ISAO 600-1

A Framework for State-Level Information Sharing and Analysis Organizations

V1.0

ISAO Standards Organization
June 11, 2018

Acknowledgments

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, PhD
ISAO SO—Executive Director
Director, Center for Infrastructure Assurance and Security, UTSA

Allen Shreffler
ISAO SO—Deputy Director
Senior Consultant, LMI

Tommy McDowell
Director
Retail Cyber Intelligence Sharing Center

Working Group 6—ISAO Government Relations

Mark Boggis
Cybersecurity Policy Solutions, LLC
Board Member, Cyber Resilience Institute

Douglas M. DePeppe
Board President, Cyber Resilience Institute
Founder, eosEdge Legal

The ISAO SO leadership would also like to acknowledge those individuals who contributed significantly to the development of these guidelines:

Hon. Stuart M. Gerson, Epstein Becker & Green, P.C.; David Halla, Senior Professional, Johns Hopkins University Applied Physics Laboratory; Isaac Janak, Cybersecurity Program Manager, Commonwealth of Virginia; Elizabeth McGrath, the MITRE Corporation; Nick Sturgeon, Security Operations Center Director, Pondurance, LLC, Vice President, Cyber Leadership Alliance

Special thanks from the authors go to the ISAO SO advisors and staff who provided amazing support and guidance in the development of this document: Josef Klein, James Navarro, and Jeremy West.

This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award No. 2015-PD-128-000001.

Table of Contents

Figures

Tables

Revision Updates

Item	Version	Description	Date
1	V1.0	Initial version	6/11/2018

1 INTRODUCTION

In February 2015, then-President Barack Obama signed Executive Order 13691, describing the critical need for cybersecurity information sharing and strongly encouraging the formation and development of Information Sharing and Analysis Organizations (ISAOs).

An ISAO is “any entity or collaboration created or employed by public- or private-sector organizations for the purposes of—

- gathering and analyzing critical cyber and related information in order better to understand security problems and interdependencies related to cyber systems, so as to ensure their availability, integrity, and reliability;
- communicating or disclosing critical cyber and related information to help prevent, detect, mitigate, or recover from, the effects of an interference, compromise, or incapacitation of critical cyber systems; and
- voluntarily disseminating critical cyber and related information to its members; federal, state, and local governments; or any other entities that may be of assistance in carrying out the purposes specified above.”

In the three full years since the executive order was issued, a significant number of public and private organizations have responded to this national imperative and have begun to share cybersecurity threat information, improve collective understanding of the threat environment, increase security and preparedness, and collaborate on best practices. This cohesive public and private community-based cooperation has enabled ISAO members and partners to become stronger, safer, and more resilient. Information sharing at the state, local, tribal, and territorial (SLTT) level has similar manifest value and should be targeted for expansion. Many private and governmental entities, however, have not yet undertaken effective cybersecurity threat information sharing, some out of reluctance, others for lack of knowledge. Accordingly, this primer provides a resource for facilitating effective cybersecurity sharing and analysis within states for those already participating in the arena and for those who should be. The matters presented include the following:

- A business case for SLTT information sharing
- The identification of state-level stakeholders
- Potential organizational models for the governance and administration of a state-level information-sharing program
- Discussion of various relevant state-level services and capabilities
- A framework for state-level partnerships and coordination between states
- Identification of potential sources of funding
- Public and private partnership mutual advantages in collaboration.

2 BUSINESS CASE: THE VALUE OF STATE-LEVEL INFORMATION SHARING

The cyber-threat landscape is both complex and still rapidly evolving. Current dangers include “Zero Day” exploits, malware, distributed denial of service, extortion, ransomware, and social engineering. Targets include critical infrastructure, universities, banking, health care, public utilities, election facilities and machinery, supply chains, cloud services, and Internet of Things (IoT) devices, among others. Threat actors range from hacktivists to nation states and their agents seeking strategic advantage, affecting political processes, and generally conducting furtive cyber warfare to criminals seeking financial gain. Each of these threats poses a significant risk to the core interests of every state and its dependent citizenry, particularly with respect to the vulnerability of the services its citizens depend upon.

In this challenging environment, state governments have a legal and practical responsibility to lead the development, delivery, and maintenance of cybersecurity programs that ensure the public safety and welfare of their residents and the security state facilities and minimize threats to information resources. At the same time, it is demonstrably clear that private-sector entities, which are directly affected by cyber threats, may have useful capabilities and experience that overburdened public bureaucracies lack in sufficiency. Thus, information sharing is a critical component and multiplier of meaningful cyber awareness and response.

Executed effectively, a state-wide information-sharing initiative can provide stakeholders with enhanced awareness of emerging and specific threats as well as best practices to mitigate or reduce risk. Many state initiatives also envision economic development opportunities arising from effective information-sharing environments.

Through multi-state information sharing and analysis centers (MS-ISACs) and fusion centers, the states provide and receive cybersecurity information from other states, the federal government, and private-sector partners. Within some states, however, information sharing is less mature, lacking both sufficient structure and effectiveness. Enacting and executing an information-sharing strategy raises the collective security of state and local agencies. It provides a foundation for a comprehensive state approach to cybersecurity; improves coordination and awareness; increases and improves state operations; enhances safety, emergency management, and delivery of services; safeguards data-driven government; and helps to preserve critical infrastructure and advance the state and local economy. Information sharing also benefits the private sector, both in terms of gaining information to strengthen security in the present and advancing relationships that produce benefits in the future, especially in what likely will prove times of crisis. Recent events suggest that in many cases, both government and the private sector share the same enemies and threats.

3 STATE-LEVEL SERVICES AND CAPABILITIES

3.1 INTRODUCTION

If states were to conduct an inventory of information sharing and analysis services and capabilities as they relate to cybersecurity, many of them would find that they already have a number of these in place. However, the maturity levels for these services and capabilities and the degree that they are implemented will vary greatly from state to state. One of the values that a state-level ISAO can realize is the ability to centralize and streamline information sharing and analysis services and capabilities that are being used. Considering the basic ISAO services and capabilities, we start with a few basic definitions. First, a service is defined as a task, process, or product that an ISAO provides to its members. A capability is a task or process that the ISAO can perform for internal support or operational necessity. A capability is not necessarily a service, but a service is always a capability. For example, an ISAO might have email as an internal capability but choose not to offer email accounts as a service to its membership. ISAO publication 100-2 provided a comprehensive list of ISAO services and capabilities, which also are located in Appendix A. These services and capabilities were categorized into three levels: Foundational, Advanced, and Unique. Foundational services and capabilities have been further defined in an upcoming publication by the ISAO-SO Services and Capabilities Working Group. One of the more difficult steps for a state-level ISAO is choosing which services and capabilities to implement. There are several factors to consider when choosing which to deploy: cost, system administration support, upkeep, technical proficiency, and personnel/staff.

3.2 FOUNDATIONAL SERVICES AND CAPABILITIES

As mentioned above, ISAO 100-2 introduced a list of ISAO services and capabilities. It stated that “foundational services and capabilities are generally considered baseline services for most ISAOs, but are established based on the needs of its members. They might include using a standard method to send and receive cyber threat intelligence, vetting members (a trust capability), and storing cybersecurity information, to name a few. The first group of services and capabilities discussed were in the foundational category.”[1] Those foundational descriptions were amplified as the collection and dissemination of information, analysis, surveying members, and facilitating member information sharing. The ISAO-SO Capabilities and Services Working Group has undertaken ongoing work to expand on the descriptions of foundational services and capabilities. Its work product is in the final stages of publication. That publication will assist ISAOs by providing a truly comprehensive review of the foundational services and capabilities of a model ISAO. In practical terms, the governing body and the leadership of an ISAO should determine the extent to which its own services and

[1] See https://www.isao.org/products/isao-100-2-guidelines-for-establishing-an-isao/.

capabilities will map to the ISAO foundational services and capabilities. The functions ultimately selected must meet the actual needs of the membership and align to the ISAO's strategic goals, mission, and vision.

3.3 STATE ISAO SERVICES AND CAPABILITIES

This section sets forth a review of services and capabilities that current state-level ISAOs are providing. This list is not meant to be all-inclusive. It is indicative of the services and capabilities that are now provided by several state-level ISAOs, including the Indiana ISAC, New Jersey Cybersecurity Communication Integration Cell, LA-SAFE, MS-ISAC, and Michigan ISAC.

- Security awareness, training, and education
- Partnerships: public, private, and academic
- Cyber indicator sharing
- Cyber-threat intelligence
- Cyber-threat analysis
- Security operations center (managed security services provider)
- K-12
  - Local
  - County
  - Higher education
- Forensic and incident response
- Malware reverse engineering and analysis
- Cyber training and tablet-top exercises
- Cyber advisories, news, alerts, bulletins, and vendor security alerts
- Membership service
  - Member surveys
  - Working groups
  - Conferences
- Vulnerability assessments
- Vulnerability management
- Cyber incident response planning.

Such services and capabilities are not necessarily provided or maintained at the same level of depth and maturity. And those that are chosen to be implemented should meet the most pressing strategic needs of the particular state-level ISAO.

A given ISAO initially might be expected only to implement a basic array of functionalities. Such a course is advantageous in that it offers an economical approach to the adoption of new technologies, requires less staff to implement support, and creates a limited, controllable amount of issues requiring resolution. Approaching development in this way also allows for the effective creation of a base upon which to add new functionalities as experience and conditions might warrant.

4 STATE-LEVEL PARTNERSHIPS

Note: An additional resource concerning the intersection of private-sector ISAO capabilities and state-level efforts will be available upon publication of ISAO 6001, “State-Level Enabling and Partnering with Private-Sector ISAOs.”

