ISAO SO 400-1

Emerging State and Local Cybersecurity Laws and Regulations Impacting Information Sharing

Version 1.0

ISAO Standards Organization

April 20, 2020

Acknowledgements

This publication was developed by the Information Sharing and Analysis Organization Standards Organization (ISAO SO) with representatives from the private, professional, and government communities in an ongoing effort to produce a unified voluntary set of guidelines 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, UTSA Center for Infrastructure Assurance and Security

Jeremy J. West

ISAO SO – Director of Lifecycle Development

UTSA Center for Infrastructure Assurance and Security

Working Group Four— Privacy and Security

David Turetsky	Norma Krayem	Carl Anderson
Professor of Practice	*Sr. Policy Advisor & Chair*	*Chief Legal Officer*
University of Albany	*Holland & Knight LLP*	*HITRUST*

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:

Stuart Gerson, Carl Anderson, Betsi McGrath, Suzanne Rutkoski, Meagan Stifle, Jay Taylor, and Patrick O'Brien.

Special thanks from the working group members and the ISAO SO to Elizabeth Doerr for her research and essential contribution to this document. The authors would also like to thank the ISAO SO advisors and staff who provided support and guidance in the development of this document: Julina Macy and Allen Screffler.

Table of Contents

Revision Updates

Item	Version	Description	Date
	V 0.5	RFC Version 0.5	15 November, 2019
	V. 0.7	Final Review	13 April, 2020
	V 1.0	Final Published Version	20 April, 2020

1 EXECUTIVE SUMMARY STATE LAWS

An Information Sharing and Analysis Organization (ISAO) is any group of individuals or organizations established for purposes of collecting, analyzing and disseminating cyber or relevant information in order to prevent, detect, mitigate, and recover from risks, events or incidents against the confidentiality, integrity, availability and reliability of information and systems.[1]

Information Sharing and Analysis Centers (ISACs), a type of ISAO, provide central resources for gathering information on cyber threats. Historically, many ISACs have focused on critical infrastructure sectors. ISAOs may share information exclusively in one sector, among similar sectors, or between the private and public sectors.

ISAOs and similar organizations can be a critical resource in providing cyber threat information (CTI) and deterrence and resilience support to states and localities. In connection with such activities, parties must be aware of the fact that state and local laws have the potential to affect both service and compliance.

The relevance and applicability of these laws varies based on the terms of the law and the promulgating jurisdiction's reach. Relevance and applicability will also vary based on the location of an ISAO, the nature and experience of its members, and the manner in which the ISAO operates. The content of these state and local laws might discourage or encourage information sharing, or otherwise influence ISAOs operational choices. It is important, therefore, for an ISAO to understand what types of state and local laws might be relevant to their general operations, and to take steps to become aware of the specific provisions of such laws and any incentives or restrictions that they impose. In that this is a dynamic field, such provisions also should be monitored periodically. For these reasons ISAOs should conduct active research and consider contributing, consistent with their resources, to the writing or revision of any legislation or regulation that directly or indirectly affects their specific area of focus. This could help ensure legislation is effective, has no unintended impacts, and also may educate the legislators about their needs.

It is generally understood that ISAOs are established to collect and share various forms of threat vector and cybersecurity risk information, along with compliance and other effective practices. This type of information could include intelligence about such things as breaches, hacks, exploits and vulnerabilities, but generally not Personally Identifiable Information ("PII"), or information that can be used to identify specific individuals, such as Social Security numbers, addresses, or drivers' license data. Often, much of an ISAOs' attention to legal and policy developments, pertaining to information sharing, has understandably been drawn to the federal and international levels. At the federal level, attention has often focused on Executive Orders relevant to information sharing

[1] ISAO SO (nd). Frequently Asked Questions. https://www.isao.org/faq/ retrieved October 30, 2019.

such as Executive Order 13691, *Promoting Private Sector Cybersecurity Information Sharing* (February 13, 2015) and on the passage and implementation of, and continuing developments related to, the *2015 Cybersecurity Information Sharing Act* ("CISA"). Since becoming law, CISA has generated public comment and discussion, and has undergone various phases of implementation and refinement in its administration.[2] Internationally, much of the focus has been on the strong privacy laws being implemented in Europe and elsewhere, particularly the European Union's General Data Protection Regulation (GDPR).[3]

There has been far less focus on how state and local laws, or proposals directly or indirectly, affect ISAOs. Even if there is no direct or indirect effect, they might still be of relevance and may inhibit or encourage information sharing or create additional opportunities for ISAOs.

