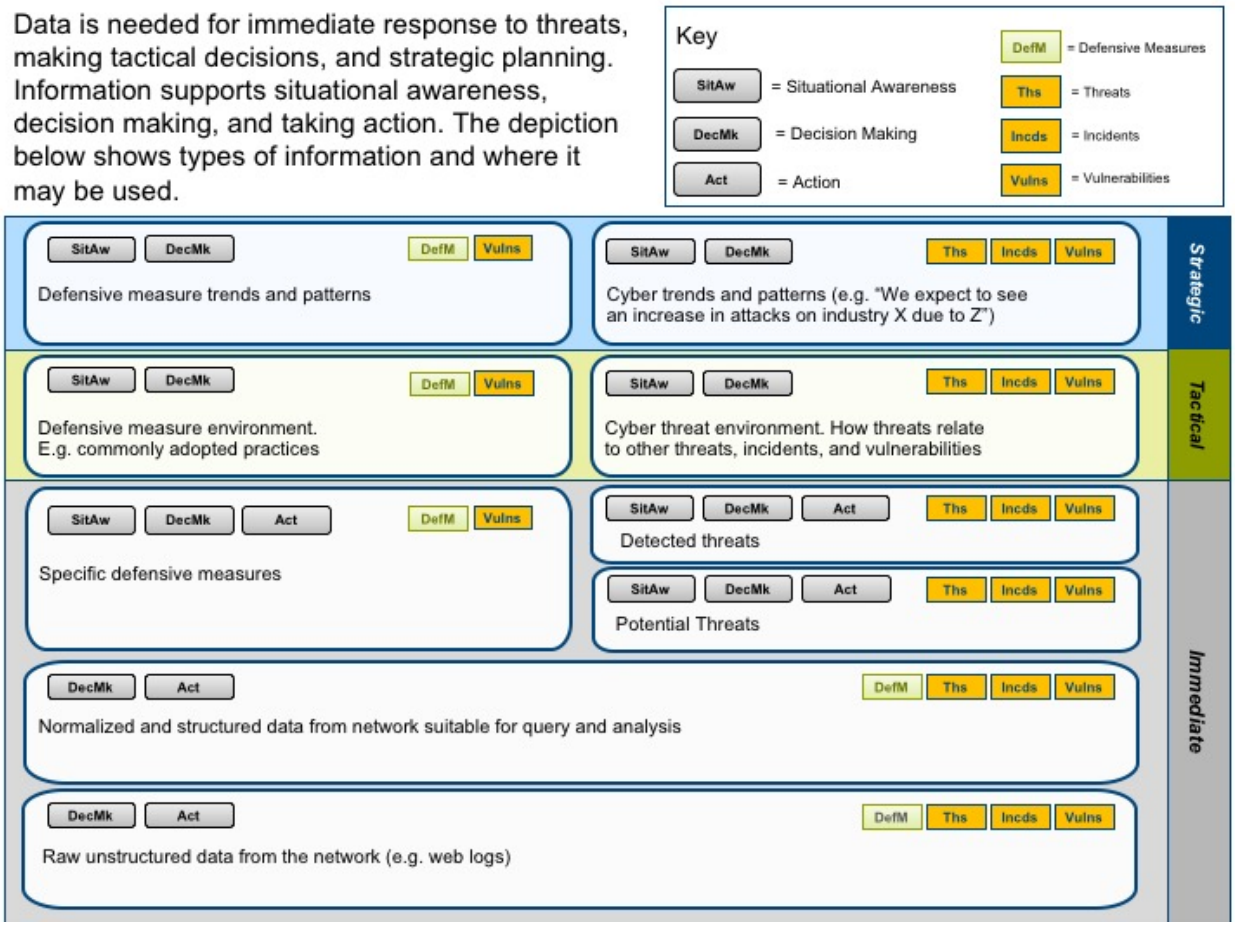
The context and conceptual framework depictions illustrate the benefits an ISAO can provide members by meeting their member information needs through information sharing efforts in the context of what organizations are doing on a daily basis to manage their cyber-related risks.

3.2 APPLYING SHARED INFORMATION

Figure 3 depicts, at a high level, how specific types of information--namely, threats, vulnerabilities and incidents--can be applied to affect situational awareness, decision-making, and actions focused on managing and mitigating cyber-related risks.

Further, progressive levels of analysis can turn raw, unstructured data into valuable knowledge and additional information from the operating environment. Armed with this knowledge and information, organizations can then prioritize efforts to defend against or respond to the most prevalent threats.

Figure 3. Applying Information to Cybersecurity Risks



3.3 FUNCTIONAL COMPONENT DESCRIPTIONS

Another way of describing the types of information an ISAO may consider sharing is to categorize the broad functions the ISAO provides its members. These functional categories can be broken down into components and aligned with supporting capabilities needed to support them.

In Table 1, these cross-cutting categories are decomposed into sub-categories to identify the more specific information capabilities needed to support those categories.

Personal or organizational interests of the members participating in an ISAO generally value the following:

- New knowledge for a better understanding of the threat and vulnerability environment in which they are operating
- Recommendations for dealing with specific threats and vulnerabilities
- Receipt of situational alerts that may affect their security posture

- Validation of their understanding of a current situation or incident
- Additional information which may improve their current understanding of threats, vulnerabilities, and/or incidents
- Knowledge of the actions being taken by others
- Coordination of collective actions
- Feedback on the effectiveness of actions being taken by others individually or collectively

These personal or organizational interests can be used to describe four functional component categories that together make up the broad tactical and strategic efforts an ISAO can perform:

- Threat landscape awareness
- Response measures
- Coordination
- Trend and pattern analysis

These broad categories, as shown below, can be further decomposed to more specific functional elements and information sharing capabilities to support the personal or organizational interests of those participating in or working with an ISAO.

Table 1 describes these categories and sub-categories and identifies information sharing capabilities supporting them.

Table 1. Functional Categories and Information Sharing Capabilities

Functional Category or Sub-category	Description	Information Sharing Capability
Threat landscape awareness	Know what's going on related to cybersecurity or other issues of interest to the ISAO	
◆ Collect information: — General	◆ Obtain threat, vulnerability, and incident information from ISAO participants and other sources for information of interest	◆ Anonymous and attributable submissions ◆ Email and Listserve ◆ Calls ◆ Meetings ◆ Secure portal submissions ◆ Automation feeds ◆ Direct cybersecurity partner feeds ◆ Traffic Light Protocol (TLP) labelling implementation
◆ Focus on community of interest	◆ As necessary, encourage community of interest participation to build deeper trust relationships	◆ Similar capabilities as above that can be segregated and tailored for community of interest participants

Functional Category or Sub-category	Description	Information Sharing Capability
— Make appropriate information available	◆ Distribute or make information available in accordance with TLP procedures and labelling	◆ Distribution through appropriate communication channels (portal access, email, automation platforms, etc.)
— Analyze collected information	◆ Review, de-conflict, validate, sanitize, and analyze collected information ◆ Conduct research or intelligence to alert the members of evolving or existing threats, incidents, and vulnerabilities	◆ Analysts and analysts' tools
— Develop alerts	◆ Identify changes in situational awareness that may be of interest to ISAO participants and others	◆ Communication mechanisms for levels of alert criticality ◆ Multiple mechanisms for highest level of alerts
Response measures	Establish operational or procedural measures to mitigate the utility or deny the effectiveness of vulnerabilities or exploits to infrastructure, operations, or systems	
◆ Distribute alerts and rapid notification	◆ Provide developed alerts and notifications to appropriate participants or partners	◆ Communication mechanisms for levels of alert criticality ◆ Multiple and diverse mechanisms for highest level of alerts
◆ Develop countermeasures: — Immediate — Long-term	◆ Develop, in collaboration with participants and partners, countermeasures to mitigate the risks of new threats or vulnerabilities ◆ Focus on immediate and then longer term measures	◆ Conferencing and networking collaboration mechanisms for both technical experts and participants ◆ Access to capabilities that provide searchable topic analysis for participants
◆ Identify "best" and "good" practice recommendations	◆ Based on interests of participants, make recommendations for "best" and "good" practices to mitigate and respond to cybersecurity and other relevant risks and incidents	◆ Conferencing, networking, and forums for collaboration among technical experts and participants ◆ Surveying capabilities ◆ Publishing and providing references and a repository for availability of recommendations to participants ◆ Access to capabilities that provide searchable topic analysis for participants
◆ Determine effectiveness	◆ Develop metrics and perform surveys to continually measure the effectiveness and satisfaction of participants with the services being provided	◆ Participant survey capabilities
Coordination	Synchronize and integrate activities to ensure the pursuit of the shared objectives established by the ISAO.	
◆ Establish coordination processes and capabilities	◆ Policy and procedures established for assessing the need for coordination among members with shared interests to discuss and coordinate	◆ Communication/network mechanism for a leadership group (identified sub-group) to make a decision to activate coordination

Functional Category or Sub-category	Description	Information Sharing Capability
◆ Activate coordination	◆ Issue notification for an "emergency" call for coordination	◆ Established diverse communication capability to initiate an "Emergency Call"
◆ Establish coordination actions and efforts	◆ Establish "playbooks" for various situations where coordination among participants is required	◆ For ongoing incidents of specified severity implement conferencing capabilities to determine the status, countermeasures, and response information related to an ongoing situation
◆ Assess coordination efforts	◆ During and following coordination events continually assess decisions and actions taken	◆ Survey capabilities. ◆ Conferencing capabilities
Trend and Pattern Analysis	Collect information and attempt to spot a pattern or trend derived from the information of interest to the ISAO participants	
◆ Retain historical information	◆ Maintain history of submissions, analysis and decisions in a secure database	◆ Secure operational database and software with appropriate access controls to segregate and deal with varied sensitivity of information
◆ Perform strategic analysis: — Identify trends, discontinuities, or patterns of activity — Determine threat actors and motivations	◆ Analyze the ISAO historical information along with other information to provide value-added insights on trends and new activity of significance to participants' interests	◆ Analysts and analysts' tools ◆ External collaboration mechanisms for analysts to engage other experts
◆ Publish analysis and recommendations	◆ Regularly communicate with ISAO participants and others based on ISAO policy and procedures	◆ Communication channels and networking events for members to receive analysis ◆ Access to capabilities that provide searchable topic analysis for participants

3.4 ESTABLISHING INFORMATION SHARING GOALS

ISAOs are established with their own specific mission and vision. Creating focused information sharing goals enables that mission and vision. This focus also plays an important role in determining what information to share, how to share that information, and the management of member and ISAO expectations.