4.1 OUTREACH AND COLLABORATION

It is a clear national policy imperative for government and industry to better collaborate to improve cybersecurity resilience. Presidential Policy Directive 21 declares, “Greater information sharing within the government and with the private sector can and must be done,” and the Department of Homeland Security (DHS) “shall conduct an analysis of the existing public-private partnership model and recommend options for improving the effectiveness of the partnership in both the physical and cyber space.” Toward this end, the Executive Order on Information Sharing calls for the establishment of ISAOs to effectuate this public-private sharing ecosystem.

Consistent with this national approach, it is highly advantageous for the state ISAO model to provide robust and effective collaboration mechanisms with the private sector, and particularly other ISAOs.

The efficacy of states sharing with private-sector counterparts through ISAOs has been magnified by two congruent conditions. First, state capacities are already stretched thin, both because of budgetary constraints and because of expanding threats affecting state interests. For example, while much of the states’ attention to cyber matters has been directed at protecting the physical critical infrastructure, such as public utilities and healthcare facilities, recently demonstrated foreign attempts at interference in the election process have added to the cybersecurity agenda of the states, which have the constitutional responsibility to conduct and administer both state and federal elections. Second, and relatedly, the private sector has a diversity of experience and a variety of capabilities that the public sector lacks, but from which the public sector can greatly benefit.

A separate consideration for fostering effective outreach mechanisms, aside from resilience, is to enable statewide adoption of information sharing to assure wider distribution of its benefits. Moreover, outreach activities might provide efficiencies and scale, including cost sharing, that could reduce the costs of participation in ISAOs and further encourage their development.

We also note that American technological advancement and world-leading success following World War II, and continuing through the age of development of computers and other technologies, was the manifest result of tripartite cooperation among government, private industry, and academia. At its best, the ISAO movement can recreate that kind of triumvirate, which is key to successfully dealing with the multifarious cybersecurity threat that all sectors increasingly face.

Through effective collaboration, up and down the market and laterally across public-private partnerships, stakeholders are afforded greater opportunities to participate in ISAO efforts and to facilitate the creation of new capabilities within the basic ISAO model.

4.2 ACADEMIC

Building relationships, creating partnerships, and collaborating with academic institutions can be extremely valuable for the state-level ISAO and academic institutions. There are a few distinct advantages that basic academic or higher education institutions bring to the table that can be extremely valuable to the state-level ISAO. Most academic institutions are focused on research and have access to students who seek opportunities to gain hands-on experience in cybersecurity. Their faculties also have access to outside research opportunities. Partnerships with the academic institution should be strategically related to the strengths of the institution. For instance, if one institution is strong in digital forensics, the partnership could be built to assist the state-level ISAO with incident response. If the institution is strong in cybersecurity policy, the state-level ISAO could build a partnership to focus on governance, risk, and compliance.

There are current examples of how such partnerships can work. One example is the relationship that has been built between the Indiana ISAC and Purdue University. The basis of this relationship began when the state of Indiana placed its security operations center in Purdue's Research Park in West Lafayette, IN. From the beginning, the partnership between the Indiana ISAC and Purdue was designed to provide ongoing internship opportunities for Purdue students interested in cybersecurity careers. Another benefit of the partnership has been its ability to develop research opportunities between Purdue University, the state of Indiana (through the Indiana ISAC), and the private sector. Another example of such a relationship between a state and an academic university is the partnership between the state of Wisconsin and the University of Wisconsin–Madison.

4.3 PRIVATE SECTOR

This section addresses a duty of government, with respect to the private sector generally and concerning private-sector ISAOs specifically, to involve and integrate public-private information sharing. ISAO 600-2 provides that

"governments at all levels share a responsibility to enable, support, and appropriately partner with ISAOs to improve the security and resilience of the nation. An effective public-private partnership implies that ISAOs have a voice in the formulation of relevant government policies that impact information sharing and analysis activities, as well as regular opportunities to provide feedback on the effectiveness of government actions."

This reasonable duty harmoniously tracks with other national policies and executive orders in the cybersecurity, information sharing, and infrastructure protection spaces. An extension of the duty to "work with" the private sector is the option and opportunity for a state-level ISAO to "lead with" a private-sector construct (see, for example, section 8.8 below).

Common sense and concern for public safety also imply a governmental duty to involve and integrate private-sector information-sharing institutions with those of the public. A routine attack vector often is directed through small business supply chains, which often connect to up-market customers, including government organizations. It is therefore prudent to ensure that the down-market, business segment is addressed as part of statewide planning of information-sharing mechanisms and institutions.

Creating an open, transparent convening and clearinghouse entity that would be fully compliant with state law would ensure fairness in acquisition. A proper and trusted convener might be a nonprofit, established with suitable governance structures that address various government ethics and arms-length relationship laws and regulations. This sort of convening and clearinghouse construct might be made available or duplicated in counties and cities.

Establishing a legal framework to support the tight integration of the private sector, and a public-private partnership model for information sharing, will be an essential part of any state's information-sharing structure. The state attorney general should be involved to ensure proper formation and integration at the state level. Additional resources are ISAO standards organization working groups and publications that deal with legal matters for ISAO formation and operations. Analog structures and relationships, as well as special authorities, should be used.

Provided below is a small sample of analogous structures and organizations that states may find useful when seeking to establish similar institutions to support ISAO efforts in their state:

- The Civil Air Patrol is a private-sector entity and auxiliary of the U.S. Air Force that performs public service functions during emergency situations.
- The Federal Trade Commission's (FTC's) 2012 Report to Congress recommended use and integration of amateur radio operators by DHS to supplement emergency communications. To respond to the FTC

recommendation, DHS established formal programs for auxiliary emergency communications in the Office of Emergency Communications. Several states have also implemented mechanisms and authorities to implement the FTC's recommendation. In Colorado, for example, a 2016 statute created the Auxiliary Emergency Communications Unit within the state's Division of Homeland Security and Emergency Management.

- The Merchant Marine is a compilation of public and private vessels and operators.

The following are other models that are less integrated as public-private structures:

- Energy-sector cooperatives
- Public-sector messaging and emergency communications that use the commercial broadcast and telecommunications infrastructure
- Public hospitals and education institutions.

There are a number of public-private models that state-level ISAOs can leverage. Models are generally organized around assigning an appropriate scope of responsibility that can vary from case to case. At one end of the spectrum, the majority of responsibility is aligned to the state ISAO, and on the other, the majority of the responsibility is delegated to the private sector (see Figure 1). On the far scale of public-sector responsibility, the partnership is fully funded and staffed (contractors/engineers/analysts) by the state-level ISAO with outside support from the private sector. At the center of the model, financing, support, and staffing is 50 percent public sector and 50 percent private sector. On the other end of the model, where the private sector assumes greater responsibility, the partnership is fully funded and staffed (contractors/engineers/analysts) by the private sector with outside support from the public sector.

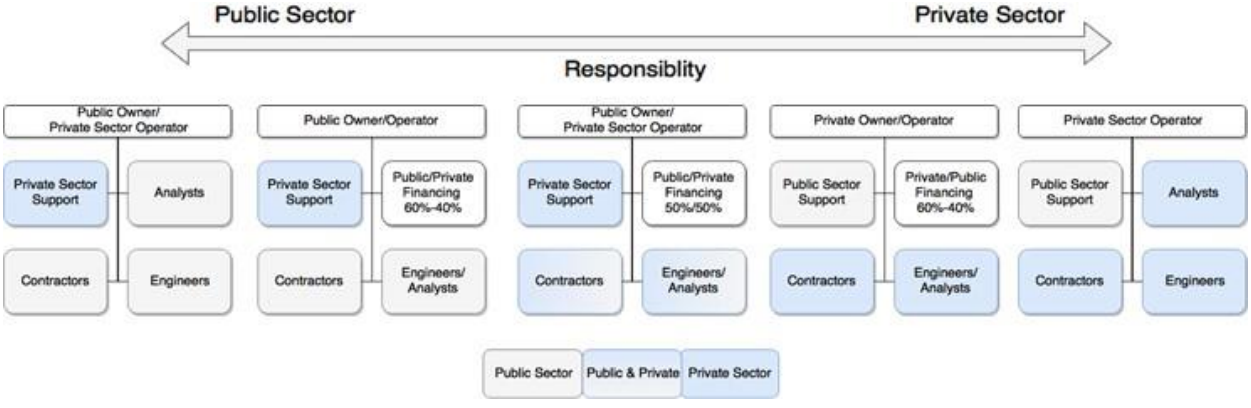

Figure 1. Public-Private Responsibility Matrix

5 STATE-TO-STATE COORDINATION

5.1 INTRODUCTION

As states seek to participate in or establish information sharing and analysis organizations, they do not have to limit themselves to coordination with and within the ISAO. State-to-state coordination also is encouraged to promote the sharing of best practices, experience, and other information. In an effort to assist states with coordination, this section will provide an understanding of existing organizations whose mission it is to facilitate partnership among states and to make recommendations on how these organizations can best be leveraged to share best practices and information and establish regional partnerships.

5.2 FACILITATORS OF STATE-TO-STATE ENGAGEMENT

There are several well-established organizations that states can leverage to facilitate state-to-state coordination. Many states also maintain intergovernmental affairs offices whose goal is to enable communication and collaboration among states and with the federal government. The following is a compendium of leading organizations that seek to improve cyber coordination.

5.2.1 NATIONAL FUSION CENTER ASSOCIATION

Fusion centers serve as the focal point for state and local governments to gather, share, and analyze threat information on a variety of vectors among federal, state, local, tribal, territorial, and private-sector partners. There are 72 fusion centers across the country, and while they primarily serve their constituents at the regional, state, or local level, they integrate with DHS and the Federal Bureau of Investigation to support national security objectives. Fusion centers are integrated as a network to facilitate nationwide information sharing and collaboration as to threats that have the potential for broader implications outside of the fusion center's jurisdiction.