ISAOs and others have been compelled by developments, however, to focus attention on state and local legislation and regulation, particularly with respect to the communication and retention of PII. Every state and territory now has a law governing breach notification and there is significant variance among them. Thus, breach subject reporting requirements aside, the sorts of information that a state or locality might benefit receiving from or sharing with an ISAO can also vary.

Of increasing significance at the sub-Federal level is the fact that a number of states have enacted, or are considering, legislation modeled upon the GDPR. Chief among these is California's Consumer Privacy Act, which became effective January 1, 2020. Nevada has passed a similar law and Illinois has promulgated a privacy statute focusing on biometric data. Although the terms of emergent state and local law is yet to be determined, the importance of this evolving legal array is highly significant. For example, some states are considering, or are in the process of passing and implementing, laws that pertain to Personally Identifiable Information (PII). Although these laws have not defined PII at this time, most ISAOs intend to and successfully avoid collecting any such PII, other than about their own employees.

---

[2] The Cybersecurity Information Sharing Act (CISA) is a federal law designed to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats. https://www.congress.gov/bill/114th-congress/senate-bill/754

[3] GDPR is a European Union (EU) regulation on data protection and privacy, protecting all individuals within the EU. Its reach further includes citizens of other countries (such as the United States) who share their personal information with European businesses or potentially even businesses operating from abroad who gather information from those in the EU. GDPR came into effect May 25, 2018 and violations carry potentially severe penalties. Generally, the GDPR requires that companies be transparent about what personal data they are collecting, what they are using customer's data for, with whom they are sharing it, allows customers to access and make certain decisions about personal data pertaining to them, and emphasizes the need to obtain consent before using data or disclosing it to a third party and to allow persons the right to be "forgotten." While a matter of importance to many American companies, the significance to ISAO members lies in the fact that much of developing U.S. law is being modeled upon the GDPR.

A number of states are looking to provide incentives for entities to engage in voluntary information sharing, as CISA sought to do at the federal level. Finally, some cities and other jurisdictions are beginning to develop sharing centers or "hubs," which collect, share, and disseminate information. *See, for example,* Section 3 below (discussion of New York City). These sharing centers could become resources for ISAOs to take advantage of and help them better serve their members. In view of the fact that some state and city offices have been subject to hacks and exploits that have interrupted various services and facilities and others have been forced to succumb to costly ransomware demands, the desire for cooperative efforts involving ISAOs ought to be increasing.

The following sections highlight examples of legislative developments for ISAOs to consider. It is not intended to be comprehensive, exhaustive, or to provide legal advice. As previously mentioned, information reporting and sharing is a dynamic and changing environment which any entity must monitor.

2 STATE LAWS

As noted above, many state and local legislators, as well as regulators and other stakeholders, have used the laws of other nations as models in implementing strong privacy legislation. The California Consumer Privacy Act is a prime example of this activity, but as noted, every state and U.S. territory has laws and regulations governing data breaches.

2.1 GDPR AS AN INFLUENCE ON THE STATES

Many state laws focus on privacy rights and not information sharing. The wide applicability of these laws affect and can be applied to any entity that acquires or shares PII. This may be relevant to an ISAO in its capacity as an employer or recipient of certain financial information, but it can also be relevant to an ISAO if it receives personal data from its members, perhaps for sharing. That being said, ISAOs typically do not intend to, nor do they, collect personal data or PII for sharing (since it typically is not necessary to satisfy their purposes). In the event, however, that an ISAO does collect personal information or data about its employees or about individuals related to its members, it is critical that it be aware of and consider these privacy laws.