In many cases, the ISAO itself is formed by a community of like-minded organizations that have made the decision to collaborate with peers or others as a means of managing risk. An ISAO should be designed by its initial members to meet the needs of its membership. With the understanding that information sharing is a means to an end, an ISAO should clearly articulate the information sharing goals it is seeking to achieve.

In defining these goals, there are a variety of questions an emerging ISAO and its potential members need to answer in order to determine its information sharing objectives. These questions can also be used during the evaluation of an existing ISAO.

The following are some questions the ISAO may wish to consider: [1]

- How will the information shared help members achieve their cybersecurity objectives?
- Which types of information does the ISAO membership want that conveys relevant situational awareness?
- Will the ISAO provide raw data, analysis, or both to assist members in their tactical decision-making efforts?
- Will members expect recommendations, related to action, including defensive measures, best practices, and/or procedures for incident coordination?
- Will the ISAO provide analysis of a strategic nature, including related to things such as trends, threat actor targeting and threat actor motivations?
- How will information sharing, mitigation, and analytic plans of the ISAO relate to each other?
- How will information sharing and trust be cultivated between the ISAO and its members?
- How will the ISAO information sharing policy guide expectations and obligations?
- Are there specific types of information the ISAO members want to share with each other?
- What information do ISAO members need to assist them in tactical decision making?
- What information sharing capabilities are achievable and sustainable within the resources of the ISAO?
- Could an existing ISAO fulfill the information needs being considered?

When organizations come together to create an ISAO, they start with an understanding of their initial information needs even though they may have an incomplete understanding of their future needs. Therefore, the ISAO needs to clearly identify its objectives and develop supporting information sharing policies to achieve those objectives. For example, if a community forming an ISAO would like more information on effective practices to mitigate specific attacks, the ISAO would want to build policies facilitating this objective.

[1] Consult ISAO 100-2, *Guidelines for Establishing an ISAO*.

Individual members or organizations participating in an ISAO have a responsibility to address their own needs as well as responsibility to the ISAO community they are participating in. When developing information sharing policies, ISAOs should align their policies with the member objectives and customer needs.

4 INFORMATION AN ISAO MAY WANT TO SHARE

ISAOs and their members may wish to share information across ISAOs, with other ISAO members, and with various government entities. Using consistent standardized terminology, frameworks and data formats helps facilitate these cross-organizational information exchanges. Additionally, leveraging a consistent framework enables integration and analysis of threat information from disparate sources that may have different focuses, such as integrating indicator information with threat actor or incident information.

4.1 KEY FACTORS

There are several key factors to consider when evaluating the types of cybersecurity information an ISAO may want to share. In addition, there are various ways to share information, including network-to-network, machine-to-machine, human-to-human, or human-to-machine. Machine-to-machine sharing requires structured information and should use standardized data formats and protocols to enable interoperability. Human-to-human sharing can be most effective when using a common framework for describing cybersecurity information. This helps to facilitate a shared understanding among members, but the information may naturally be less structured than what is required for machine-to-machine sharing.

The Structured Threat Information eXpression (STIX)[2] language is used below to describe the types of information an ISAO may want to share. STIX terminology provides the depiction needed to convey core cyber threat concepts foundational to cybersecurity information sharing.

For automation-based exchanges to work effectively, established technical standards need to be used. There are various exchange languages used for automating the exchange of structured cybersecurity threat information. Efforts through the years have tried to settle on a single format for sharing cyber threat intelligence. Most, however, were focused within a specific area, such as incident response. The Incident Object Description Exchange Format[3] is one example of a focused approach.

The STIX language is commonly used for capturing and sharing cyber threat information. STIX is a structured, machine-readable format designed specifically to convey cyber threat information, addressing the complete cyber threat. STIX defines a framework for expressing and sharing cyber threat information in a consistent manner. This framework consists of a set of core attributes that include:

[2]See https://stixproject.github.io/data-model/

[3]See https://www.ietf.org/rfc/rfc5070.txt

threat actors, campaigns, incidents, indicators, courses of actions, observables, and exploit targets, and tactics, techniques and procedures (TTPs), as well as the set of relationships among those core attributes. The STIX framework is broad enough to support the full scope of cyber threat intelligence use cases and flexible enough to allow users or communities to define the subset of the STIX language they need for their specific use cases. STIX enables users to define profiles[4] for specific cyber threat sharing needs. These profiles document which subset of the STIX language will be used during sharing. When using STIX, it may be helpful for ISAOs to develop or leverage well-known STIX profiles to document the specific data elements to be exchanged in a given scenario. STIX is in use by threat intelligence teams from government and industry, security product and service vendors, Information Sharing and Analysis Centers (ISACs), and major Computer Emergency Response Teams (CERTs).

The following sections describe commonly shared cyber threat information an ISAO may wish to share. When applicable, these sections have been aligned with the terminology and definitions used in STIX to capitalize on that work.

4.2 INDICATORS

Indicators convey specific patterns combined with contextual information intended to represent artifacts and/or behaviors of interest within a cybersecurity context and are used for detecting activity of interest. Indicators are widely shared today, with examples ranging from malicious file hashes to command and control IP addresses, phishing e-mails, and other types.

Effective indicator sharing includes contextual information to allow downstream consumers to determine whether an indicator is relevant to their organization, how to handle the indicator, what TTP is indicated, the valid time window of the indicator, and related incidents, threat actors, and campaigns.

The following fields are commonly shared:

- Title
- Description
- Pattern—the machine readable pattern
- Confidence—the level of confidence in the indicator
- Indicated TTP
- Valid time position—the time window for which the indicator is valid

Indicator sharing is more efficient via machine-to-machine information exchanges. One example of automated indicator sharing is the Department of Homeland Security (DHS)–operated Automated Indicator Sharing (AIS) initiative

[4]See https://stixproject.github.io/documentation/profiles/

to enable cyber threat sharing among the federal government departments and agencies and the private sector.[5] This initiative uses STIX and Trusted Automated eXchange of Indicator Information (TAXII)[6] for the automated exchange of cyber threat information. TAXII defines a standardized set of services to enable the exchange. AIS has defined a profile of the STIX language for indicator exchange. The AIS STIX profile describes the specific data elements of the STIX language used for AIS cyber threat sharing. The profile provides a useful starting point for basic cyber threat indicator sharing–whether automated or manual–and can be easily leveraged to establish a consistent approach to sharing indicators within and among ISAOs.

Indicators are often generated through malware analysis, incident response, and endpoint and network monitoring. As such, indicator information frequently comes from a variety of sources including ISACs, CERTs, security product and service vendors, organization-specific security teams, and open source reporting. These various sources of indicator information drive the need to convey contextual information along with the shared indicators. A common challenge to indicator sharing today is simply determining which indicators are relevant and useful in discovering intrusions into the environment.

Indicator reports may also include indicator sighting information. This reports a given indicator matched or was seen within some sector or even a specific organization. In aggregate this sighting information can assist in understanding the prevalence of specific campaigns or threat actors, targeting information, and more. This aggregate sighting information is widely seen as a low-cost and low-risk method of supporting more sophisticated cyber threat intelligence analysis.

4.3 VULNERABILITY INFORMATION

Vulnerability information may include details about the vulnerabilities in specific systems or infrastructure, specific application vulnerabilities, or general classes of vulnerabilities.

The following fields are commonly shared:

- Title
- Description
- Vulnerability ID—a reference to a Common Vulnerabilities and Exposures (CVE)[7] threat or other well-known identifier
- Score—a Common Vulnerability Scoring System (CVSS)[8] rating or similar score for the referenced vulnerability

[5]See https://www.us-cert.gov/ais
[6]See https://taxiiproject.github.io/about/
[7]See https://cve.mitre.org/
[8]See https://www.first.org/cvss

- Affected software.

Mature software vendors routinely publish vulnerability information related to their products and services. Many governments issue vulnerability reports or security advisories to raise awareness as well. The US-CERT alerts[9] are one example of these government advisories.

Shared vulnerability information frequently informs immediate response actions, especially when the information is related to recently discovered high-severity vulnerabilities in exposed systems. Vulnerability trends and more general classes of vulnerability information regularly inform tactical and strategic situational awareness and decision making.

4.4 COURSES OF ACTION

Courses of action are specific measures to mitigate a threat or respond to an incident. They may be relatively targeted, such as blocking a specific IP address, or may encompass enterprise practices, such as using application whitelisting. As such, sharing courses of action can span the full range of immediate, tactical, and strategic information to impact decision making and actions.

The following fields are commonly shared:

- Title
- Description
- Type—Training, monitoring, patching, blocking, etc.
- Objective
- Impact
- Cost
- Efficacy
- Course of action—firewall or intrusion detection system rule, specific configuration change, etc.

Sharing courses of action can enable automated actions to mitigate threats as well as enable organizations to collaborate and arrive at the overall best course of action given a variety of options.

4.5 INCIDENTS

Incident information is specific information related to or discovered while investigating or responding to a cybersecurity incident. The amount and level of detail

[9]See https://www.us-cert.gov/ncas/alerts

included in shared incident information varies widely depending upon the intended use of the shared information and sensitivities related to financial, reputational, or other concerns.

The following fields are commonly shared:

- Title
- Description
- Category—improper usage, scanning or probing, denial of service, etc.
- Reporter—the reporting source of the incident description
- Victim—details about the victim of the incident
- Affected assets—describes the assets that were affected during the incident
- Impact assessment—describes the impact of the incident
- Related indicators—IP addresses, file hashes, domains, etc.
- Leveraged TTPs—attack techniques, malware, tools, etc.
- Attributed threat actors
- Intended effect—theft, disruption, account take over, fraud, etc.
- Related incidents
- Courses of action

The U.S. government publishes well-known guides for reporting incident information and incident handling, such as the following:

- *The Federal Incident Notification Guidelines* document provides guidance for submitting incident notifications to the United States Computer Emergency Readiness Team (US-CERT).[10]
- The National Institute of Standards and Technology (NIST) published *Special Publication 800-61, Computer Security Incident Handling Guide*, a useful resource on incident handling.[11]

These are excellent references for the type of information commonly shared to support incident response and analysis.