5.2.2 NATIONAL ASSOCIATION OF STATE CHIEF INFORMATION OFFICERS

The National Association of State Chief Information Officers (NASCIO) is a nonprofit organization focused on sharing tools and services with, and facilitating collaboration among, information technology (IT) executives within state government. Though NASCIO is focused on a broad range of issues facing state IT executives, cyber has emerged as a key issue in recent years. NASCIO provides a platform for state chief information officers (CIOs) and chief information security officers (CISOs) to share best practices and experiences among peers.

5.2.3 MULTI-STATE INFORMATION SHARING AND ANALYSIS CENTER

The MS-ISAC is a 24-7 threat-monitoring center dedicated to the protection of state, local, tribal, and territorial government networks. The MS-ISAC is operated by the Center of Internet Security, a nonprofit organization, and is a key partner of the Department of Homeland Security. The MS-ISAC primarily caters to the CISO role within the SLTT community but has expanded the scope of its engagement to include law enforcement and fusion centers. The MS-ISAC also provides a number of services, including network monitoring, threat reporting, and incident response.

5.2.4 NATIONAL GOVERNORS ASSOCIATION

The National Governors Association (NGA) is a bipartisan forum for the nation's governors to "share best practices, speak with a collective voice on national policy and develop innovative solutions that improve state government and support the principles of federalism." NGA recognizes cybersecurity as a critical threat to states and has worked to assist governors in crafting policy, legislation, and programs to secure their states from cyber attacks.

5.2.5 GOVERNOR'S OFFICES OF INTERGOVERNMENTAL AFFAIRS

Many states maintain offices in the Washington, DC, area to facilitate coordination among states and with the federal government. This enables state governments to coordinate with each other on policy, engage in national dialogues on policy and legislation, and enhance state-to-state communication and partnership. These offices are instrumental in sharing best practices across states on issues pertaining to cybersecurity.

5.2.6 ORGANIZATIONAL RESOURCES

The aforementioned organizations serve a broad range of state-level stakeholder communities including police, IT, and executive leadership. Each provides a unique perspective and set of resources to assist the SLTT community in addressing the cyber challenge. Table 1 depicts the various state-level communities that are involved with each organization.

Table 1. State-Level Communities Represented in National Organization

Organizations	CIO/CISO	Law Enforcement	Fusion Centers	Governor's Office
NFCA		X	X	
NASCIO	X			
MS-ISAC	X	X	X	
NGA	X	X	X	X
Governor's Office of Intergovernmental Affairs				X

5.2.7 LEVERAGING STATE-TO-STATE COORDINATION TO SUPPORT STATE ISAOS

There are several aspects of state-to-state coordination that can provide added benefit to state-level ISAOs. These include the sharing of best practices, the sharing of cyber threat and vulnerability information across jurisdictional boundaries, and the establishment of regional, multi-jurisdictional partnerships. This section will break down each aspect and describe its influence on state-level ISAOs.

5.2.8 RECOMMENDED PRACTICES

Each state will likely take a unique approach to the management of its own state-level ISAO. These approaches may manifest themselves in a variety of ways, including how the ISAO is managed and governed, the services and capabilities offered, the stakeholders targeted, and so forth. However, there is, at minimum, a set of common recommended practices that states should implement regardless of the way they have structured their ISAOs. Leveraging the abovementioned facilitators of state-to-state engagement, states should share these core practices among themselves, particularly between states with established ISAOs and those in formative stages of development.

5.2.9 INFORMATION SHARING

States are susceptible to risks that are unique compared to any other type of organization, requiring a need to share information both internally across partner agencies and organizations and externally to other state-level ISAOs. Fusion centers manage this type of interstate collaboration through the National Network of Fusion Centers, which provides a trusted and secure means of sharing threat-related information. Should a state establish an ISAO independent of an existing entity like the fusion center, interstate relationships should be formed to facilitate this type of information sharing. Organizations such as the NGA, NASCIO, and MS-ISAC can also facilitate the exchange of information or the establishment of partnerships among states to enable such sharing to occur.

5.2.10 REGIONAL PARTNERSHIPS

Regional partnerships are effective in establishing state-to-state collaboration given geographic proximity and existing mechanisms for regionalized partnerships such as the Federal Emergency Management Agency (FEMA) regions or urban area security initiatives (UASIs). The following provides additional detail on each of these:

- *FEMA regions.* FEMA divides the country into 10 geographic regions, each with a permanent regional office that serves as FEMA's permanent presence for states within each respective region. The DHS National Protection and Programs Directorate also leverages FEMA's regions to maintain partnerships at the state and local levels to fulfill its mission of

cyber security and infrastructure protection. States will often collaborate with their regional partners to address all hazard threats. Rather than developing a new regional approach, states could look to adopt the FEMA regions that are already established and used by the federal government information-sharing and resource support.

- *UASI.* Born from the federal Homeland Security Grant Program, UASIs are designated regions that contain major metropolitan areas. Oftentimes, UASIs are composed of several local jurisdictions and can even contain multiple states, such as the National Capital Region (NCR), comprising Washington, DC, Virginia, and Maryland. UASIs may form their own regional ISAO, may form a natural multi-state partnership (e.g., NCR), or may warrant specialized attention from the state-level ISAO given their level of criticality to national security.
- *Neighboring states*. States may simply look to their neighbors to develop partnerships and coalitions either in the form of information sharing among state-level ISAOs or to form a regional ISAO.

6 STATE-LEVEL STEERING AND STAKEHOLDERS

6.1 INTRODUCTION

Creating a state-level ISAO necessitates the early involvement of interested and effective stakeholders. Various criteria should be considered when choosing who should be involved, and the roles and levels those individuals should assume, particularly their levels of responsibility and authority within their states (executive, manager, technical lead), which agency they are from, and the specific background and qualifications of the individuals. Moreover, the state's constitution, structure, enacted laws, and administrative code could also determine who will need to be involved. This section addresses some of the key stakeholders who should be involved in the creation of a state-level ISAO and lists a few of the specific roles in the creation.

We use the terms state "agency" and "department" interchangeably. Additionally, the ISAO-SO recognizes that that there are structural similarities and differences among the states. This presents a challenge in ensuring that the position and roles are applicable to as many states as possible. Therefore, the agency titles listed in this section will be described generically. Specific roles and responsibilities of an agency in one state might be completely different in another state or may fall to multiple agencies.

There are several key positions, typical from state to state, that are highly recommended to be included. These positions include the governor, lieutenant governor, secretary of state, adjunct general, CIO, CISO, and attorney general. The level of participation of these executives will likely vary from state to state. Those who are interested and involved in information technology, cybersecurity,

and technology may be more involved with developing the state-level ISAO. More information about these specific positions will be discussed in detail later in this section. This will include suggestions for the roles, duties, and responsibilities for each position. This information is also important to the governance of the state-level ISAO, which is also addressed in a later section.

As the discussion proceeds into the specific roles and responsibilities of each position, this document is organized by the branch of government, the agency/office, the position, and a brief generalized description of that position. Table 2 shows an example of a summary of the position, its roles, duties, and responsibilities.

Table 2. Summary Example

Position/title: Example
Role: Strategy/policy
Duties/responsibilities: Examples of the duties and responsibilities that the position could have in the development of the state-level ISAO

6.2 EXECUTIVE BRANCH

The executive branch of state government is generally structured to be almost identical to that of the federal government. Granted there will be differences from state to state on the executive branch's scope, authority, and structure. Those specifics will be determined by each state's constitution, laws, and administrative code.

6.2.1 GOVERNOR

As the chief executive in each state and the highest politically elected official in the executive branch, the governor's commitment and participation is the most important factor for long-term success and sustainability. For those executive branch agencies that would be involved in the creation, development, and implementation of the state-level ISAO, the governor's involvement will set the tone for each agency. It is suggested that the governor should determine the authority and responsibility of each agency under his or her span and control. Bottom line: It is his or her role to provide the ultimate strategic direction for cybersecurity. The overall mission of the state-level ISAO should reflect the particular needs of the state, but to ensure the highest levels of participation from those agencies participating, the governor should be the driving force. Having the governor's approval and support is only the beginning. Having the right group of agency heads, project managers (PMs), and technical advisors is all necessary to move the state-level ISAO from strategy development to being fully operational. By no means is this an exhaustive or mandatory list of individuals or positions.

Position/title: Governor
Role: Strategy/policy
Duties/responsibilities: Could include chairing a steering committee, providing overall strategic direction, setting policy, directing the mission, goals, and capability requirements for the ISAO. Additional responsibilities could include providing guidance for legislative agendas.

6.2.2 LIEUTENANT GOVERNOR

The lieutenant governor is the second-highest elected political official in the executive branch and would succeed the governor if that office is vacated. Having the lieutenant governor's representation in the development of the state-level ISAO will be beneficial. According to a study by Julia Nienaber Hurst, on average, lieutenant governors have eight statutory requirements. Those duties can range from serving as an agency or department head to leading commissions.[2] Additional roles of the lieutenant governor can include presiding over the state Senate, serving as head of the election division (in a few states), and working in economic development.[3] Depending on the current commissions, boards, or councils, involvement in the development could align with one or more of those roles. However, the specific type and level of involvement from the lieutenant governor my ultimately be determined by the governor, state statue, or state constitution.

Position/title: Lieutenant governor
Role: Strategy/policy
Duties/responsibilities: Could include chairing or co-chairing the committee, providing strategic input on the mission, and performing goals and capability requirements for the ISAO.