As is mentioned above, the prime, though far from the only, example of emergent state law is California's privacy law originally passed in 2018. It is known as the *California Consumer Privacy Act of 2018* and is sometimes referred to as the CCPA or even as "GDPR Lite."[4] The law's purpose is to "…ensure the privacy of Californians' personal information through various consumer rights. Consumer rights established … include

[4] Kari Paul. (December 30, 2019 Monday). California's groundbreaking privacy law takes effect in January. What does it do? The Guardian. https://www.theguardian.com/us-news/2019/dec/30/california-consumer-privacy-act-what-does-it-do

the right to know whether a person's personal information is being collected and whether it is being sold; the right to have businesses delete a person's personal information; the right to opt-out of or opt-in to the sale of a person's personal information."[5] The breach of any of these provisions could result in a business being required to pay damages to a customer whose rights are violated, injunctive or declaratory relief, or other damages the court deems proper.[6] The Act was introduced and passed quickly to derail a citizens' ballot initiative that many in industry thought could be even more onerous that otherwise would have been included on California's November 2018 election ballot. The sponsors of the ballot initiative agreed to take a step back if the legislation was passed.[7] This does not necessarily preclude future ballot initiatives after implementation of the CCPA.

There have been numerous proposals in other states to take on some of the same subjects as the California privacy law. Nevada, as noted, followed suit. In July 2019, New York passed the Stop Hacks and Improve Electronic Data Security Act (SHIELD Act), which expands the definition of PII for New York residents to include biometric data, username or email address in combination of password or security questions, and account numbers, credit or debit card, if they can be used exclusively to access accounts.[8] In the past, there has been uncertainty if exfiltration of PII or accessing the data constitutes a breach. In the case of ransomware, some attackers only access the data without acquiring it. Under the SHIELD Act, New York joins a few other states that consider having access to the data as constituting a breach.[9] As of October 23, 2019, the expanded definition of PII took effect and the law requires notification of impacted residents, state, regulators, and under certain conditions consumer reporting agencies.[10] In addition, businesses are still required to notify the New York Attorney General, New York Secretary of State, and the Division of the State Police in the case of a breach.

In several states, legislation often requires that breach notification be provided to the state attorney general and specifies notification timetables, available fines, etc. A court may also impose penalties on a business in addition to the payment of attorney's fees if the customer prevails in their suit.

---

[5] See: California Consumer Privacy Act of 2018. Assembly Committee on Appropriations, Lorena Gonzalez Fletcher, chair. SB 112. Date of Hearing August 29, 2019.

[6] See § 1798.150 of the California Consumer Privacy Act

[7] https://www.akingump.com/en/news-insights/california-passes-landmark-consumer-privacy-act-what-it-means.html

[8] See: https://www.offitkurman.com/blog/2019/08/18/stop-hacks-and-improve-electronic-data-security-act-shield-act/

[9] See: https://www.varonis.com/blog/nys-shield-law-updates-to-pii-data-security-and-breach-notification/

[10] See: https://www.insideprivacy.com/data-security/new-york-passes-new-data-security-and-breach-notification-requirements/

Some of these emergent state laws allow for private rights of action without any compliance safe harbor and, often, without the need for plaintiffs to show economic loss or other material damages. The SHIELD Act does not provide a private action, instead the state attorney general may bring actions to enjoin violations and obtain civil penalties.[11]

While these laws do not single out ISAOs or information sharing specifically, they are important to note. They represent a baseline of actual or potential state privacy legislation that ISAOs should be aware of as more states are considering or are implementing similar privacy laws of general applicability. By understanding what a particular state's privacy law says and being aware of the repercussions for violations, ISAOs will have an additional reason to avoid collecting such personal data. In the event ISAOs do collect any such data, they need to maintain an active compliance program to prevent unauthorized disclosures and avoid legal liability. This need is magnified if ISAO members operate in multiple states or internationally. And, if an ISAO decides that it somehow needs to gather and potentially disseminate PII, it should consider purchasing cyber risk insurance.