Sharing incident information can enable or support a wide variety of use cases, each with different incident information requirements. Incident information sharing can enable large scale analysis to uncover adversary trending across the cybersecurity ecosystem. Detailed incident information sharing may enable advanced cyber threat intelligence analysis related to specific threat actors and

[10]See https://www.us-cert.gov/incident-notification-guidelines

[11]See http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

campaigns. Incident information sharing can also help uncover key indicators of malicious activity to inform partner cyber defenses.

One well-known example of large scale incident analysis enabled by the sharing of detailed incident information is Verizon's Data Breach Investigations Report (DBIR)[12]. The incident data collected to form the Verizon DBIR are structured using the Vocabulary for Event Recording and Incident Sharing (VERIS) framework. VERIS includes a schema for a number of aspects of cyber threat activity, including detailed categorizations for threat actors, actions, assets and other incident attributes. The Verizon DBIR is the result of analyzing a large collection of incident information contributed by a variety of organizations. This report is oriented toward providing strategic and tactical value to inform situational awareness and decision making.

4.6 THREAT ACTORS

Threat actor information describes malicious actors that may represent a cyber threat or have been historically observed or related to known incidents.

The following fields are commonly shared:

- Names—short names or aliases used for the threat actor
- Description—a textual description of the threat actor
- Identity—Information that may identify the actor
- Type—hacker, hacktivist, state actor, electronic crime actor, insider threat, etc.
- Motivation—political, economic or financial, ideological, military, etc.
- Sophistication—novice, practitioner, expert, innovator, etc.
- Intended effects—military, economic, or political advantage, theft, destruction, disruption, etc.
- Observed TTPs—TTPs an actor has been observed to use
- Related campaigns—campaigns that have been attributed to the actor

Tracking and sharing threat actor information is critical for cyber threat intelligence analysis. This information allows organizations to develop an understanding of the threats they face as well as the specific objectives and capabilities an adversary or group is believed to have employed. Sharing threat actor information among organizations can help all participants develop a much more comprehensive understanding of these threats.

Threat actor information often comes from government or industry cyber threat intelligence sources. More established sharing organizations including ISACs

[12]See http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

may operate their own cyber threat analysis teams and track threat actors relevant to managing their cybersecurity risk or risk to their members.

Threat actor information is frequently more strategic in nature and used to inform situational awareness and decision making.

4.7 TACTICS, TECHNIQUES, AND PROCEDURES

Tactics, techniques and procedures represent a fairly broad set of information used to describe the behavior or capabilities of a threat actor or campaign. TTPs characterize what adversaries do and how they do it. As such, TTPs encompass specific adversary behaviors, the resources leveraged, target victim information, and the vulnerabilities or weaknesses being targeted.

The following fields are commonly shared:

- Title
- Description
- Intended effect
- Behavior—specific attack patterns, malware, or exploits
- Resources—tools, infrastructure, or personas
- Victim targeting—people, organizations, information or access being targeted
- Kill chain phase
- Related TTPs

Malware samples represent one commonly shared type of TTP. Sharing malware samples can enable broad distributed analysis of the sample as well as higher-level trending of both malware and the types of organizations being targeted.

TTPs are a critical component to cyber threat intelligence analysis and they are frequently related or shared in the context of incidents to describe the TTPs detected during an incident investigation. Cyber threat indicators relate low-level observables to TTPs to give context to what defenders should look for. Campaigns and threat actors are often related to TTPs to characterize either previously observed or expected adversary capabilities.

Aggregated TTP information can enable cyber threat analysts to develop a more holistic understanding of the threat or more narrowly advance the understanding of a specific adversary. This information may inform strategic, tactical, and immediate situational awareness, decision making, and actions.

4.8 CAMPAIGNS

Campaign information can relate information about the intended effects of an adversary or group with the tools they employ, the threat actors believed to participate, the incidents associated with the group, and other related campaigns.

The following fields are commonly shared:

- Names—short names or aliases used for the campaign
- Description
- Intended effects—Military, economic, or political advantage, theft, destruction, disruption, etc.
- Related TTPs
- Related incidents
- Associated campaigns
- Attribution (related threat actors)

Tracking and sharing campaign information is critical for threat intelligence analysis. This information allows organizations to develop an understanding of the threats they face as well as the specific objectives and capabilities an adversary or group is believed to have employed. Sharing campaign information among organizations can help all participants develop a much more comprehensive understanding of these threats.

Organizations may be reluctant to include attribution information when sharing campaign information due to its sensitive nature. Sharing campaign attribution information is not always necessary to facilitate a broader understanding of a given campaign.

Campaign information often comes from government or industry cyber threat intelligence sources. More established sharing organizations including ISACs may operate their own cyber threat analysis teams and track campaigns relevant to managing their cybersecurity risk or risk to their members.

Campaign information is frequently more strategic in nature and used to inform situational awareness and decision making.

4.9 ANALYTICAL REPORTS

A number of important types of information an ISAO can choose to provide its participants are based on analysis. Many organizations focus on information sharing, but analysis can also provide valuable information for ISAO stakeholders. Participants who engage in analysis can find benefits in their immediate, tactical and strategic decision-making.

Common communication report types are alerts, notifications, and assessments. The following are examples of content for information analysis reporting:

- The impact of threats to core corporate functions
- Description of threat activity relative to an attack life cycle
- Trends of malicious activity as it relates to an organization's infrastructure (e.g. infrastructure most targeted, configurations most exploited, etc.)
- Effectiveness of mitigations
- Cyber threat trend reports
- Threat horizon reports
- Proactive (assessments) and reactive reporting (post-mortem to an incident)

4.10 THREAT INTELLIGENCE REPORTS

Threat intelligence reports are a broad category of cyber threat information ranging from high-level trending reports to detailed analysis of specific campaigns. Vendors, governments, and independent organizations produce various types of reports, including open source intelligence reports. Some are targeted at specific incidents, some are predictive, while others describe the current state of the cyber threat landscape. These reports can include the full range of cyber threat intelligence providing strategic, tactical, and immediate response value. The report can include campaign, threat actor, TTP, and indicator information. Some reports are the result of several years of analysis and tracking of cyber threats.

4.11 SECURITY ADVISORIES AND ALERTS

Security advisories and alerts are published by a variety of sources, including international CERTs, governments, software and security tool vendors, ISACs, not-for-profit organizations, and security researchers. These publications vary from the rebroadcasting of important software vendor's security advisories to tailored products aimed to raise awareness of important new vulnerabilities and security issues.

Many of the major international CERTs provide security advisories and alerts. For example, US-CERT publishes alerts about current security issues, vulnerabilities, and exploits. These alerts attempt to describe the issue, explain the impact of the issue, and offer suggested mitigations to address the issue.[13]

Sharing security advisories and alerts can provide the full range of immediate, tactical, and strategic information to impact decision making and actions.

[13]See https://www.us-cert.gov/ncas/alerts

4.12 OPERATIONAL PRACTICES

Sharing operational cybersecurity practices among ISAO members is an important way for organizations to collaborate and build trust, learn from each other and collect feedback as they mature their own cybersecurity practices. This type of sharing enables an organization to benefit from methods for solving a problem that other members may be using successfully. This type of information can include best or effective practices, effective architectures, effective or ineffective system configurations, manning strategies, and more. Sometimes sharing what did not work is as valuable to the ISAO membership as knowing what did.

5 STEPS TO CONSIDER WHEN SHARING INFORMATION

The first step is to identify what information an ISAO and its members will share. The ISAO and its members should determine what information is shared and when it is shared based on the goals and mission of the ISAO and the needs and capabilities of its members and customers. Identification of what information to share is the basis on which subsequent decisions should be made.

After identifying the information to be shared, the ISAO and its members should identify sensitive data that they wish to share and the procedures for handling that data. For example, some ISAOs may choose to enable sharing without attribution, while other ISAOs may choose to require attributing shared information with a specific member. Non-attribution could make a member feel more comfortable in sharing, but knowing who is sharing the information could provide greater confidence in its quality and accuracy. Other examples could include, but are not limited to, personally identifiable information (PII), business sensitive information, or information with legal requirements for protection. ISAOs should establish the policies that they determine best meet the operational needs and legal requirements of their organization, membership, and customers. More information on sensitive data can be found in Section 8, Operational Considerations, and Section 9, Information Privacy.

Once the information to be shared and the sensitivity issues associated with it have been identified, it is important for members to agree on the mechanism and methods to be used to meet the goals of the ISAO.

For example, an ISAO could do one or more of the following:

- Provide a platform for and facilitate member sharing
- Implement and manage technology that gathers information
- Subscribe to a third-party service providing threat intelligence feeds
- Collect, aggregate, and disseminate open-source reporting
- Collect, aggregate, and disseminate reporting from partner organizations

ISAOs can choose to share information via automation, human interaction, or a combination of the two. Sharing among members and the ISAO may be done through machine-to-machine automation. Sharing indicators in an automated fashion can enable information to be shared more rapidly, increase the volume of indicators shared, and also increase the quality of shared data. This technology is emerging and needs to be driven by organizationally established policies for automated information exchange when sharing between members and potentially other ISAOs. In most cases, an ISAO will share with members using multiple means. Human-to-human sharing can increase trust among participants, making them more willing to share. As such, there is value in both automated exchange and human exchange.

To capture the goals, principles and methods an ISAO will operate under, an ISAO and its members should develop information sharing policies guiding members in how they can use the information shared within the ISAO and among its partners. These policies should include the types of information to be shared, the appropriate methods for sharing, identification and handling of sensitive data, and safeguarding requirements. Other areas for consideration could include the following:

- How should information shared be marked?
- Can members externally share the information they receive from the ISAO?
- Can the ISAO share the information with other partners or ISAOs?
- How should information shared over the phone or during virtual and in person meetings be handled?
- What policies, privacy controls, and protection should an ISAO have for shared information in motion and at rest?

There are various ways to incorporate such policies. Some of these include:

- Asking members to sign a non-disclosure agreement
- Using a carefully designed process for information sharing
- Requiring an effective and comprehensive ISAO employee code of conduct
- Using the Traffic Light Protocol (TLP)[14] or similar to ensure that sensitive information is only shared with those who are authorized to receive it
- Detailing how the information can be used in a concept of operations (CONOPS)
- Developing a separate, stand-alone, information use agreement within the ISAO

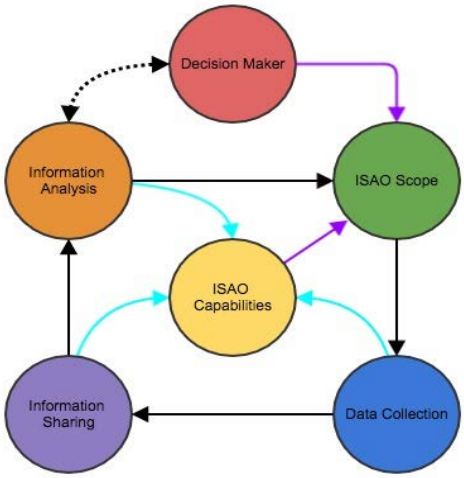
[14]See https://www.us-cert.gov/tlp

To ensure that members share and receive information valuable to them and others, ISAOs should consider establishing periodic reevaluations of these policies to ensure member needs are continuing to being met.