6.3 STATE IT/TECHNOLOGY AGENCY

Several states have a consolidated IT/technology agency that is responsible for the state's IT infrastructure, security, IT procurement, and end user support. Given that such an agency "owns" a majority, if not all, of the responsibility for maintenance and cybersecurity of the state's network, systems, and data, the state's CIO and CISO or chief security officer (CSO) are two critical positions whose knowledge and expertise with the state's IT environment is a necessary ISAO component. As a byproduct of this, in some states, the state IT/technology agency has taken the lead in the development of their ISAC/ISAO and then has been "housed" within that agency. Additional information about how ISAOs are modeled will be discussed in a later section. From a technical and tactical

[2] See Julia Nienaber Hurst, *Lt. Governors' Statutory Duties,* http://www.nlga.us/wp-content/uploads/CSG-BoS-JHurst-Stat-Duties.pdf.

[3] See Julia Nienaber Hurst, *Lt. Governors Impact States,* http://www.nlga.us/wp-content/uploads/BOS-2015-Lt.-Governors-Impact-States.pdf.

knowledge base, it is important to have at least one cybersecurity technical lead to serve as a subject matter expert (SME) and to serve in a support capacity.

Position/title: CIO
Role: Strategy/policy/core team
Duties/responsibilities: Potential sponsor for the ISAO. Would provide strategic technological direction. Would have ultimate authority over the organization's resources; evaluates milestones and approves budgets; evaluates and approves the communication plan, including status reports; approves the project charter and project plans; and would have ultimate authority over all work products.

Position/title: CISO or CSO
Role: Strategy/policy/core team
Duties/responsibilities: Could serve as a co-sponsor for the ISAO. Would provide strategic direction as it relates to the specific cybersecurity issues the ISAO would be addressing, discusses and resolves issues that cannot be resolved by the project team, and is responsible for organization-wide communications. Approves changes to the scope and provides whatever additional funds those changes request; evaluates and approves change requests; evaluates milestones and approves budgets; evaluates and approves the communication plan, including status reports; approves the project charter and project plans; provides guidance and mentoring to the project lead, PM, and teams; and has authority over and is accountable for the project. Additionally, could have control of the business aspects of the project and assist in developing the project charter and project plans.

Position/title: Cybersecurity and intelligence technical lead(s) or SME(s)
Role: Project support
Duties/responsibilities: Would serve as an expert in the state's cybersecurity system and liaison to the project support team. Would provide insight into the specific cybersecurity roles, jobs, tasks, or skills needed in the state-level ISAO. Would assist the project team in developing the specific business process, systems, and applications the ISAO would use. Would assist the project team in understanding how those systems and applications would integrate into the state's current process to the project leadership and project team. As additional qualifications, would need to be able to answer specific technical questions and have in-depth knowledge of the state's technical interdependences.

6.4 STATE DEPARTMENTS/DIVISION OF HOMELAND SECURITY

A state DHS is typically the leader of the state's emergency management and homeland security efforts, including planning, training, emergency response and recovery, certifications, grants administration and fire and building safety, which includes building construction plan review and all manner of inspections for the public's safety: mainly public buildings and structures and safety at public events.

In several states, cybersecurity falls to their department or division of Homeland Security. Given the relationship between the state-level DHS and the U.S. Department of Homeland Security (US-DHS), the state-level DHS is another critical partner in the development of the state-level ISAO.

Position/title: Executive director/director/agency head
Role: Strategy/policy/core team
Duties/responsibilities: Could serve as a sponsor or co-sponsor of the ISAO. Would provide strategic direction as it relates to the critical infrastructure sectors, emergency response, planning, training and exercising of the cybersecurity issues the ISAO would be assisting, mitigating, and responding to. Their goal is to serve as the primary liaison of the state DHS agency to the core team. If serving as a co-sponsor, additional duties would include discussing and resolving issues that cannot be resolved by the project team responsible for organization-wide communications. Would approve changes to the scope of activity and provide whatever additional funds those changes require. Would be responsible for the evaluation and approval of change requests; the evaluation of milestones; approving budgets, evaluation, and communication plans, including status reports; and approval of the project charter and project plans. Would provide guidance and mentoring to the project lead, PM, and project teams. Would have authority over and accountability for the project. Additionally, could have control of the business aspects of the project and assist in developing the project charter and project plans.

Position/Title: Cybersecurity program manager/director
Role: Project support/SME
Duties/responsibilities: Would serve as an expert in the state's critical infrastructure, have experience in cybersecurity and IT, and liaison to the project support team. Would provide insight into the specific cybersecurity roles, jobs, tasks, or skills needed in the state-level ISAO. Would assist the project team in developing the specific business process, systems, and applications the ISAO would use. Would assist the project team in understanding how those systems and applications would integrate into the state's current process to the project leadership and project team. Also would need to be able to answer specific technical questions and have in-depth knowledge of the state's technical interdependences.

Position/title: Liaison or representation from state agencies or systems of administration
Role: Institutional expertise
Duties/responsibilities: Ensure integration and compliance of ISAO governance and operations within the execution responsibility of the appropriate agency.

Position/title: Coordinator for private-sector integration
Role: Outreach and relationship building with the private sector

Duties/responsibilities: Design and implement the governance framework that integrates information sharing across a public-private partnership model.

6.5 STATE LAW ENFORCEMENT AGENCIES

The role(s) of the relevant state law enforcement agencies will depend on their specific mission. In a few states, the state law enforcement responsibilities are split between an investigation bureau and a traffic enforcement department—for example, the Georgia Bureau of Investigation and the Georgia State Police; the Tennessee Bureau of Investigation and the Tennessee State Police; and the Florida Department of Law Enforcement and the Florida Highway Patrol.

Position/title: Superintendent/director/commissioner/agency head
Role: Strategy/policy/core team
Duties/responsibilities: Could serve as a sponsor or co-sponsor for the ISAO. Would provide strategic direction as it relates to law enforcement, criminal law, cybercrimes, incident response and incident command. Their goal is to serve as the primary liaison of the state law enforcement agency to the core team. If serving as a sponsor, additional duties would include discussing and resolving issues that cannot be resolved by the project team responsible for organization-wide communications. Would approve changes to the scope and provide whatever additional funds those changes request. Would be responsible for the evaluation and approval of change requests; evaluation of milestones; approval of budgets; evaluation and approval of the communication plan, including status reports; and approval of the project charter and project plans. Would provide guidance and mentoring to the project lead, PM, and project teams. Would have authority over and be accountable for the project. Additionally, could have control of the business aspects of the project and assist in developing the project charter and project plans.

Position/title: Cyber-crimes unit commander
Role: Project management/support team/advisor
Duties/responsibilities: Would serve as an expert in cyber-crime, forensics, incident response, and liaison to the project support team. Would provide insight into the specific cybersecurity roles, jobs, tasks, or skills needed in the state-level ISAO. Would assist the project team in developing the specific business process, systems, and applications the ISAO would use. Would assist the project team in understanding how those systems and applications would integrate into the state's current process to the project leadership and project team. As additional qualifications, would need to be able to answer specific technical questions and have in-depth knowledge of technologies that could be used by the ISAO.

6.5.1 FUSION CENTERS

Fusion centers serve as a primary focal point within the state and local environments for the receipt, analysis, gathering, and sharing of threat-related information among federal, state, local, tribal, and territorial partners located in

states and major urban areas throughout the country.[4] Fusion centers also have a public-private partnership mission. Incorporating and synchronizing their mission with the state-level ISAO will allow for greater coordination and utilization of limited resources.

Position/title: Fusion center executive director
Role: Strategy/policy/core team
Duties/responsibilities: Could serve as a sponsor or co-sponsor for the ISAO. Would provide strategic direction as it relates to information sharing, analysis, law enforcement, criminal law, cyber-crimes, incident response, and incident command. Their goal is to serve as the primary liaison of the state law enforcement agency to the core team. As the head of a fusion center, its executive director is uniquely situated to assist in developing strategies for the ISAO to better serve front-line law enforcement, public safety, fire service emergency response, public health, critical infrastructure protection, and private-sector security personnel to lawfully gather and share cyber-threat information.

Position/title: Public-private coordination director
Role: Private-sector coordination
Duties/responsibilities: Some states have established relationships with the private sector with direct roles and physical presence inside the fusion center, which is akin to how the US-DHS National Cybersecurity and Communications Integration Center (NCCIC) has private-sector partners on the operations floor. These private partners tend to be member based and offer member intelligence and also gaps and needs to help establish a tighter nexus to stakeholder communities.

Position/title: Fusion center cybersecurity analyst
Role: Support team
Duties/responsibilities: Would serve as an expert in cybercrime and cyber analysis and serve as liaison to the project support team. Would provide insight into the specific cybersecurity analytic processes and the tactics, techniques, and procedures (TTPs). Would assist in identifying roles, jobs, tasks, or skills needed in the state-level ISAO. Would assist the project team in developing the specific business process, systems, and applications the ISAO would use. Would assist the project team in understanding how those systems and applications would integrate into the state's current process to the project leadership and project team. As additional qualifications, would need to be able to answer specific technical questions and have in-depth knowledge of technologies that could be used by the ISAO.

Position/title: Fusion center analyst
Role: Support team

[4] See the National Network of Fusion Centers Fact Sheet, https://www.dhs.gov/national-network-fusion-centers-fact-sheet.

Duties/responsibilities: Would serve as an expert in crime analysis and as liaison to the project support team. Would provide insight into the general analytic processes and TTPs. Would assist in identifying roles, jobs, tasks, or skills needed in the state-level ISAO. Would assist the project team in developing the specific business process, systems, and applications the ISAO would use. Would assist the project team in understanding how those systems and applications would integrate into the state's current process to the project leadership and project team. As additional qualifications, would need to be able to answer specific technical questions and have in-depth knowledge of technologies that could be used by the ISAO.