2.1.1 INFORMATION SHARING OFFICERS

GDPR has not only influenced state privacy laws, but its influence can also be seen in changes to the roles of certain state officers, such as state Chief Information Officers (CIOs). GDPR defines the role of Data Protection Officers (DPOs) and mandates that they be heavily involved in data collection and dissemination of information. CIOs are increasingly expanding their responsibilities in some of these areas.[12] Aspects of a DPO's role (such as being a business's single point of contact who is responsible for every stage of data collection) will likely be absorbed into the responsibilities and job descriptions of CIOs in some states.[13] This may give more state CIOs a clear role in information sharing. In turn, this can create opportunities for ISAOs to partner with states to provide and receive more information for the benefit of members as well as provide insight into how states view information sharing best practices and concerns.

The state of Oregon, for example, is in the process of creating its own "Cybersecurity Center for Excellence," which will act as a ISAC.[14] The state CIO's job within the

---

[11] See: https://datamatters.sidley.com/new-york-enacts-stricter-data-cybersecurity-laws/

[12] The role of state chief information officers is not a new idea in the United States. In fact, its prevalence led to creation of the National Association of State Chief Information Officers ("NASCIO") in 1969 (see: https://www.nascio.org/). Later, state chief information security officers (CISOs) became more prevalent too, and they often are included in NASCIO. Increasingly, however, new state laws are creating additional responsibilities for CIOs.

[13] Section 4, Article 37 of GDPR describes the role of DPOs. This officer is the single point of contact within a business or an organization involved with data processing tasks. Many CIOs will take on this role.

[14] See: https://www.pdx.edu/cps/sites/www.pdx.edu.cps/files/Cybersecurity%20Needs%20Assessment%20Final%20Draft.pdf

Cybersecurity Center for Excellence entails coordinating information sharing relating to any cybersecurity risks. The CIO will further act as a liaison with the National Cybersecurity and Communications Integration Center (NCCIC) in the United States Department of Homeland Security, as well as other federal agencies, and other public and private entities.

Once the CIO receives any relevant information, including threat information, he or she may disseminate the information to the appropriate sources including other ISAOs or ISACs, Multi-State ISAC (MS-ISAC), the federal government, law enforcement agencies, public utilities, and private industry.

The changing roles of state CIOs concerning information sharing and privacy, as seen in Oregon, may be useful for ISAOs to monitor and learn about. The broadening of state CIO roles may create opportunities and precedents.

2.2 INCENTIVES

Some states have realized the importance of information sharing with, in addition to the federal government, their own state entities. This has led some state governments to create incentives through legislation to encourage information sharing. Among such incentives are "safe harbors" that can insulate a defendant from some or all liability in enforcement actions or litigation. ISAOs promote information sharing by working with private and often public sector stakeholders to create best practices and share cyber threat information on a voluntary basis.[15] State laws do not usually mandate that companies participate in information sharing with ISAOs, but ISAOs can potentially use state support as another mechanism to promote the services that ISAOs can provide.

For example, Ohio enacted Senate Bill 220, also known as the Ohio Data Protection Act (DPA)[16], which took effect in November 2018. This law's purpose is to "provide a legal safe harbor to covered entities that implement and maintain a specified cybersecurity program."[17] The law states:

> Sec. 1354.02. (A) A covered entity seeking an affirmative defense under sections 1354.01 to 1354.05 of the Revised Code shall do one of the following: (1) Create, maintain, and comply with a written cybersecurity program that contains administrative, technical, and

[15] See: https://www.isao.org/about/

[16] See: https://www.jdsupra.com/legalnews/ohio-s-data-protection-act-27275/

[17] A "covered entity" under this statute includes any business that accesses, maintains, communicates, or processes personal information or restricted information in or through one or more systems, networks, or services located in or outside this state. See full Bill Text here: https://www.legislature.ohio.gov/legislation/legislation-summary?id=GA132-SB-220

> physical safeguards for the protection of personal information and that reasonably conforms to an industry recognized cybersecurity framework, as described in section 1354.03 of the Revised Code; or (2) Create, maintain, and comply with a written cybersecurity program that contains administrative, technical, and physical safeguards for the protection of both personal information and restricted information and that reasonably conforms to an industry recognized cybersecurity framework, as described in section 1354.03 of the Revised Code. (B) A covered entity's cybersecurity program shall be designed to do all of the following with respect to the information described in division (A)(1) or (2) of this section, as applicable : (1) Protect the security and confidentiality of the information; (2) Protect against any anticipated threats or hazards to the security or integrity of the information; (3) Protect against unauthorized access to and acquisition of the information that is likely to result in a material risk of identity theft or other fraud to the individual to whom the information relates.[18]