6 INFORMATION ANALYSIS

Successful information sharing and analysis depends on the production of actionable intelligence accessible and useful to participating analysts. The purpose of information analysis is to learn from and understand the data, combining context with other data, to produce information and gain insights which are not readily obvious. Information sharing and information analysis interdependence, combined with data collection and an ISAO's scope and capabilities, creates the framework for delivering intelligence to decision makers, as shown in Figure 4.

Figure 4. Framework for Delivering Intelligence



Cybersecurity information analysis involves reviewing data for signs or indications of unusual or malicious activity. The findings from the review can identify artifacts or evidence that analysts can use to link with similar threat data, helping to identify malicious TTPs, threat groups, or campaigns. ISAOs all perform some form of analysis, even if it is only the decision to share relevant information. ISAOs however, are uniquely positioned to bring together data from multiple sources and engage the expertise of their participants to produce actionable intelligence.

Information analysis involves interpretation and operational learning based on available data sources. The first stage is the initial review of shared data. For example, an ISAO may assess shared data to identify related threats across multiple organizations. In the second stage, analysts interpret relevant threat data to produce threat group, campaign summaries, or business risk assessments.

Information analysis has inherent challenges. First is identifying the questions of interest to ISAO members. Second is identifying the relevant data among multiple streams of data feeds and data repositories. Third is making analysis available, at the appropriate level, to ISAO members and helping them understand its relevance to other data, and its applicability to their organization.

The ISAO and its membership need to agree on the data points collected and how data will be accessed and securely stored. The ISAO can then consider their analytic approach and the types of reports which will be valuable to their members. ISAO members may have different appetites for intelligence consumption.

For example, an ISAO focused on security or network operations may desire information that filters relevant data from network noise. Another ISAO may choose to engage on threat activity that occurs across multiple members. An ISAO should consider a survey of their members to understand what type of reporting is most useful and what each member can contribute to the aggregate collection.

The analytical options an ISAO may provide could include detection of first-seen or anomalous activity, identification of an exploit to a software or network vulnerability, collection of related threat activity, or attribution to an individual, criminal enterprise, or nation-state. ISAOs considering analytical services should consider secure data stores and/or facilities to enable analysis and facilitate member communication about threats. For example, an ISAO could create a threat knowledge base consisting of indicators for detection, threat information for response, and attribution for risk management. This threat knowledge base enables the ISAO and its participants to use analytic methods and share their knowledge and assessments.

While all members must agree on what types of analysis to share or work collaboratively on, there are a number of common reports an ISAO could consider developing. These include but are not limited to:

- Pivot reports—observed IP addresses depicting connecting hop points. Members can use these reports to identify areas of common concern.
- Malware—an ISAO could collect the hash values of malware that members see on their networks each month.
- Campaigns—ISAO members may want to share information on a given campaign, such as ransomware or business email compromise. They can also share observed TTPs used by the actors.

Analyst assessments helps to better understand relevant threat information; however, the analyst's environment or visibility may introduce bias when categorizing threat or attributing threat activity to an actor. ISAOs are uniquely placed to help mitigate against this bias. By establishing a threat intelligence sharing community, an ISAO can help foster a culture which reduces analyst bias and provides continuous feedback through detection, peer communication, and external confirmation.

To assist in sharing trends and pattern analysis among the membership, an anonymous member survey can be an effective tool. Through the use of a collaborative tool, members can collect aggregated metrics from each of the organizations on an agreed upon frequency. This can include the number of phishing attempts, intrusion attempts, successful intrusions, number of accounts compromised, and distributed denial of services attacks. From this data, the ISAO can create a trend analysis for its members without specific attribution to any one member. For example, the ISAO weekly or monthly report could identify attack types by the size of the business, the sector, the time of day the activity occurred

during, the IP address and the country of origin of the attacker (if known), the attack vector used, and so forth.

6.1 ANALYTICAL CONSIDERATIONS

An ISAO offering dedicated information analyst services should be capable of securely storing data from varied data sources (both privileged and public) and leveraging analysts experienced in data review, threat interpretation, and development of intelligence assessments.

Before doing analysis, ISAOs may want to begin by helping their members take data quality measurements. The validity of trend and pattern analysis relies on accurate and relevant inputs.

If member organizations agree, an ISAO may consider utilizing sensors on member networks and report attributes back to a secure shared repository managed by the ISAO for generating reports and alerts. Some ISAOs may allow members access to the repository allowing individual members the ability to query and generate their own analytical reports.

ISAOs should consider using a common vocabulary for reporting cyber activity, which can be aggregated across ISAOs and, if they choose, with government agencies.

As ISAOs mature and aggregate data, they can look at creating baselines of normal behavior and doing predictive analytics which will identify anomalies and indicators of future actions.

Analysts ultimately communicate their assessments to decision makers. Common communication report types are alerts, notifications or assessments. ISAOs may need to survey their members to determine the content format that works best for their decision makers.

6.2 ANALYSIS SERVICES

An ISAO can provide a trusted environment for its participants to encourage analysts to collaborate and share relevant information. ISAOs providing, facilitating and leading these analysis activities can significantly increase the value of their efforts. ISAOs can serve as the aggregator of the analysis of their members or embed some level of capability in the ISAO. The decision whether to utilize member's analysts, ISAO analysts, or a combination of both should be driven by the ISAOs information sharing goals.

ISAOs perform some form of analysis, ranging from the decision to share relevant information, to full pattern and trend analysis. In addition to the items discussed below, an ISAO may produce other operationally oriented analysis products. Further, beyond these operational products, ISAOs may be in a position to provide trending analysis reporting and strategic analysis to help those

who make decisions affecting their organization's future planning and resource requirements.

The following are examples of how an ISAO can support analysis:

- **Risk awareness and mitigation communications.** One of the most valued analytical contributions an ISAO can make is to promote the collaboration among ISAO participants, its analysts, and others to raise awareness and educate participants on cybersecurity risks and approaches to be considered for mitigating those risks. In some cases, the sharing of collective knowledge and collaboration among expert personnel might involve only a small number of the ISAO participants, but could result in broader communication to the ISAO participants. These "*tactical*" or operations-focused communications can provide guidance to prevent successful attacks, identify methods or procedures to mitigate specific risks, identify effective practices being applied by others, and report details from participants on their experiences and the effectiveness of actions they have taken.
- Such communications can be tailored for various audiences within the ISAO constituency (executives, managers, and operational personnel) and delivered as required and/or as a periodic communication. Communication can take the form of emails, reports, briefings (webinars), conference calls, and other networking/collaboration events among participants and others. These communications will assist those responsible for making informed decisions for their organization.
- **Alert notifications**. By examining the flow of information through an ISAO, the ISAO has the opportunity to identify new, changing, or escalating cybersecurity risks or incidents of particular interest to its participants and others. This analysis can alert members and partners to urgent, crisis, or other levels of notification and help ISAOs provide information and recommendations to their members and partners on immediate action they can take to mitigate the risk. Providing subsequent updated alerts and additional analysis can further assist an ISAO, its partners, and others to understand the evolving nature of an incident, threat, or risk.
- **Incident response coordination**. Some ISAOs may envision a role of understanding and sometimes becoming actively involved in responding to cybersecurity-related incidents. ISAOs may be asked by some members to assist in incident response. In such cases, an ISAO can provide an opportunity for collaboration among analysts of member organizations to determine necessary operational coordination and the effectiveness of response actions taken as a situation progresses and is resolved. After-action and root-cause reports can be prepared and provide valuable information to be shared among ISAO participants and others. If an ISAO is to assume a role in coordinating incident response, it may want to consider identifying the specific value of its incident response function, its role in incident response, and the triggers for activating it.

7 ARCHITECTURAL CONSIDERATIONS

People share information in many ways, but information sharing can be viewed through three architectural constructs: sharing models, sharing methods, and sharing mechanisms.

Ultimately, how models, methods, and mechanisms are implemented will vary widely based upon ISAO member needs, administrator capabilities, community goals, available technology, and the centers and dynamics of trust in a community.

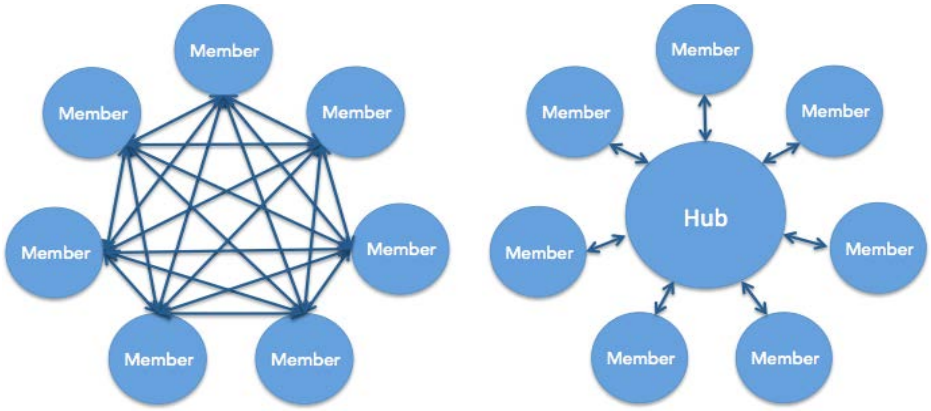
ISAOs should consider what models and mechanisms could be a good fit for the context in which each operates. This can best be accomplished by comprehensively mapping all information sharing and analytic services and touch points to the delivery of sustainable member value. Doing so enables ISAOs to construct an information sharing and analytic architecture to provide long term strategic sustainment of member value and ISAO viability and maturation.

7.1 SHARING MODELS

This section details two common sharing models ISAOs may consider adopting: peer-to-peer and hub-and-spoke. They are driven primarily by the role of an information "authority" and can be blended into hybrid approaches.