6.6 NATIONAL GUARD

Over the past few years, the National Guard Bureau has been working to build up its cyber capabilities. This includes the development of cyber protection teams (CPTs). The first three CPTs were activated in fiscal year (FY) 2016, a second set of three were activated in FY17, and the final four were activated in FY18. The main goal of the CPTs is to boost the defense capabilities of both the federal government and the state governments. The greatest advantage that the National Guard CPTs offer is that "Guard Soldiers are uniquely postured to support the CPT mission, having a large number of Soldiers who work within the Information Technology or academic sector, and who may offer expertise and competencies on cutting-edge cyber defense policies, tactics, techniques, and procedures."[5]

Additionally, each state has a congressionally authorized eight-person Computer Network Defense Team (CND-T) National Guard team, responsible for defending GuardNet.

Position/title: Adjunct general
Role: Strategy/policy/core team
Duties/responsibilities: Could serve as a sponsor or co-sponsor for the ISAO. Would provide strategic direction as it relates the state's national guard readiness, disaster response, military coordination, incident response, and incident command. The goal is to serve as the primary liaison of the state's National Guard to the core team. As the head of a National Guard, the adjunct general is situated to assist in developing cyber defense strategies for the ISAO to better serve critical infrastructure protection, the CPTs, and private-sector security personnel to defend and share cyber threat information.

Position/title: CPT commander/CND-T commander
Role: Project management/support team/advisor
Duties/responsibilities: Would serve as an expert in cyber defense, forensics,

[5] See National Guard Bureau, February 24, 2015, http://www.nationalguard.mil/News/ArticleView/Article/577375/national-guard-cyber-protection-teams-announced/.

incident response, and liaison to the project support team. Would provide insight into the specific cyber defense and response roles, jobs, tasks, or skills needed in the state-level ISAO. Would assist the project team in developing the specific business process, systems, and applications the ISAO would use. Would assist the project team in understanding how those systems and applications would integrate into the state's current process to the project leadership and project team. As additional qualifications, would need to be able to answer specific technical questions and have in-depth knowledge of technologies that could be used by the ISAO.

Position/title: CPT soldier/CND-T soldier
Role: Project support
Duties/responsibilities: Would serve as an expert in cyber defense, incident response, and forensics and serve as liaison to the project support team. Would provide insight into the specific cybersecurity analytic processes and TTPs. Would assist in identifying roles, jobs, tasks, or skills needed in the state-level ISAO. Would assist the project team in developing the specific business process, systems, and applications the ISAO would use. Would assist the project team in understanding how those systems and applications would integrate into the state's current process to the project leadership and project team. As additional qualifications, would need to be able to answer specific technical questions and have in-depth knowledge of technologies that could be used by the ISAO.

6.7 STATE ECONOMIC DEVELOPMENT CORPORATION

Position/title: Cybersecurity/IT/technology advisor
Role: Project support/project advisor
Duties/responsibilities: Would serve as a subject matter expert on the economic impact, workforce development, and business impact that the state-level ISAO could have on the state. Would also be integral in serving in a leadership role with developing public-private partnerships.

6.8 LEGISLATIVE BRANCH

The legislative branch of state government is generally set up in the same bicameral manner (save for Nebraska) and performs the same types of law-making and investigative duties as the U.S. Congress. For the most part, it provides the same types of checks and balances and is a co-equal branch of the state government.

Position/title: Legislators (House/Senate/General Assembly/General Court)
Role: Advisor
Duties/responsibilities: The level of involvement of state legislators will be determined by a state's constitution, laws, administrative code, and who sponsors the creation of the state-level ISAO. In some states, members of the legislature serve as non-voting members of an executive branch council. They can serve as a liaison to the legislative branch, provide insight into the legislative

process, and be the representation of the legislative body. Individual state legislators also serve on committees that provide budgetary and substantive oversight of executive-branch functions and also conduct investigations. Legislators also maintain constituent services offices through which private input can be gained concerning emerging threats and useful practices. Additionally, having individual legislators involved will ensure they are kept aware of the cybersecurity initiatives of the executive branch. It is recommended to have at least one senior legislative member who serves on a homeland security, public safety, and/or IT committee and who is involved in this project.

6.8.1 SECRETARIES OF STATE

The secretary of state is the chief election official in approximately 40 states. Though roles and responsibilities will vary from state to state, they usually include, besides the oversight and administration of both state and federal elections, the maintenance of state records, preservation of the state seal, chartering of new business, regulation of the securities industry, commissioning of notaries' public, registration of trademarks, and licensing of vehicle dealerships. With the attention that has been placed on election system security, a focus of the state-level ISAO should include sharing cyber-threat information with the secretary of state's office. Moreover, elections span operations down to county and community levels and hence afford a natural nexus to state-wide adoption and integration of information-sharing activities. As noted earlier, recent events involving attempted interference in U.S. elections by antagonistic nation-states magnify both the cyber burdens that states face and the necessity and utility of involving state officers in activities such as ISAOs.

Position/title: Secretary of state
Role: Advisor/policy/strategy/core team
Duties/responsibilities: Serve as primary liaison from the secretary of state's office to the state-level ISAO core team. Provide official guidance and policy recommendations on how the ISAO can engage with the election system security within that state.

Position/title: Deputy secretary of state
Role: Advisor/policy/strategy/core team
Duties/responsibilities: Serve as the backup or proxy for the secretary of state. Serve as an advisor to the ISAO core team and provide subject matter expertise on the state's election system.

Position/title: IT director
Role: Advisor/project support team/technology SME
Duties/responsibilities: Provide technical expertise on the specific systems, applications, and technologies used in the state's election system. Serve as a liaison to the project support team to the secretary of state.

6.8.2 STATE ATTORNEY GENERAL

The state attorney general serves as the chief legal officer and advisor and is often the chief law enforcement officer for the state. One of the common duties of the attorney general is consumer protection. Given that many cybercrimes involve fraud and scams, the attorney general is another key stakeholder to have involved in the development of the state-level ISAO.

Position/title: Attorney general
Role: Advisor/policy/strategy/core team
Duties/responsibilities: Provide strategic and policy guidance and serve as the primary liaison of the attorney general's office to the core team. Ensure that the state-level ISAO's mission is coordinated with its efforts.

Position/title: Consumer protection SME
Role: Advisor/project support team/technology SME
Duties/responsibilities: Serve as a subject matter expert on consumer protection practices for that state. Serve as a liaison to the project support team.

Position/title: Identity theft SME
Role: Advisor/project support team/technology SME
Duties/responsibilities: Serve as a subject matter expert on identity theft protections for that state. Serve as a liaison to the project support team.

6.9 OTHER

Several other positions can provide significant value to the state-level ISAO. Assuming a reasonable level of experience and technical ability, using a pre-existing project management office within the IT or technology department would be optimal, as it should be familiar with handling IT-specific projects. The remainder of this document may provide considerations for other areas of focus and potential positions that may be formed within the state structure.

Position/title: Project manager
Role: Project support
Duties/responsibilities: The PM will be responsible for evaluating the quality of the product or service. Will oversee the analysis, design, and development of all aspects of the project. Works with the project lead to generate analysis, design, and development of all aspects of the project. Works with the project lead to generate the communication plan, including status reports. Works with the project lead to review the project charter and project plans. Will generate change requests, will generate milestone and budget change requests, and will work with the project lead to ensure the quality of the product or service. Will execute and maintain the project communication plan, including status reporting; conduct formal reviews and support management reviews; track and dispose of issues; help to resolve issues; help to resolve change requests; and track action items through completion.

Position/Title: Project lead
Role: Project support
Duties/responsibilities: The project lead supports and controls the day-to-day aspects of the project. Works with the PM to generate the analysis, design, and development of all aspects of the project. Works with the PM to generate the communication plan, including status reports. Assists in developing the project charter and project plans. Works with the PM to review the project charter and project plans. Provides input for progress reports. Works with the PM to generate change requests and to generate milestones and budget change requests. Works with the PM to ensure the quality of the product or service and is accountable for that quality.

6.10 CONCLUSION

The development of a state ISAO can be complicated, given the political, legal, and structural differences from state to state. Having the correct mixture of positions at the appropriate levels within the state will allow those who are most knowledgeable about cybersecurity and those who can get things accomplished to maximize the possibility of long-term success. As mentioned earlier, the exact roles and responsibilities will vary from state to state. The goal of this section is to provide a starting point for state officials to quickly identify the key stakeholders within each state. A potential roadblock to an effective implementation can come from interagency conflicts. A clear definition of each agency's roles, responsibilities, and duties is the antidote to such an issue.

7 POTENTIAL ORGANIZATIONAL MODELS

Over the past few years, several states have developed and implemented state-level ISAOs, including Arizona, Indiana, Louisiana, Michigan, New Jersey, Kansas, and Virginia. The organizational modules and the services and capabilities that these states employ are varied. The goal of this section is to provide state governments that have yet to create an ISAO, and those looking to formalize and/or centralize current information-sharing practices, with a list of possible organizational modules. Differing variations of the state ISAO and where they fall within the overall state organizational structure will depend on several factors. Those factors include the types of services, level of services, capabilities, and overall mission of the state-level ISAO. The following are only intended to serve as examples and are not meant to be prescriptive. The organizational branches listed in the examples below are not specifically required of the ISAO in that particular model. Again, their purpose is to serve only as a guide or offer a possibility of how the state-level ISAO could be structured.

7.1 INTEGRATED—STATE HOMELAND SECURITY DEPARTMENT

In this model, the state-level ISAO falls under the state's Department of Homeland Security (DHS) (see Figure 2). The branches within this model include

security awareness and training, security operations center, analysis, partnerships and governance, risk, and compliance. The advantage of this model would be in its ability to incorporate the cyber emergency response plan into the state's overall emergency operations. A disadvantage would be the need to recruit and retain cyber talent. A challenge for this ISAO is being able to easily integrate into the state's cybersecurity systems (if implemented by the state's technology agency). One reason for adopting this model would be to leverage the DHS's response capabilities throughout the state.