In essence, under the Ohio law, the businesses who choose to implement written cybersecurity programs and best practices may claim an affirmative defense that can free them from liability if there is a breach in their system and customer PII is compromised. DPA is intended to provide an *incentive* to encourage businesses to achieve a higher level of cybersecurity through voluntary action.[19] DPA does not, nor is it intended to, create minimum cybersecurity standards that must be achieved,[20] nor should it be read to impose liability upon businesses. New York's SHIELD Act contains similar compliance provisions as DPA; however, it does not provide an "expressed affirmative defense against state tort actions for entities with compliance information security programs."[21]

This Ohio law does not require companies to participate in information sharing. However, the possibility of additional liability protections may sway some companies to decide to participate. ISAOs could consider reaching out to companies who fall within

[18] See: https://www.legislature.ohio.gov/legislation/legislation-summary?id=GA132-SB-220

[19] The affirmative defense is to a cause of action sounding in tort (negligence, invasion of privacy, etc.), including allegations of a data breach resulting from a failure to implement reasonable information security controls.

[20] In addition to certain initiatives like Ohio's legal safe harbor law, there are other state initiatives that may be sector specific. New York's financial institution's cybersecurity law is a prime example. Beginning September 4, 2018; banks, insurance companies, and other financial service institutions that are regulated by DFS are required to be in compliance with new provisions of cybersecurity regulations. These provisions require a covered entity to establish written incident response plans, comply with breach notification policies, have policies in place concerning the disclosure of information to third parties, and comply with data retention policies. See more at: https://www.dfs.ny.gov/about/press/pr1808081.htm

[21] See: https://datamatters.sidley.com/new-york-enacts-stricter-data-cybersecurity-laws/

the definition of a covered entity and invite and encourage new members to join by using the additional liability protections provided by the bill as an incentive. Companies may see these additional liability protections as reason to engage in information sharing and as a potentially valuable addition to written cybersecurity plans or policies, thereby showing the state that they are taking important and valuable steps to guard against data or privacy breaches.

Additionally, ISAOs located within Ohio might want to consider whether they also wish to have written cyber policies and measures in place, thereby allowing an ISAO itself to qualify for the affirmative defense. By having these policies and programs, the ISAO might have an additional defense available if ever needed in an Ohio action against them.

2.3 GENERAL LEGISLATION CAN BE OF RELEVANCE

Sometimes an ISAO may need to look particularly closely at the jurisdictions most relevant to it to uncover relevant laws or developments. Potentially relevant provisions may be buried in laws with a purpose broader than cybersecurity or privacy.

An example is Virginia's Budget Bill (Bill 50002, enacted June 2018). This bill includes a provision that provides funding to state police to develop and operate cybersecurity and management tools to address any risks, threats, and/or vulnerabilities to data that are outside of the scope of their memorandum of understanding (MOU) with the Virginia Information Technologies Agency (VITA). The state police collect this information and report it to VITA, who in turn actively participates with and shares information with the Multi-State Information Sharing and Analysis Center (MS-ISAC).[22]

Furthermore, several states have implemented general laws that protect critical infrastructure as well as the PII of their citizens.[23] The texts of these laws guide state entities to follow Emergency Response Plans (EPRs) which have already been implemented. These governmentally mandated regimes typically require their components to detail training and set forth Business Continuity Plans (BCPs) or Incident Response Plans (IRPs) specifically written to address data breaches, including who affected entities should report to, when they should report, how the information should

[22] Virginia Information Technology Agency is Virginia's consolidated information technology organization. The Commonwealth Security and Risk Management (CSRM) COV Security Outreach & Information Sharing Team actively participates with MS-ISAC, Local, State (VA Fusion Center and Commonwealth Preparedness Working Group), and Federal Law Enforcement (FBI), and multiple Commonwealth of Virginia Information/Infrastructure Security groups.