Peer-to-peer and hub-and-spoke sharing models may be the most useful basic arrangements that new ISAOs can consider when getting established.

Figure 5. Sharing Models



7.1.1 PEER-TO-PEER

The peer-to-peer sharing model is defined generally by the ability of any member of a community to interact and share with any other member. Peer-to-peer networks can be especially beneficial for smaller communities or when members only interact with a part of a community. They may also be especially beneficial

for those whose members have asymmetrical trust relationships or share under highly dynamic conditions that often change based upon content, current threat, and so on. Members generally have a high degree of choice when determining with whom they share in the community. In this model, there is no "gatekeeper" governing event-by-event sharing, or how and what sharing occurs. That is not to say an authority (ISAO administration, for example) does not create or enforce a sharing policy, or perform other authoritative duties. Instead, members of the community generally share when, what, and with whom they see fit, based upon established ISAO policy and procedures and within the confines of the tools used.

A challenge with this model is the difficulty managing many trust relationships when community membership grows. In addition, redundant sharing of the same information may be more likely in this model, and it may lead to inefficient "churn" depending upon ISAO technology and other conditions.

7.1.2 HUB-AND-SPOKE

Generally, the hub-and-spoke sharing model incorporates a "gatekeeper" at the center, or hub, of the community. Members share through the hub while some combination of people, process, and technology drives redistribution out to the rest of the community. This sharing model provides opportunities to centralize, formalize, or otherwise influence information exchange for the benefit of the community. This may take the form of ISAO administration funneling and vetting widely disparate member and vendor threat intelligence, offloading threat analysis services from the membership to achieve economies of scale, enforcing policy, or simply playing a more central and visible role in the day-to-day activities of the ISAO. In addition, the hub is a logical place for a single "ground truth" to exist for the community, whether that has to do with policies and procedures, analysis of recent incidents or campaigns, or other areas relevant to the ISAO.

There are a few challenges to consider with this model. Dependency on the hub could lead to problems if the hub is not performing as well as it should. A high degree of trust should exist in the people, process, and technology at the hub in order for this sharing model to succeed. And regardless of the level of trust in the hub, members will always have varying degrees of trust relationships elsewhere among ISAO membership. Always funneling threat data or cyber threat indicators exclusively through the hub could inhibit the growth of personal relationships among ISAO members. Relationship building will lead to trust among the membership, and trust is arguably the primary key performance indicator for successful threat intelligence sharing.

7.1.3 HYBRID APPROACH

An ISAO can address some of the challenges of the peer-to-peer and hub-and-spoke models by forming a hybrid approach combining elements of both. This

could take virtually limitless forms, but the following are some possibilities to consider:

- Channel some kinds of threat intelligence through the hub for redistribution or analysis, based upon hub strengths and core competencies. Budget, people, technology, or geography, and how these factors impact member requirements and objectives could all help determine what obligations and tasks are a good fit for the hub.
- Leverage peer-to-peer sharing for certain kinds of intelligence, such as strategic intelligence. Peers working together to build a threat actor profile, for example, is a great way to leverage community resources, build relationships and trust among ISAO membership, and make a positive contribution back to the ISAO community. And the work product could be redistributed through the ISAO hub, combining aspects of both peer-to-peer and hub-and-spoke models.

These sharing models are high-level conceptualizations of how an ISAO can share information. Once a newly forming ISAO has a good sense of what it wants to do, selecting the appropriate sharing methods and mechanisms it employs will be critical to getting things done efficiently and effectively.

7.2 SHARING METHODS

This section details methods that can be applied to either of the above models. Sharing methods are largely directed by community requirements and concepts of operations, and also tied to the tools and technology adopted by an ISAO to enable certain kinds of sharing.

7.2.1 PUBLISH–SUBSCRIBE

A publish-subscribe method for sharing threat intelligence consists of a producer who publishes information on a regular or irregular basis, and whose publications are individually subscribed to by one or more community members. This approach can be applied in either the peer-to-peer or the hub-and-spoke sharing models. In the case of a peer-to-peer network, a producer could, for example, automate cyber threat indicator sharing into a repository from which other members pull feeds, or a producer can post to a message board/forum and subscribers receive alerts. In the case of the hub-and-spoke model, the publisher may be the ISAO hub and the producers (members) could submit to the hub for processing—usually to verify, refine, de-duplicate, or correlate with other known threat intelligence—before publishing it out to the ISAO subscriber base. The precise role of the hub can vary widely, depending upon the ISAO CONOPS and other conditions. One of the benefits of the publish-subscribe method in a hub-and-spoke model is the ability for the ISAO to aggregate and analyze information in a central location and then publish a richer, more complete picture of an incident or actor. This is very useful in a rapidly evolving environment when many participants may be sharing different observations and analyses.

7.2.2 CROWDSOURCING

Crowdsourcing occurs when ISAO members collectively contribute to a discussion thread, an automated cyber threat sharing repository, or another system to organically transform granular threat data into more coherent threat intelligence. By virtue of participating in crowdsourcing the intelligence picture, the information is also shared with members. Like the publish-subscribe method above, crowdsourcing can take place in both peer-to-peer and hub-and-spoke networks—the key distinction being the presence of a central party directing the crowdsourcing through the hub, versus true organic freewheeling among the community. Both, of course, can be very effective. One of the benefits of crowdsourcing is that the virtual social interactions among ISAO members help to build trust and strengthen the community.

These are two common sharing methods closely tied to the tools and technology an ISAO uses to support its CONOPS. New ISAOs can seek certain tools to enable sharing methods it already believes will be effective. Alternatively, the tools it already uses may determine what sharing methods are at its disposal.

7.3 SHARING MECHANISMS

A variety of mechanisms and practices can be used to share information among an ISAO's members and partners. Table 2 depicts the types of mechanisms and practices an ISAO may want to consider as initial or additional sharing capabilities. The mechanisms and practices selected will need to be tailored to the scope, timeliness, and sensitivity of the information to be shared.

Information sharing can occur one-to-one, one-to-many, many-to-many, and many-to-one. As a result, practices an ISAO selects for communication and sharing information must reflect the overall objectives it is seeking to achieve for its members.

Due to the sensitivity of some information, methods and mechanisms used to share information must be capable, in accordance with an ISAO's policies or other authoritative restrictions, to protect and provide information to authorized members. For example, an ISAO using a Traffic Light Protocol (TLP) to handle and distribute sensitive information will need to use mechanisms providing it the capabilities to comply with its TLP policy.

If source anonymity is required, additional information sharing processes, procedures, and features will be needed by the ISAO. For that reason, the practices selected by an ISAO and its operational procedures will need to provide the operational, security, and management features necessary to meet the ISAO members' objectives.

Information sharing mechanisms should also be selected with consideration for the importance, timeliness, and criticality of receipt of information by ISAO participants. Members should be able to authenticate and trust the information comes

from expected sources. In some cases, positive confirmation of receipt of information may be required to ensure delivery of time-sensitive information.

Effective ways of sharing information among ISAOs can include the use of automated information sharing platforms for primary indicators and defensive measures, as well as follow-on information from ISAO members. ISAO's may also include feeds received from threat intelligence firms to supply members with information, or members may subscribe to these feeds and relay relevant information to the ISAO and other members. Email, chat, and social media platforms may also be used to enable collaboration and information sharing between personnel from ISAO members.

Table 2 below lists a number of sharing mechanisms to consider.

Table 2. Sharing Mechanisms to Consider

The mechanisms listed below provide general guidance on various options and their applicability:								
Description		**Applicable To (* Note)**				**Can provide Anonymity**	**Access control features**	**Comment**
		one to one	one to many	many to many	many to one			
In person meetings	Individuals physically meet with participation restricted to authorized individuals.		X	X		No	One Level: All authorized receive the information.	Access control to information can be restricted to a selected participating community through procedures.
Tele-conferencing/WebEx, etc.	Commercial conferencing and collaboration services		X	X		No/Yes	One Level: All authorized receive the information.	A central management function required to achieve anonymity but in general not anonymous. Access control to information can be restricted to a selected participating community through procedures.
Email (general)	Internet-based email	X	X	X	X	No/Yes	Distribution can be restricted	A central management function required to achieve anonymity but in general not anonymous. Distribution restrictions possible but difficult to manage for a large number of participants.
Email (with encrypted message)	Encrypted file or message	X	X			No/Yes	Access to information based on	Use of end-to-end encryption mechanisms, e.g. S/MIME, PGP, etc.
Email - List servers	Services for managing email lists		X	X		No/Yes	Distribution can be restricted	A central management function required to achieve anonymity but in general not anonymous.
Messaging Services (Short, Enhanced and Multi-media)	Carrier and vendor based services	X	X			No	Distribution can be restricted	Examples, Slack, HipChat, etc. Challenge-reply authentication can prevent spoofing.
Peer-to-Peer Networks	Characterized as a server-less network.			X		No	Distribution can be restricted	Security policies should be implemented to define what types of P2P software is acceptable and what information can be shared through them due to various risks.

The mechanisms listed below provide general guidance on various options and their applicability:								
Description		Applicable To (* Note)				Can provide Anonymity	Access control features	Comment
		one to one	one to many	many to many	many to one			
Website (Public)	All pages available at the sites URL		X			No/Yes	No restrictions	Central management trusted to be responsible for assuring posted information is anonymous.
Website (Private)	Selected pages at website require access credentials		X			No/Yes	One Level: Those with website access credential	Central management trusted to be responsible for assuring posted information is anonymous.
Secure Portal	Electronic gateway to a collection of digital files, services, and information, accessible over the Internet through a web browser. A client-server based system with multi-levels of access control to searchable databases.		X	X	X	No/Yes	Multi-levels of access control based on authorized access policies and authorized credentials.	Central management enforces authorization and rules-based access control policies. Anonymity achieved through an anonymous access credential distribution process and posting/review by portal management policies and procedures.
Automated Mechanisms	Structured representations of cyber threat information automatically shared among trusted partners and communities in a machine processing structure.	X	X	X	X	Yes	Multi-levels of access control based on authorized access policies and authorized credentials.	An example is STIX™ (Structured Threat Information eXpression) language <https://www.mitre.org/sites/default/files/publications/stix.pdf>
Notification Services	Notification Services generate and send messages to users or other applications that have subscribed to the service.	X	X			No	Multi-levels of access control based on authorized access policies and authorized credentials.	Notifications may be by e-mail, telephone, fax, text messages, etc.
* Note:	One-to-One	One sender and One Receiver						
	One-to-Many	One Sender and Many Receivers						
	Many-to-One	Many Senders and One Receiver						
	Many-to-Many	Many Senders and Many Receivers						

8 OPERATIONAL CONSIDERATIONS

The trusted relationships essential to an effective ISAO are best achieved when organizations embrace a culture of operational security among their members, partners, and those with whom they share information. This culture is enabled through well-designed ISAO operational policies, procedures, awareness, and good practices.