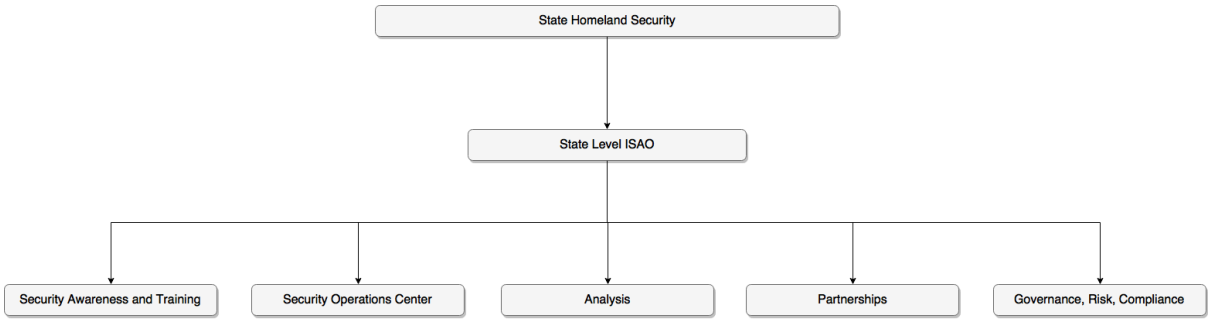

Figure 2. State ISAO Integrated with DHS

7.2 INTEGRATED—STATE IT AGENCY REPORTING TO CIO

In this model, the state-level ISAO reports directly to the state CIO (see Figure 3). The organizational services in this model could include security awareness and training, the security operations center, and partnerships. Advantages of this model include direct access to the highest IT officer in the state and being within the state's IT agency. One disadvantage is that the state-level ISAO does not fall directly within the state CISO's responsibility. This could create potential conflicts in roles and responsibilities within the state's security team.

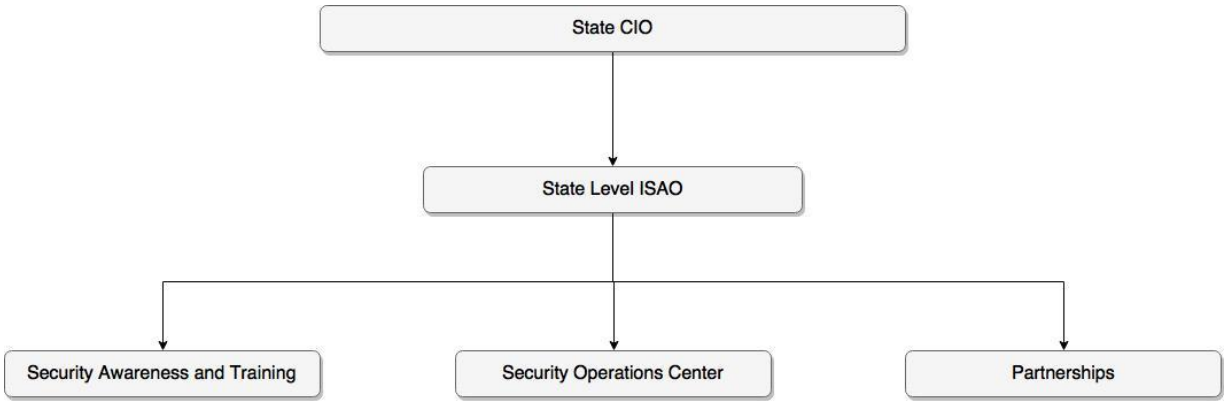

Figure 3. State ISAO Reporting to State CIO

7.3 INTEGRATED—STATE IT AGENCY REPORTING TO CISO

In this model, the state-level ISAO reports directly to the state CISO (see Figure 4). The organizational services in this model could include security awareness and training, the security operations center, and partnerships. The advantages of this model include being directly integrated with the state's security team and being within the state's IT agency. One disadvantage is potential communication challenges among the state's homeland security department, state law enforcement, and the National Guard.

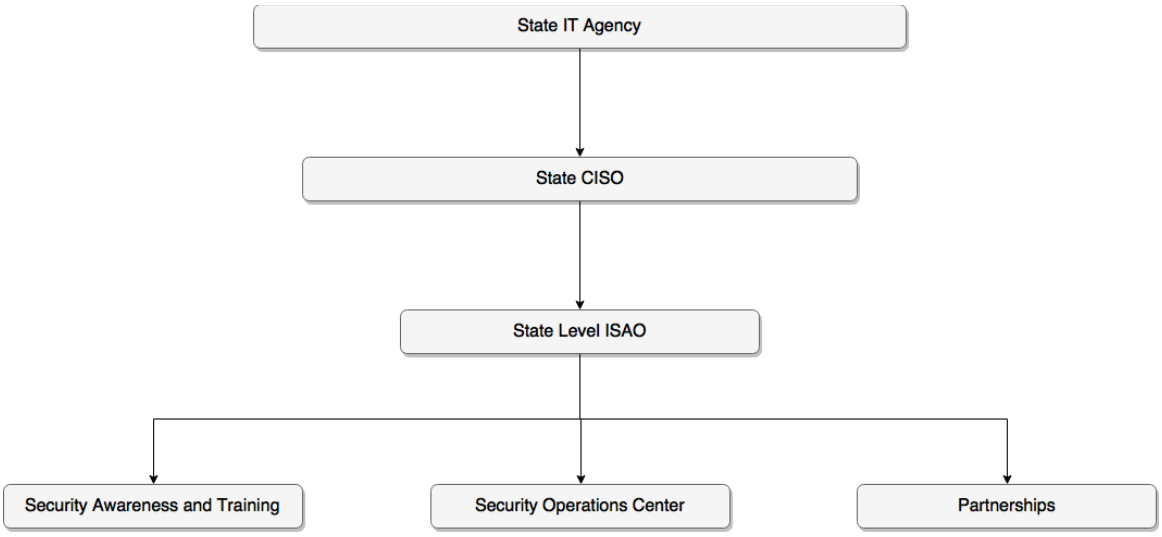

Figure 4. State ISAO Reporting to State CISO

7.4 INTEGRATED—STATE POLICE

In this model, the state-level ISAO reports within the state law enforcement agency (see Figure 5). The organizational services in this model could include security awareness and training, cyber-threat intelligence sharing, and cyber

analytics. A reason for choosing this model would be if the mission of the ISAO is primarily to support law enforcement and provide investigative services. One disadvantage is potential challenges in getting access to the state's security systems. There could also be challenges posed if the designated functions are under the same legal constraints as those governing a law enforcement agency.

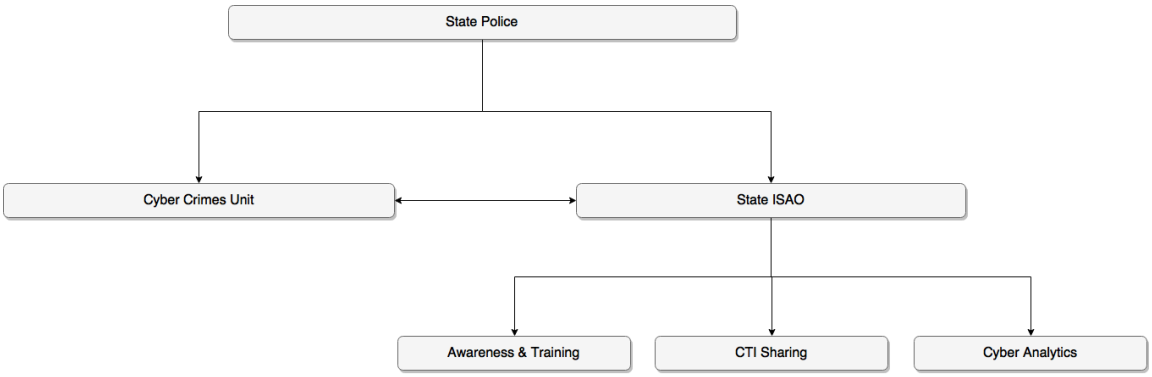

Figure 5. State ISAO Reporting to State Police

7.5 COMBINED INTO A FUSION CENTER'S MISSION

In this model, the state-level ISAO is integrated into a state-level fusion center (see Figure 6). The organizational services in this model could include security awareness and training, cyber-threat intelligence sharing, and cyber analytics. The primary advantage with this model is that the state-level ISAO can take advantage of the fusion center's preexisting infrastructure, analytical expertise, contacts, and partnerships. One disadvantage is with potential challengers getting access to the state's security systems and tools. There could also be challenges with the types of services and capabilities the ISAO offers being under the same legal constraints as the fusion center.