[23] States that have begun enacting broader legislation include, but are not limited to: Arkansas (*regarding emergency powers of bank commissioner, relating to cyberattacks and cybersecurity breaches*); Colorado (*this law concerns the authority of the Joint Technology Committee; regarding data privacy and cybersecurity within state agencies and may coordinate with the Colorado cybersecurity committee*), Maryland (*making proposed appropriations within the state Budget Bill*). See more at: http://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2017.aspx

be reported, etc. The state of Iowa, for example, not only has a state level information security office, but also reports any data breaches to MS-ISAC. As noted, the breach notification laws of all 50 states and U.S. territories vary significantly among themselves, but all impose on private data holder's notification and response requirements. These laws provide guidance with respect to reporting and, in some cases, best practices. Generally, most ISAOs will have no need for sharing PII and do not do so. ISAOs should consider obtaining additional guidance on relevant state statutes and regulations, highlighting private or state entities who receive funding to perform cybersecurity related activities. These laws may open the door for ISAOs to help identify and serve potential recipients who might wish to participate in sharing and becoming ISAO members.

3 LOCAL LAWS

Municipalities typically have not chosen to implement local laws that would directly regulate or affect ISAOs. This does not necessarily mean that municipalities do not take cybersecurity precautions. New York City, for example, is in the forefront of implementing new cybersecurity policies that may have a major impact on privacy and cybersecurity within its jurisdiction.

The New York City Economic Development Corporation (NYCEDC) unveiled its plan to transform New York City into the next cybersecurity "hub," to be known as "Cyber NYC." A main driver behind this initiative is the goal of creating thousands of jobs in the cybersecurity field as part of New York Works Plan."[24] The City's Chief Information Officer and head of NYC Cyber Command stated, "EDC's Cyber NYC initiative establishes a partnership positioned to powerfully combine expertise in technology and business innovation, education, job growth, and community collaboration to help fuel our City's forward progress in the rapidly growing industry of cybersecurity."

They will try to accomplish this initiative in three different ways. The first is by opening a Global Cyber Center to bring together an international community of corporations, investors, and startups. This will enable them to collaborate and share information on an international scale.[25] The second method is to develop a workforce through an applied learning initiative. For this, the city has selected local colleges to pick from and train students through the use of a "Cyber Boot Camp" and other degree and certificate initiatives programs. The program initiative anticipates that students from these programs will be hired in significant numbers by cybersecurity companies and or firms seeking cybersecurity expertise in the area. The final approach the NYCEDC is taking is

[24] See: https://newyorkworks.cityofnewyork.us/?ddownload=1263 The New York Works plan is a series of initiatives to create 100,000 jobs within New York City, with the de Blasio administration investing heavily in the cybersecurity industry as well as other fields.

[25] See: https://www.nycedc.com/press-release/nycedc-unveils-global-cyber-center-innovation-hub-and-new-talent-pipelines-secure-nyc#_ftn1

See: https://www.law.com/legaltechnews/2018/10/09/3-ways-nyc-is-looking-to-change-u-s-privacy-and-cybersecurity/?slreturn=20180919132708

by working with industry leaders (such as Goldman Sachs and Facebook) to collaborate and have those firms work on advisory boards, hire students, and advise the overall direction of the initiative training provided.

Initiatives, such as from the NYCEDC, provide potential partnership opportunities for ISAOs in various ways. An ISAO might consider joining the initiative as a business who could hire out of the boot camp program, which might be helpful in building a trained workforce. An ISAO might also find opportunities for sharing or obtaining new members in connection with the initiative.[26]

More generally, the public has been made aware that municipalities and the states that empower them have been subject to hacking of public utilities and health facilities. Most concerning, these organizations have been compelled to pay a ransom to de-encrypt and regain access to their data, which have been attacked by both individuals and state sponsored actors. These are the same types of threats that the private sector is exposed to and it is clear that information sharing would benefit all concerned parties. Such sharing should be encouraged and exploited by ISAOs and their members.