An ISAO's operational security efforts should include the following considerations:

- Establishing the criteria and vetting process for those eligible to participate in the ISAO.
- Examining the full range of the sensitive information an ISAO will be handling and communicating, and then using a risk-based assessment to develop the ISAO's operating rules,[15] information policies, and controls to be implemented across the ISAO and for members when interacting with the ISAO.
- Defining policies that address any identification of membership, the ownership of the information shared with the ISAO, the use of the information shared, and the sharing of information among members and with others, along with any analytic product developed by the ISAO. To implement these policies, the agreed upon controls and practices to be exercised by members should be documented and be a condition for participation in the ISAO.
- Specifying how information is to be provided to the ISAO and its members along with any review processes that may be implemented to protect the confidentiality and privacy of the content.
- Establishing procedures for expediting and prioritizing the timely sharing of information, allowing members to achieve the greatest value and to meet any immediate threat that could be posed by the attacks.
- Defining the labeling and handling procedures for the range of sensitive information to be handled within the ISAO and among members which could include using the Traffic Light Protocol (TLP)[16] approach currently used by ISACs and others for these purposes.
- Specifying procedures and practices where anonymity of information sources will enhance the sharing and trust among members and maintaining them in the operations of the ISAO. In practice there will be times when the owner of the information can decide that anonymity is not necessary or practical, and procedures should accommodate an information owner's prerogative.
- The leadership/management of an ISAO should ensure there is an active and periodic awareness effort to keep members informed of the expected code of conduct and their responsibilities in accordance with the ISAO's security and privacy policies. Any changes made should be fully vetted with and promulgated to participants.
- Developing specific operating rules for automation capabilities for real-time or near-real time information sharing, if used by the ISAO, because of the critical

[15] As an example, the "Operating Rules" of the FS-ISAC are available at https://www.fsisac.com/sites/default/files/FS-ISAC_OperatingRules_2015.pdf

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

impacts (both positive and negative) such capabilities can have on an ISAO or those participating in the automated sharing of information.

- Establishing procedures and criteria for removing members who violate the trust and agreements of the ISAO; ensuring organizations that assign personnel to be a member of an ISAO notify the ISAO of any changes in their assigned personnel status; and ensuring access authorizations are periodically reviewed and procedures are in place for immediately removing access authorizations that are no longer valid.

These operational considerations only highlight general aspects ISAOs should consider establishing. An ISAO's specific operational security policies and procedures must address its specific operations and the sensitivity of information being handled. ISAO operations will change over time, and periodic review of operational security procedures and policies may require updates. Annual reviews can be an effective check to ensure they are up to date. Any changes made should be consistent with the organization's governing documents.

9 INFORMATION PRIVACY

It is important for ISAOs that receive, analyze, retain, use, or disseminate cyber threat indicators or other information through a voluntary cybersecurity information sharing process to be sensitive to and protective of privacy considerations and be aware of and comply with applicable privacy law. ISAOs will need to maintain a careful focus on managing information privacy. Ensuring privacy protections is critical to the process of information sharing and will increase partners trust in the overall structure of the ISAO itself. Attention to privacy can help the ISAO to manage or eliminate barriers and concerns around voluntary sharing of its members and partners. While ISAO participants may vary in having individual privacy officers, it is critical the ISAO itself be capable of managing these issues. These outcomes support sustainable and continuously improving ISAO business performance and viability. A focused approach to ensuring full privacy protections allows a broader awareness of the benefits of information sharing as a whole. It is also an important part of an appropriate risk management structure that is important to any ISAO.

At a minimum, privacy considerations should include the individual members of an organization, the privacy of any individuals whose data may be included in cyber threat indicators to the extent provided by law, and a full range of other constituencies, customers, and individuals. To adequately protect privacy while accomplishing the goals of an ISAO, it is important for the ISAO to provide guidance to members, participants, and ISAO staff that will be helpful in striking a balance between allowable sharing of cyber threat information and protecting privacy. The purpose of this section is to help ISAOs attain that balance, without describing all existing laws and when, how, and where they might apply.

Before sharing cyber threat indicators, it is important to consider the privacy implications of what is being shared, including:

- whether the indicator contains information the ISAO knows at the time of sharing to be personal information about a specific individual or that identifies a specific individual;
- whether that identifying information is not directly related to a cybersecurity threat, and if so,
- whether the ISAO or member has identified and removed, as appropriate, such 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 opportunity to consent to involvement in the process used to collect that information or access or correct that information. ISAOs should attempt to limit the impact of the data they collect on individual privacy where they can do so and maintain the effectiveness of cyber threat information sharing arrangements.

It is permissible under the Cybersecurity Information Sharing Act (CISA) of 2015[17] to share personal information as part of a cyber threat indicator but only in circumstances where it is directly related to the threat at the time of sharing. ISAOs may be at risk even beyond a possible failure to qualify for liability protections under CISA without appropriate limitations on the receipt, retention, use, and dissemination of personally identifiable information (PII) when it is not part of a cyber threat indicator.[18] DHS has issued privacy guidance[19] concerning information shared with the U.S. government. In some instances, sensitive information such as PII, intellectual property, and trade secrets may be inadvertently encountered when handling cyber threat information. The improper disclosure of such information could cause harm to individuals, companies and others. Accordingly, organizations should consider and implement security and privacy controls and handling procedures necessary to protect this information from unauthorized disclosure or modification.

Often data requires protection, either by law, regulation, or contractual obligation. This includes PII and other sensitive information afforded protection under the Sarbanes-Oxley Act, the Payment Card Industry (PCI) Data Security Standard, the Health Insurance Portability and Accountability Act (HIPAA),[20] the Federal Information Security Modernization Act (FISMA) of 2014, the Gramm-Leach-Bliley

[17]See https://www.congress.gov/114/plaws/publ113/PLAW-114publ113.pdf

[18]See National Institute of Standards and Technology, U.S. Department of Commerce, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

[19]See https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec 105%28a%29%29.pdf

[20]See https://www.congress.gov/104/plaws/publ191/PLAW-104publ191.pdf

Act (GLBA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, and the Children's Online Privacy Protection Act (COPPA), among others. The Federal Trade Commission and States each address privacy and data protection and, depending on the source and type of any personal information, and whether there are any relevant cross-border transfers, the law of non-U.S. jurisdictions may apply. Not all ISAOs will handle information that is subject to all or any of these laws and regulations, so ISAOs will not necessarily need to understand all of these laws. It is important, however, for ISAOs to understand, what, if any, information they might receive, have or share is subject to specific regulations and to identify and appropriately protect such information.

ISAOs should establish policies against sharing PII or other sensitive data not related to cyber threat indicators. As mentioned above, an ISAO may be subject to HIPAA, PCI, or other regulations on data it holds or stores. For example, an ISAO collecting credit card payments is subject to PCI requirements and employee health records are covered under HIPAA regulations. Therefore, it is important for ISAOs storing or collecting this or related information to understand their obligations under the appropriate regulations.

ISAOs should consult, as necessary, legal, privacy, and data security experts familiar with the various regulatory frameworks when developing procedures for identifying and protecting sensitive information to ensure compliance with all existing privacy regulatory and legal requirements at the federal, state, local, and international levels.

9.1 CORE PRINCIPLES

As with security policies, it is most effective to establish privacy policies during the earliest stages of an ISAO's formation. Depending on what information is to be collected and shared, and where, developing privacy policies to meet the various applicable laws can be complex. It may be necessary to engage appropriate legal counsel. In developing such policies, ISAOs and their members should consider the following principles:

- ISAO members are encouraged to identify and contribute indicators critical to identifying threats, while making efforts to minimize the PII shared with the ISAO or other members, and ensure compliance with all existing privacy regulatory and legal requirements at the federal, state, local, and international levels.
- If a member inadvertently submits PII not directly part of a cyber threat indicator to an ISAO, the member should understand the appropriate process for notifying the ISAO.
- The ISAO should consider having procedures in place to remove and remediate PII or other types of sensitive information when notified by an ISAO member. This may include developing policies and procedures providing reasonable and appropriate timeframes for the timely destruction or return of

cyber threat indicators containing personal information about specific individuals or information that identifies specific individuals.

- ISAOs are encouraged to consider policies that provide transparency to members about their intended sharing partners and notice of any material changes in policy or practice. An ISAO should also seriously consider (after obtaining any legal advice it may need) disclosing to its members whether it seeks to operate within the confines of CISA in order to obtain liability protection and how it may do so, including the potential risks and implications of that choice for privacy and other matters.

9.2 SUPPORTING PRINCIPLES

DHS has issued guidance related to privacy issues when sharing between industry and government. It has acknowledged that limited liability protections provided under CISA relating to privacy and sharing also apply when sharing is only within industry and does not include government. That guidance delineates the processes that must be used for attaining limited liability protections under U.S. law. It is important that ISAOs and their participants and member organizations are familiar with applicable privacy law and policies and incorporate appropriate commitments and policy provisions into member rules, foundational documents, and user agreements.

ISAOs may want to consider designating a specific staff member, board member, or outside party (such as a contractor or attorney) with responsibility for and authority to ensure compliance with applicable state and other privacy laws and to take action if such issues arise.

Segmentation, a process for identifying certain data fields that may require special handling of sensitive personal information, may be useful to ISAOs when developing cyber threat indicators. Segmentation may include a process for identifying certain data fields requiring 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, if any, who frequently handle PII with less than the necessary care. If information to be shared is not always subjected to a privacy review by the ISAO, it may want to consult with legal experts to identify whether there are any implications for liability or the availability of liability protection.

When sharing automated indicators with DHS, ISAOs may be required to adhere to various practices and agreements, including the DHS Automated Information Sharing (AIS) Terms of Use.[21]

[21]See https://www.us-cert.gov/sites/default/files/ais_files/AIS_Terms_of_Use.pdf

Certain DHS requirements of note are included in 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."