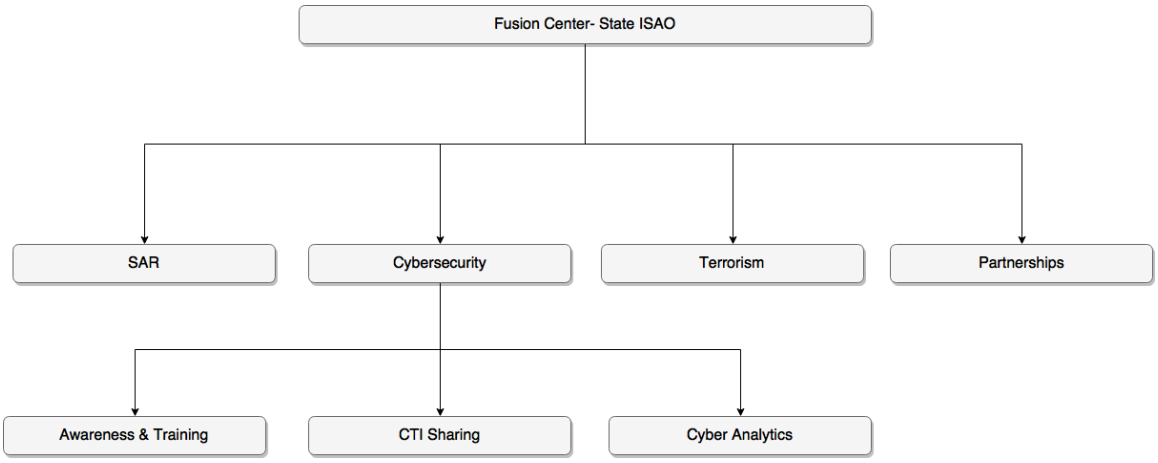

Figure 6. State ISAO Integrated with Fusion Center

7.6 STATE ISAO SUPPORTING FUSION CENTER

This is a similar model to that above, with one slight addition. In this example, the state-level ISAO organizational structure falls under the state's IT agency. However, there is an official relationship with the state's fusion center (see Figure 7). An example of this is the Indiana Information Sharing and Analysis Center, which through a memorandum of understanding serves as the primary cyber capability for the Indiana Intelligence Fusion Center. There are a few advantages with this model. First, both agencies can leverage the strengths of each other. Second, this allows for an improved synchronization of cyber efforts. One of the main disadvantages with this model is that policies, processes, and communication can become more challenging because multiple state agencies are involved.

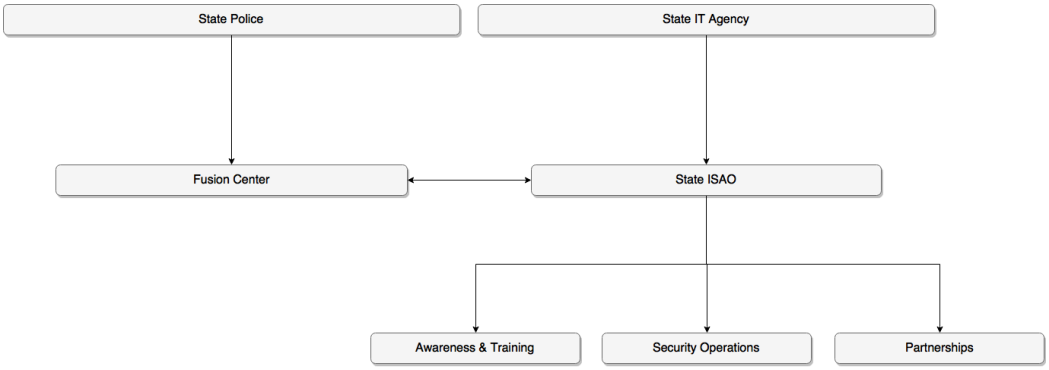

Figure 7. State ISAO Supporting Fusion Center

7.7 REPORTING TO THE GOVERNOR'S OFFICE

In this model, the state-level ISAO reports directly to the governor's office (see Figure 8). The organizational services in this model could include security awareness and training, the security operations center, cyber analysis, and

partnerships. The advantages of this model include direct access to the highest executive office in the state. This would ensure that the state's cybersecurity concerns are being addressed with the governor. One disadvantage is that the state-level ISAO does not fall directly within the state CIO's or CISO's responsibility. This could create potential conflicts in roles and responsibilities within the state's security team.

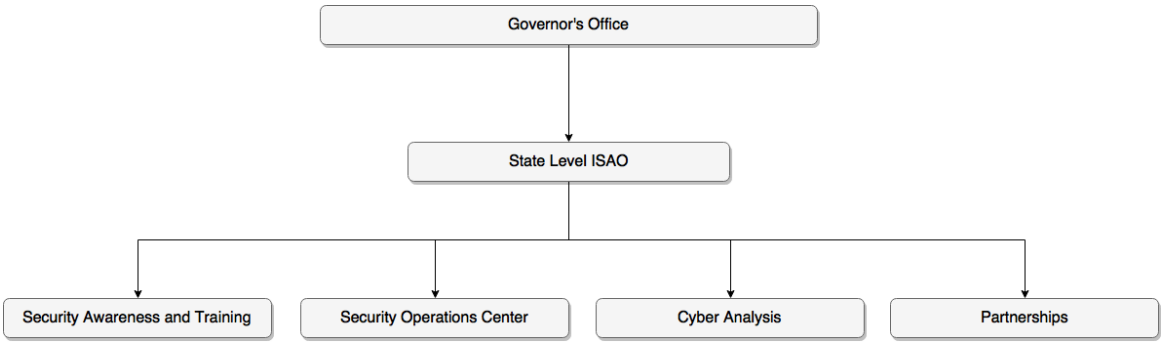

Figure 8. State ISAO Integrated with Governor's Office

7.8 NONPROFIT 501(C)(3) MODEL

Some states, such as Arizona and Wisconsin, have chosen to use a nonprofit model for a public-private partnership (see Figure 9). Arizona joined the Arizona Cyber Threat Response Alliance (ACTRA) and incorporated ACTRA into its emergency response plan Annex G for cyber incident response. In this model, the state and municipalities are members of the nonprofit ISAO and share non-attributable information with other member organizations through the Security Operations Center. In addition to free training, the state and municipalities also benefit from crowd-sourcing cyber incident response, if requested, to assist with cyber incidents. Finally, in Arizona, the 501(c)(3) also places a person inside the state fusion center for cyber situational awareness in the private sector.

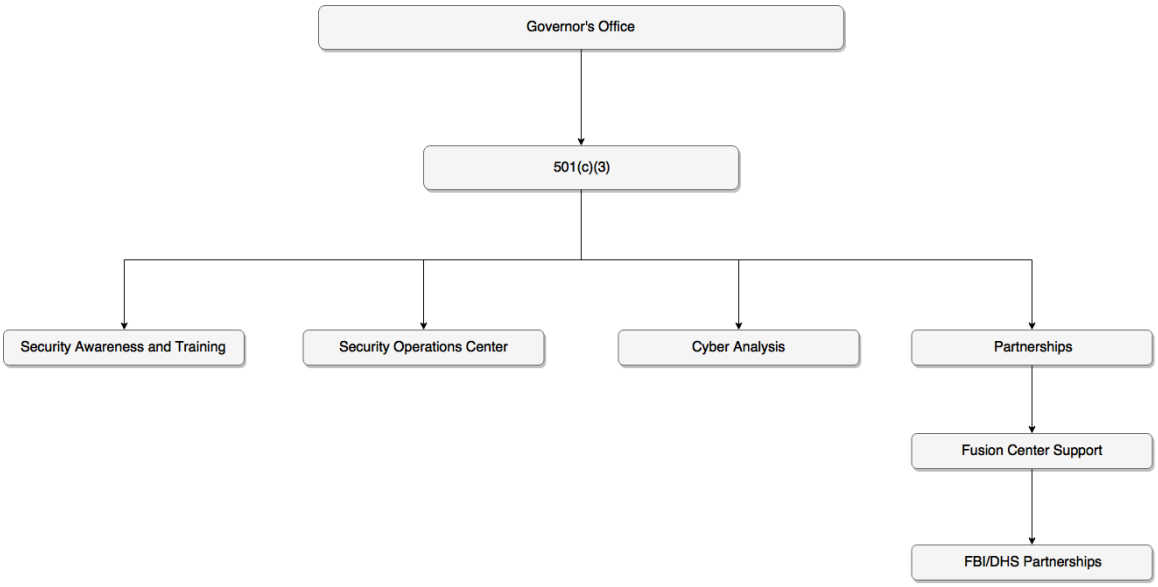

Figure 9. Nonprofit Model

8 GOVERNANCE

A formal operational governance model (Figure 10) helps people answer questions—such as “Why are we doing this?” “Is this OK?” “Whose call is this?” and “Who do we need to tell about this?”—and to know when to ask such questions. A formal governance operating model is the mechanism used by the board and management to translate the elements of the governance framework and policies into practices, procedures, and job responsibilities within the state-level ISAO. The major components of a formal operational governance model are structure, oversight responsibilities, culture, and infrastructure.

Structure will vary, depending upon design and reporting factors. Section 7 presents several potential organizational models for consideration. In each model presented, a Board of Advisors will most likely include a number of the stakeholders identified in Section 4. This board will set the strategic vision for the state-level ISAO. The reporting structure of a state-level ISAO will consist of a structure that is understandable to internal employees and external stakeholders, as shown, for example, in the diagram depicted in Section 7.1 of this document.

Oversight responsibilities create well-understood lines of authority and accountability at all levels and areas of the organization. This includes both the Board of Advisors oversight and responsibilities and management authority and accountability. It is critical within a state-level ISAO that there are clearly defined decision rights such that people understand the authority—and the limits of the authority—associated with their positions in a state-level ISAO. The management of the state-level ISAO should include an executive director to direct or coordinate the day-to-day activities of the ISAO, in support of the board’s strategic vision, and directors for each of the services that the state-level ISAO

wants to provide. Selection of these individuals should be compatible with their current state positions.

The culture of the organization is summarized by the business and operating principles of the organization. For example, the state-level ISAO might decide to create a culture of trust by ensuring that all information sharing is anonymized by the ISAO by removing the entity name from any shared reporting. This is the guiding principle that the organizational infrastructure will be designed around.

Infrastructure includes the policies, procedures, reporting, and communication methods designed to meet the business and operating principles, while also including the technology to be used by the organization. These are the “how to” procedures the organization will use, and they should support the business and operating principles set by the Board of Advisors.