3.1 GEOGRAPHICAL SHARING

While some local laws or initiatives might not be specific to ISAOs, it is still helpful to understand other municipal efforts to encourage information sharing. One increasing trend is for municipalities and other governmental entities at similar levels to engage in public-private partnerships that include information sharing. The Federal Bureau of Investigation (FBI) created the InfraGard Program, which fosters collaboration and information sharing between public and private partnerships across the United States. Active chapters exist in every state and U.S. territory. (https://www.infragard.org/) This creates additional collaborative opportunities for ISAOs that can benefit their members. It can help them better to understand risk, threat, and vulnerability information, and targets and enables ISAOs to become more involved in relevant geographic communities. ISAOs will want to watch specifically for the establishment of geographically focused information sharing centers. These centers could be productive ISAO partners, magnifying the ability of both ISAOs and governments alike to gain actionable threat and vulnerability information as well as tested best practices to manage or reduce risk. These partnerships can also be equipped to disseminate actionable information efficiently to those entities that would particularly benefit from it.

For example, Los Angeles is at the forefront of this kind of sharing. The Los Angeles Cyber Lab, a cybersecurity risk, threat, and vulnerability sharing group, shares cyber threat intelligence with area public and private organizations, and citizens. This Lab is led by a Board of Advisors including the Mayor of Los Angeles as well as top businesses and government officials. This Lab begins by sharing information generated from its Integrated Security Operations Center (ISOC). The Lab allows members (business and private citizens of the greater Los Angeles area and surrounding cities

and counties) to send any compromising cyber information they know of to the Lab. Then, at no cost, the Lab communicates if there are any active phishing schemes, ransomware, or data stealing apps. Additionally, it allows its members to share data with organizations for both public and private exchange. The Cyber Lab states that it is the first public entity to implement real time information sharing capabilities.[27]

4 CONCLUSION

There is a significant and increasing amount of legislative and regulatory activity at the state and local level, some intended to impact information sharing directly, and some with broader intentions but which still might be relevant to information sharing entities, such as ISAOs. Recent events affecting state and local services and interests magnify the utility of information sharing between the public and private sectors. To be effective partners in such activities, it is incumbent upon ISAOs to be cognizant of relevant state and local laws and regulations. The laws, initiatives, and resources described in this document are in various stages of enactment or enforcement. ISAOs should continually review individual laws or initiatives as they are dynamic and subject to change. Collectively, these state and local laws and policy initiatives identify a landscape that are important for ISAOs to understand and monitor.

[27] See: https://www.lacyberlab.org/what-los-angeles-cyber-lab and See Also: https://www.smartresilient.com/la-cyber-lab-gets-funding-announces-expansion

APPENDIX A - GLOSSARY

Selected terms used in the publication are defined below.

Actor: See threat actor.

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.[28]

Attack: attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.[29]

Authentication: provision of assurance that a claimed characteristic of an entity is correct.[30]

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.[31]

Availability: property of being accessible and usable on demand by an authorized entity.[32]

Center for Infrastructure Assurance and Security (CIAS): is developing the world's foremost center for multidisciplinary education and development of operational capabilities in the areas of infrastructure assurance and security. The CIAS is a part of The University of Texas at San Antonio (UTSA).

Confidentiality: property that information is not made available or disclosed to unauthorized individuals, entities, or processes.[33]

Control: measure that is modifying risk.[34]

---

[28] ISAO 100-1. (2016, October 14). *Introduction to Information Sharing.* Retrieved from ISAO Support Organization: https://www.isao.org/wp-content/uploads/2016/10/ISAO-100-1-Introduction-to-ISAO-v1-01_Final.pd

[29] ISO/IEC 27000:2018(en). Information technology — Security techniques — Information security management systems — Overview and vocabulary. https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en. Retrieved: October 30, 2019

[30] Ibid

[31] ISAO 100-1, 2016

[32] ISO/IEC 27000:2018(en)

[33] Ibid

[34] ISO/IEC 27000:2018(en)

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.[35]

Cyber Threat Information (CTI): 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.[36]

Cybersecurity information sharing: the exchange of data-related risks and practices relevant to increasing the security of an information system.[37]

Event: occurrence or change of a particular set of circumstances.[38]

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.[39]

Incident: a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.[40]

Indicator: a technical artifact or observable that suggests an attack is imminent or is currently underway, or that a compromise may have already occurred.[41]