When engaging with international partners or sharing information across national borders, ISAOs and their members should be aware that international privacy laws may differ from U.S. federal, state, or local laws. For example, depending on membership and circumstances, if an ISAO includes an European Union (EU) component, ISAOs should seek to understand what information, if shared, might need to be compliant with U.S.- EU agreements such as Privacy Shield[22], the EU General Data Protection Regulation (GDPR),[23] and the Network and Information Security Directive (NIS)[24].

If an ISAO decides to share threat indicators or defensive measures with the NCCIC at the Department of Homeland Security or other government partners—particularly if it intends to secure the explicit legal protections available under CISA when doing so—it is important it is familiar (with the help of legal counsel, if needed) with the requirements in CISA, and relevant privacy guidance.

An ISAO should implement appropriate processes and procedures consistent with CISA if it chooses to seek the full scope of liability protections available under that law. This 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, whether sharing with the federal government through the NCCIC or sharing only in the private sector. To be in compliance with CISA, sharing organizations

[22]See https://www.commerce.gov/page/eu-us-privacy-shield

[23]See http://www.eugdpr.org/

[24]See https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

should, at the time of sharing, remove PII not directly related to a cybersecurity threat.

The DHS document *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*[25] provides examples of certain personally identifiable information that can be part of a threat indicator and be shared. This includes particular IP addresses in certain circumstances and gives examples of personal or other information that should not be shared and of impermissible uses of shared information.

The following are additional examples of actions an ISAO may wish to consider and address in processes and procedures developed to guide its functions:

- Socializing the processes, procedures, plans, and exercises to ensure that ISAO managers know what to do and respond appropriately if the ISAO receives PII that it possibly should not have received.
- Reviewing various guidance on privacy considerations, such as the privacy section in the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (aka, The Cybersecurity Framework)[26] and determine which of those recommended actions are relevant and may be desirable to use in its operations.
- Identifying the safeguards that may be necessary at all stages of the PII 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.
- Identifying the processes and procedures to securely dispose of, de-identify, or anonymize PII that is no longer needed.
- Identifying the processes to ensure that access to databases containing PII may be audited. Log PII as part of an independent audit function, and determine how such PII could be minimized while still implementing the cybersecurity activity effectively.
- Evaluating the DHS profile for the AIS portal, including any privacy requirements.
- Determining whether a minimum information exchange process is needed to minimize information shared to only the data necessary to address the threats the ISAO is intending to cover.
- Developing a preventive plan for data protection, including both systems and human elements, and an equally clear remedial plan in the event of a breach.

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

[26]See https://www.nist.gov/cyberframework

- Developing an encryption policy that meets the needs and expectations of employees, customers, and counterparts.
- Determining its core membership and audience, and building in security and privacy requirements matching the maturity levels commensurate with its membership, recognizing that not all entities or participants receiving information have equal capabilities or equal privacy concerns.
- Adopting privacy and security controls that match the capabilities of its members and the criticality of the information shared. This may mean, for example, that sharing threats via e-mail 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.
- Establishing clear policy and procedures for data retention and disposition.

10 INFORMATION SECURITY

ISAOs will vary in size, sophistication, and abilities. They will also vary in the amount and types of information they share. However, all ISAOs, no matter how established or new, face common security challenges. ISAOs need to consider these security challenges and include security considerations at the beginning of the ISAO's business process through appropriate governance, risk and security policies. Doing this can facilitate success as ISAOs and their members will be more effective in building trust among the members, and between the members and the ISAO. Established ISAOs may also use this guidance to assess their own security. Ensuring that security is addressed as part of overall ISAO governance enables ISAO members and prospective members to make appropriate risk decisions about their participation in information sharing activities.

Security policies of an ISAO may vary to reflect the various types of information being shared, the different degree of sensitivity of that information, and the method by which that information is shared amongst and between members. For example, a security policy related to sharing automated indicators likely will be different from a security policy related to sharing PDF documents. Similarly, the policy for storing open-source news might differ from the policy for storing sensitive and otherwise confidential or non-public member submissions.

An ISAO's membership may also drive the levels of security needed. ISAOs whose members individually have robust security capabilities will likely have more robust security procedures together as an ISAO than ISAOs whose members have less advanced capabilities. Differences in an ISAO's and/or members' general capabilities may be driven by disparate legal requirements, risk tolerance, industry practice, or maturity in the information sharing ecosystem. Regardless of whether an organization is for-profit or non-profit, large or small, security is an important component of an ISAO's success.

CISA-required guidance issued by the Department of Justice (DOJ) and DHS outlines procedures for private-sector entities to follow when sharing cybersecurity information with the federal government. The guidance also includes basic structures and security requirements companies must meet to participate in the information sharing process with DHS. CISA also defines strong privacy protections, which are further detailed in companion documents. Not all ISAOs will participate in this DHS program, for a variety of reasons, but DHS guidelines may serve as an important reference for ISAOs choosing to participate in the program. ISAOs who choose not to participate might still benefit from an understanding of the security requirements of CISA and the AIS program at least as a comparison, as they develop and implement their own information sharing policies and procedures. DHS and DOJ have issued CISA implementation guidance for the private sector.

10.1 BASIC SECURITY COMPONENTS FOR AN ISAO

When establishing an ISAO, and at periodic intervals thereafter, ISAO members may want to consider and discuss the minimum levels of security they require to perform the basic functions expected of their ISAO.

10.1.1 SECURE COMMUNICATIONS

When establishing an ISAO, and at periodic intervals thereafter, ISAOs and their members should discuss and decide on appropriate requirements for securing communications, such as the appropriate use of encryption. Once the internal requirements are established, the ISAO can deploy the appropriate tools to meet them.

When establishing an ISAO, members may want to understand the security levels and capabilities of individual members. This will help ensure security policies are developed in a manner effective and appropriate for all members. Once an ISAO is formed and established, the ISAO may want to conduct a periodic review to ensure its capabilities and policies are appropriately calibrated to evolving member capabilities and requirements.

An ISAO may want to assess its participation (or anticipated participation) in various other information sharing programs and consider the security requirements of such programs. DHS has information sharing programs that have defined security requirements for how shared information needs to be stored and handled. For example, the DHS Cyber Information Sharing and Collaboration Program (CISCP)[27] has specific requirements for participants regarding how an organiza-

[27]See https://www.dhs.gov/ciscp

tion must store CISCP information. If ISAOs intend to participate in such programs, they should ensure they establish security policies that meet these requirements.

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

Before building or buying a platform for information sharing, an ISAO should establish the basic security requirements needed to facilitate information sharing among members should be established. It is much easier and less expensive to build the security requirements into the system up front, than it is to add them later. Those entities that participate in an ISAO will also have basic expectations that the ISAO itself is secure.

This includes considering whether encryption is required and, if so, what level of encryption is appropriate.

As an example, policies could detail whether all members will use certificates for signing and authenticating emails in a PKI exchange mechanism, whether the ISAO will deploy multifactor authentication, and whether documents being shared would be encrypted separately from the PKI process.

10.1.3 ACCESS CONTROLS

One key component of security is access controls, which derive from the fact not everyone in an organization needs access to all of its documents. Therefore, appropriate controls should be put in place so people are only allowed to access documents they are authorized to access. It also is appropriate for the ISAOs and their members to discuss and decide on appropriate access controls for ISAO staff and individuals within member entities.

Another component of access control is to be able to revoke credentials for people who have changed jobs within an organization or leave an organization completely. Thus it is appropriate for ISAOs and their members to agree on a common policy on how to ensure individual credentials are revoked when a member or employee is no longer permitted access to information.

Another general security principle is that data should be federated based upon criticality. As such, access controls may vary for different types of data. For example, it might be appropriate to allow the head of marketing access to an organization's collection of open source news reports, but that person may not need access to sensitive indicators shared by members or partners.

10.1.4 CYBERSECURITY ATTACK AND DATA BREACH NOTIFICATION

To maintain a level of trust and dependability between and among members, ISAOs may want to establish internal reporting plans and communication lines

with members in the event they are a victim of a cybersecurity attack impacting the ISAO and its members. It should be noted ISAOs are also subject to state and local data breach notification laws and could also be victims of a cyberattack that impacts PII, intellectual property or other sensitive data an ISAO holds for ISAO employees, contractors, members, or partners. In some cases, ISAOs may be regional in nature or include members from varying states; as a result, the ISAO will need to be cognizant of the different state data breach laws. Further, while an attack and a subsequent breach may not rise to the level of notification under a specific state law, ISAO members may want to establish their own baseline requirements that could go farther than may be required by law as a part of the trust factor within the ISAO. Finally, certain sectors have varying federal requirements for certain types of notifications that ISAOs should be familiar with, some of which extend to third party vendors as well.

10.1.5 DATA CLASSIFICATION, DISTRIBUTION, AND LABELING

Another general security principle is the need to appropriately mark and label information. This could include noting specific handling instructions for a particular document or marking it with a general classification. Such marking helps ISAO members understand how the information can be used and stored. ISAOs and their members can develop a classification scheme that fits their individual security policies. Further, a common practice is to enable the entity that owns the document to control how that information is shared. This concept is commonly known as “originator control.” The following are some examples of potential components to consider in a security policy:

- Using the Traffic Light Protocol (TLP) or other classification schemes, can help members understand how to share information according to data classification standards.
- Policies detailing how members can use shared indicators. For example, can they use those indicators to protect their customers or to only protect their specific network?
- Internal structures and policies limiting the risk of members sharing non-security proprietary information.
- Determining whether the ISAO should establish multiple sharing groups or forums that reflect the ability of its members to receive or store various levels of sensitive information.
- Issues for anonymizing member submissions, as well as establishing parameters for sharing when they want to use anonymization.
- Clear data retention and disposition policy and procedures.
- Options for sharing information including automated intake and dissemination, email, and other methods.
- Policies dealing with verbal submissions by members.

As an example, it would be helpful to consider distribution policies to set up rules for sharing data via email. Policies could cover matters such as:

- when to use the blind copy email feature,
- what information should be sent via encrypted email,
- criteria for who has access to and who can be on the mailing lists, and
- when to use “reply all” structures.

10.2 ISAO MEMBER SECURITY

Security of both the ISAO itself and individual members is critical. Trust is enhanced when members understand how other members will handle and store information being shared through and within the ISAO. Therefore, the ISAO and its members may want to consider developing policies related to the security responsibilities of member organizations. Potential considerations include the following:

- Detailing, in a common member agreement or other document common to all members, what the responsibilities are of each member in securing information shared through the ISAO.
- Detailing what tools will be used for sharing information and the policies for granting members access to those tools.
- Establishing methods to communicate and/or train members on what their responsibilities are under the ISAO security policy.

It is important to note these ISAO security policies are not a replacement for enterprise-wide cybersecurity practices of an ISAO member company. They also are not a replacement for any regulatory requirements or obligations ISAO member companies may be required to follow. ISAO members should take all appropriate steps to secure their own enterprises. There is a myriad of guides to help ISAO members manage cyber risk, including the NIST Cybersecurity Framework. The point of an ISAO security policy is to detail member responsibilities specific to securing information they receive from or share with the ISAO.

10.3 GLOBAL SECURITY ISSUES

If ISAOs include global corporations or entities, it is important for the ISAO to be aware of and discuss other requirements for members involving information security, cybersecurity, privacy, and overall cyber 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 (U.S.) and the EU reached an agreement on Privacy Shield, which includes directives on how data on European citizens can be collected, used and transferred, along with associated information security and privacy

requirements.[28] Other important EU requirements to be aware of include the EU GDPR and the EU Network and Information Security Directive.[29] The U.S. has agreements in place with the G7 and G20 nations around different aspects of cybersecurity and information sharing. In addition, other nations have different requirements for consent from individuals before use of personal data that will also relate to information sharing that ISAOs and their members will need to be fully aware of in advance.

- 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.

[28] See https://www.privacyshield.gov/welcome

[29] See http://ec.europa.eu/justice/data-protection/reform/index_en.htm
https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

APPENDIX A ADDITIONAL RESOURCES

This appendix is a list of resources that provides useful information for ISAOs.

Cybersecurity Information Sharing Act (CISA)

https://www.congress.gov/114/plaws/publ113/PLAW-114publ113.pdf

CISA implementation guidance for private sector

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

Cyber Information Sharing and Collaboration Program (CISCP)

The CISCP is a program managed by the US-DHS National Cybersecurity Communications Integration Center. This is the main information sharing program between public and private entities.

https://www.dhs.gov/ciscp

Department of Homeland Security, United States Computer Emergency Readiness Team (US-CERT) Automated Indicator Sharing (AIS)

https://www.us-cert.gov/ais

https://www.us-cert.gov/sites/default/files/ais_files/AIS_Terms_of_Use.pdf .

Department of Homeland Security and the 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, including at p. 14 and Annex 1: Sharing of Cyber Threat Indicator and Defensive Measure Sharing between Non-Governmental Entities under CISA, June 15, 2016.

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

European General Data Protection Regulation (GDPR)

These are a set of regulations for countries in the European Union to strengthen data protection for individuals.

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

EU Network and Information Security (NIS) Directive

The NIS Directive is a European wide legislation aimed at enhancing and increasing cybersecurity capabilities of all EU states.

https://ec.europa.eu/digital-single-market/en/news/directive-security-network-and-information-systems-nis-directive

Public Key Infrastructure (PKI)

PKI consists of all of the policies, procedures, and technology that is used to establish secure communication between two parties. Public-key encryption Is also known as asymmetric-key cryptography. It uses a key pair to encrypt and decrypt. They keys are made up of one public and one private. Both keys are mathematically associated.

https://msdn.microsoft.com/en-us/library/windows/desktop/bb427432(v=vs.85).aspx

http://searchsecurity.techtarget.com/definition/PKI

https://docs.oracle.com/cd/B10501_01/network.920/a96582/pki.htm

PCI Security Standards Council, LLC (2016). Requirements and Security Assessment Procedures Version 3.2 Wakefield, MA.

Payment Card Industry Data Security Standard (PCI DSS) Requirements and security standards.

https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf?agreement=true&time=1470830604318

National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity,

The NIST Cybersecurity Framework is a voluntary set of standards to increase cybersecurity and reduce risk to critical infrastructure.

http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

U.S House of Representatives (2014). Federal Information Security Modernization Act. Washington DC.

The Federal Information Security Modernization Act updates and expands the framework initiated in Title III of the e-Government Act of 2002, i.e., the Federal Information Security Management Act (FISMA) of 2002.

https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf

U.S House of Representatives (1999). Gramm-Leach-Bliley Act. Washington DC.

The Gramm-Leach-Bliley Act (GLBA) is the Financial Modernization Act of 1999 and sets controls for the way financial institutions handle personally identifiable information (PII) and other sensitive data.

https://www.congress.gov/106/plaws/publ102/PLAW-106publ102.pdf

U.S. House of Representatives (1996). Health Insurance Portability and Accountability Act. Washington DC.

The Health Insurance Portability and Accountability Act (HIPAA) places limits on who has access to and provides protections on all forms of health information of individuals.

https://www.congress.gov/104/plaws/publ191/PLAW-104publ191.pdf

U.S. House of Representatives (2009) Health Information Technology for Economic and Clinical Health Act. Washington DC.

The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 was enacted as part of the American Recover and Reinvestment Act (ARRA) of 2009. The purpose of the law was to encourage the implementation and "meaningful use" of health information technology.

https://www.congress.gov/111/plaws/publ5/PLAW-111publ5.pdf

http://www.hhs.gov/hipaa/for-professionals/special-topics/HITECH-act-enforcement-interim-final-rule/index.html

U.S. House of Representatives (2002). Sarbanes-Oxley Act. Washington DC.

The Sarbanes-Oxley Act of 2002 (SOX) is the Corporate and Auditing Accountability and Responsibility Act.

https://www.congress.gov/107/plaws/publ204/PLAW-107publ204.pdf

US-CERT Traffic Light Protocol

The Traffic Light Protocol was developed by US-CERT to designate sensitive information and to ensure the correct distribution of that information.

https://www.us-cert.gov/tlp

APPENDIX B GLOSSARY

Selected terms used in the publication are defined below.

Alert: Timely information about current security issues, vulnerabilities, and exploits.

Analysis: A detailed examination of data to identify malicious activity and an assessment of the identified malicious activity to existing threat information to say something greater about the data at hand.

Automated Cybersecurity Information Sharing: The exchange of data-related risks and practices relevant to increasing the security of an information system utilizing primarily machine programmed methods for receipt, analysis, dissemination, and integration.

Campaigns: In the context of cybersecurity, a campaign or attack via cyberspace that targets an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure, destroying the integrity of the data, or stealing controlled information.

Computer Security Incident: See "Incident."

Computer Security Incident Response Team (CSIRT): A capability set up for the purpose of assisting in responding to computer security-related incidents; also called a Computer Incident Response Team (CIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability).

Cyber Threat Information: Information (such as indications, tactics, techniques, procedures, behaviors, motives, adversaries, targets, vulnerabilities, courses of action, or warnings) regarding an adversary, its intentions, or actions against information technology or operational technology systems.

Cybersecurity Information: Data-related risks and practices relevant to improving the security of an information system.

Cybersecurity Information Sharing: The exchange of data-related risks and practices relevant to increasing the security of an information system.

Cybersecurity Threat: An action on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system. The term does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

Cyber Threat Indicator: Information that is necessary to describe or identify—

- malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;
- a method of defeating a security control or exploitation of a security vulnerability;
- a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;
- a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;
- malicious cyber command and control;
- the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat; or
- any combination thereof.

Defensive Measure: An action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability.

Incident: A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

Incident Handling: The mitigation of violations of security policies and recommended practices.

Incident Response: An organized approach to addressing and managing the aftermath of a security breach or attack (also known as an incident). The goal is to handle the situation in a way that limits damage and reduces recovery time and costs.

Indicator: An artifact or observable evidence that suggests that an adversary is preparing to attack, that an attack is currently underway, or that a compromise may have already occurred.

Malware: A program that is covertly inserted into another program or system with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system.

Malicious Cyber Command and Control: A method for unauthorized remote identification of, access to, or use of an information system or information that is stored on, processed by, or transiting an information system.

Malicious Reconnaissance: A method for actively probing or passively monitoring an information system for the purpose of discerning its security vulnerabilities, if such method is associated with a known or suspected cybersecurity threat.

Monitor: To acquire, identify, scan, or possess information that is stored on, processed by, or transiting an information system.

Mitigation: The act of reducing the severity, seriousness, or painfulness of security vulnerability or exposure.

Operational Analysis: Examination of any combination of threats, vulnerabilities, incidents, or practices that results in methods to protect specific data, infrastructure, or functions (for example, incident analysis, identification of specific tactics, techniques, procedures, or threat actors, etc.)

Secure Portal: A web-enabled resource providing controlled secure access to and interactions with relevant information assets (information content, applications, and business processes) to selected audiences using web-based technologies in a personalized manner.

Security Control: The management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity, and availability of an information system or its information.

Security Vulnerability: Any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

Sensitive Information: Information, the loss, misuse, or unauthorized access to or modification of, that could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

Signature: A recognizable, distinguishing pattern associated with an attack, such as a binary string in a virus or a particular set of keystrokes used to gain unauthorized access to a system.

Situational Awareness: Comprehension of information about the current and developing security posture and risks, based on information gathered, observation, analysis, and knowledge or experience.

Threat: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation through an

information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.

Threat Actor: An individual or group involved in malicious cyber activity.

Threat Source: The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally exploit a vulnerability.

Trend Analysis: Examination of data to identify any combination of broad, non-obvious, or emerging actions (for example, threat actor campaigns and intent, common vulnerabilities and configurations exploited, merging operational analytics with non-like data streams such as assessments, etc.).

Vulnerability: A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

APPENDIX C ACRONYMS

AIS	Automated Indicator Sharing
CERT	Computer Emergency Response Team
CISA	Cybersecurity Information Sharing Act
CVE	Common Vulnerabilities and Exposures
CONOPS	Concept of Operations
DHS	Department of Homeland Security
EU	European Union
GDPR	General Data Protection Regulation (Directive 95/46/EC)
HIPAA	Health Information Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health Act
IP	Internet Protocol
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
IT	Information Technology
NCCIC	National Cybersecurity & Communications Integration Center
NIS	Network and Information Security Directive (NIS)
NIST	National Institute of Standards and Technology
PCI	Payment Card Industry
PII	Personable Identifiable Information
SO	Standards Organization
STIX	Structured Threat Information eXpression
TAXII	Trusted Automated eXchange of Indicator Information
TLP	Traffic Light Protocol
TTP	Tactics, Techniques & Procedures