---

[35] ISAO 300-1. (2016, October 14). Introduction to Information Sharing. Retrieved January 23, 2019, from ISAO Standards Organization: https://www.isao.org/storage/2016/10/ISAO-300-1-Introduction-to-Information-Sharing-v1-01_Final.pdf

[36] Ibid

[37] ISAO 100-1, 2016

[38] ISO/IEC 27000:2018(en)

[39] ISAO 300-1

[40] ISAO 100-1

[41] NIST. (2016, October). Guide to Cyber Threat Information Sharing. NIST Special Publication 800-150. doi:http://dx.doi.org/10.6028/NIST.SP.800-150

Information security: preservation of confidentiality, integrity, and availability of information.[42]

Information Sharing and Analysis Organization (ISAO): an ISAO is any group of individuals or organizations established for purposes of collecting, analyzing and disseminating cyber or relevant information in order to prevent, detect, mitigate, and recover from risks, events or incidents against the confidentiality, integrity, availability and reliability of information and systems.[43]

Integrity: property of accuracy and completeness.[44]

Jurisdiction: The geographic area over which authority extends; legal authority; the authority to hear and determine causes of action.

Mitigation: the act of reducing the severity, seriousness, or painfulness of security vulnerability or exposure.[45]

Monitor: to acquire, identify, scan, or possess information that is stored on, processed by, or transiting an information system.[46]

Multi-State ISAC: an organization whose mission is to improve the overall cyber security posture of state, local, tribal and territorial governments.

Policy: intentions and direction of an organization, as formally expressed by its top management.[47]

Process: set of interrelated or interacting activities which transforms inputs into outputs.[48]

Requirement: a need or expectation that is stated, generally implied or obligatory.[49]

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.[50]

Security vulnerability: any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.[51]

---

[42] ISO/IEC 27000:2018(en)
[43] ISAO SO (nd)
[44] ISO/IEC 27000:2018(en)
[45] ISAO 300-1
[46] Ibid
[47] ISO/IEC 27000:2018(en)
[48] Ibid
[49] Ibid
[50] ISAO SO 300-1
[51] Ibid

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.[52]

Stakeholders: a person, group, or organization that has interest or concern in an organization.

Threat actor: an individual or a group posing a threat.

Threat information: any information related to a threat that might help an organization protect itself against a threat or detect the activities of an actor. Major types of threat information include indicators, TTPs, security alerts, threat intelligence reports, and tool configurations.[53]

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.[54]

Training: NIST 800-84 defines training as “informing personnel of their roles and responsibilities within a particular IT plan and teaching them skills related to those roles and responsibilities, thereby preparing them for participation in exercises, tests, and actual emergency situations related to the IT plan”.[55]

Vulnerability: a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.[56]

Working group: a committee or group appointed to study and report on a particular question and make recommendations based on its findings.

[52] NIST 800-151

[53] Ibid

[54] NIST 800-151

[55] NIST SP 800-84 – September 2006 - Tim Grance (NIST), Tamara Nolan (BAH), Kristin Burke (BAH), Rich Dudley (BAH), Gregory White (UTSA), Travis Good (UTSA) - Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities. - https://csrc.nist.gov/publications/detail/sp/800-84/final

[56] ISAO 300-1

APPENDIX B - ACRONYMS

BCP	Business Continuity Plans
CIO	Chief Information Officer
CISA	Cybersecurity Information Sharing Act
CTI	Cyber Threat Information
DPA	Ohio Data Protection Act
DPO	Data Protection Officers
ERP	Emergency Response Plan
EU	European Union
FBI	Federal Bureau of Investigation
GDPR	General Data Protection Regulation
IRP	Incident Response Plan
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
ISAO SO	Information Sharing and Analysis Organization Standards Organization
ISO	International Standards Organization
ISOC	Integrated Security Operations Center
IT	Information Technology
MS-ISAC	Multi-State Information Sharing and Analysis Center
NCCIC	National Cybersecurity and Communications Integration Center
NIST	National institute of Standards and Technology
NYCEDC	New York City Economic Development Corporation
PII	Personally Identifiable Information
SHIELD Act	Stop Hacks and Improve Electronic Data Security Act
TTPs	Tools, Techniques, and Procedures