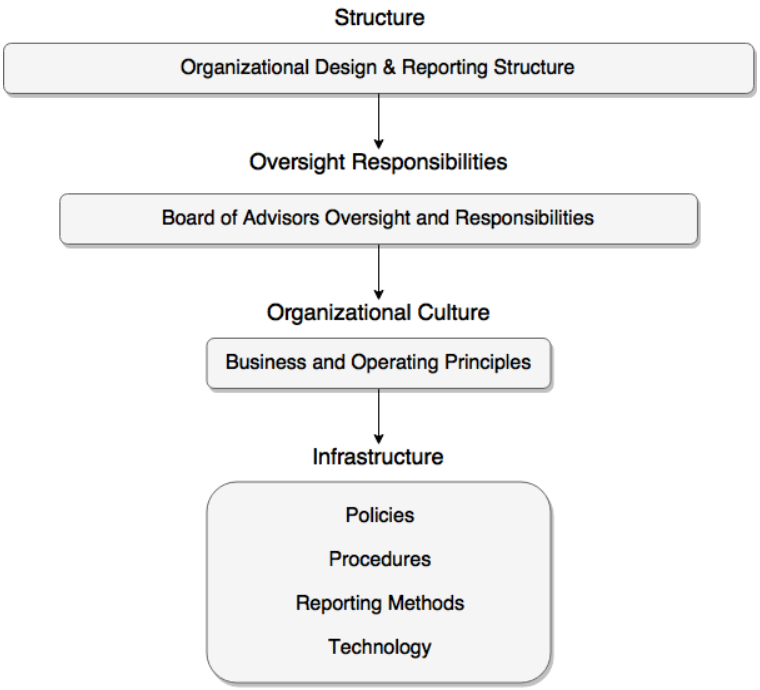

Figure 10. Governance Model

9 ADMINISTRATION

Figure 11 depicts the state ISAO administration organizational chart.

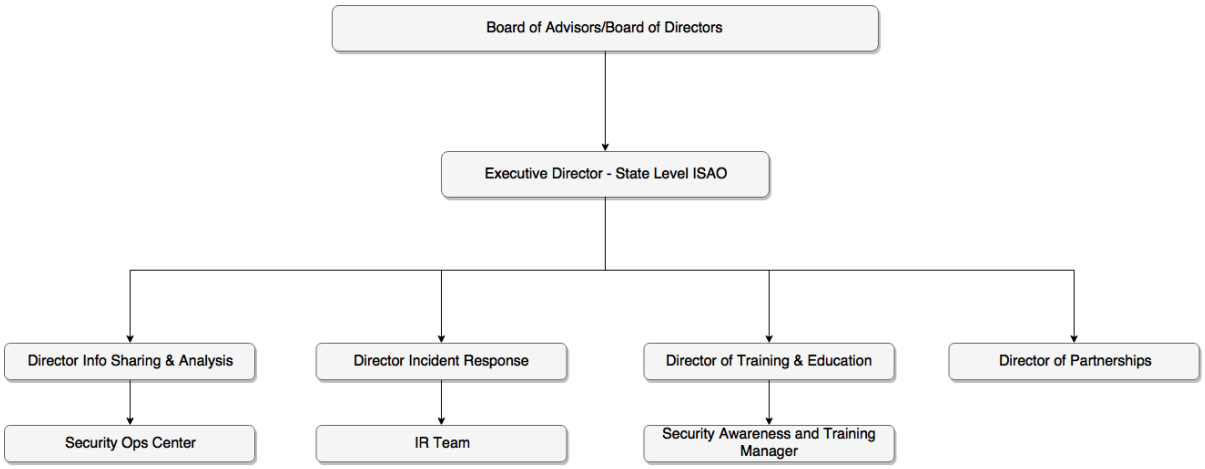

Figure 11. State ISAO Administration Organizational Chart

ISAO 100-2, Section 4.1,[6] discusses the importance of creating an effective governance model for an ISAO, stating that "the need for a defined governance model that articulates how the ISAO will be directed and overseen is an important initial requirement for an emerging ISAO. Depending on its vision and goals, the ISAO may choose to establish itself as an informal group with a looser set of operating rules, or it may choose at the outset to establish itself as a formal operating entity. It is important to recognize that the vision, goals, and membership of the ISAO may change considerably over time, which may support consideration of starting an ISAO with a smaller, less-formal organization and making changes to the governance structure as the ISAO evolves and matures."

There are many ways a state might have an informal ISAO. For example, the state CIO or CISO may be the executive director of the state ISAO, responsible for the overall daily direction of the ISAO. A Board of Advisors, consisting of many of the senior leaders identified in Section 4.2 or leaders of agencies participating in the ISAO, would set the strategic direction of the ISAO. Virginia, for example, has a State Cybersecurity Panel that meets quarterly in a public forum, focusing on cybersecurity issues. This panel consists of representatives from many of the agencies listed in Section 4.2, and for Virginia, this would be the ideal venue for the state ISAO executive director to report to and receive strategic direction from.

9.1 POSITIONS

The following is a list of potential duty positions required to support a state-level ISAO. However, it is dependent on the services the ISAO plans to provide. While it is assumed that the ISAO is focused on information sharing and analysis, if the ISAO also desires to provide training and education, consider having separate directors for each branch of service the ISAO provides, unless these services are

[6] See https://www.isao.org/products/isao-100-2-guidelines-for-establishing-an-isao/.

common to the mission. For example, the information-sharing branch may also include the personnel who would provide incident response. In this instance, the director of this branch would be responsible for overseeing both services.

Position/title: Executive director
Role: Strategy/policy/core team
Duties/responsibilities: Would have ultimate authority over and is responsible for the ISAO; reviews progress reports; would have ultimate authority over the technology agency resources; evaluates milestones and approves budgets; evaluates and approves the communication plan, including status reports; approves the project charter and project plans; and would have ultimate authority over all work products.

Position/title: Director (of information sharing and analysis/incident response/training and education, etc.)
Role: Core team
Duties/responsibilities: Leads the project team in developing the specific business process, systems, and applications the ISAO would use. Leads the project team in understanding how those systems and applications would integrate into the state's current process to the project leadership and project team. As additional qualifications, would need to be able to answer specific technical questions and have in-depth knowledge of the state's technical interdependences.

10 FISCAL CONSIDERATIONS

10.1 INTRODUCTION

This purpose of this section is to offer an approach to ISAO structuring and planning at the state level, including support to public-private partnership efforts, that reviews the fiscal aspects from regulatory structures, so that a state considers operational and organizational formation against this important structural backdrop.

10.2 SCOPE

Funding for the advancement of ISAOs should encompass both initial rollout and mature operations at scale. Each state, considering a variety of factors (e.g., population density, risks to critical infrastructure, budget, projected end-state), needs a fiscal plan that meets the objectives of its information-sharing system. At one end of a range of options, for example, an exemplar for an ISAO operations and organization plan may entail municipal-level ISAOs and public-private ISAOs in multiple localities across the state linked via a distributed operations model. The financial model supporting such an extensive structure, for example, would differ from the stand-up and operation of a single ISAO at the state level. Moreover, a mix of public and private funding sources can be considered for any range of options, when legally permissible.

10.3 ORIENTATION: REGULATORY STRUCTURES AND FUNDING MODELS

The current large systems of administration in the states represent an available structure for institutionalizing and funding ISAOs, at least in part, and potentially producing financial benefits. There will be benefits and tradeoffs, including regulatory considerations, that would come in implanting an ISAO administration within any preexisting system of administration. Additionally, enabling legislation might be necessary to authorize the incorporation of ISAO operations within a system of administration. Still, all of the listed systems have a logical and mission-oriented nexus to ISAO incorporation within them. In some instances, the list represents a budget line item rather than a fiscal model (i.e., ISAO operations would become part of a department budget). The following list is representative only, and states are encouraged to explore alternative systems of administration. Note also that the listed titles may represent a fiscal approach that is not necessarily organized in a state as a system of administration. Our objective in providing this representative list is to offer concepts for a state to consider in its ISAO fiscal planning efforts. It is not to mandate any specific level of state financial support. That will vary from state to state and be dependent upon both economic and political factors. Finally, funding strategies indicated in a particular model may be mixed with other strategies, if legally permissible.

As a matter of clarification, we note that the following subsections should not be interpreted as a call for regulation. Rather, various systems of administration exist across the states, some in highly regulated or deregulated forms. This section, therefore, is intended only to highlight systems of administration that exist in order to trigger statewide assessment of their utility in helping enable and support ISAOs.

10.3.1 CONSUMER PROTECTION

Many of the alleged harms from cyber threats are being addressed through consumer protection authorities at the state and federal levels. Even in civil litigation, most breach lawsuits have relied upon state laws when they afford a private cause of action, which federal law does not. These approaches represent enforcement and financial compensation strategies that typically address data holders' malfeasance or misfeasance in the event of a data compromise or other breach. Conversely, an ISAO represents a resource to improve situational awareness and to share defensive mechanisms in response to cyber-attack trends. In the context of consumer protection laws, a state may choose different ways to address ISAOs. Different approaches may afford remedies, civil litigation opportunities, or protections, as well as institutionalizing certain consumer protection activities. Such measures might provide, for example, safe harbors for participation, requirements or incentives for participation, or ISAO cyber-threat data-sharing mechanisms that protect consumer interests, and so forth. Some approaches could entail budgetary considerations that would have to be addressed.

10.3.2 PUBLIC UTILITY COMMISSIONS

An ISAO represents an institutional approach to sharing information to reduce risk across public and private sectors. Cyber attacks have the potential to create catastrophic public risk. The dimensions of that risk and the ISAO construct indicate that an ISAO could be deemed a public utility—an entity engaged in benevolent efforts to protect the public from cyber threats and to help respond to a cyber-attack. As such, a state might consider comprehensively governing ISAO operations, including funding, within the authorities of its public utility commission.

10.3.3 STATE STRUCTURES AND BUDGET (PUBLIC SAFETY, NATIONAL GUARD, LAW ENFORCEMENT, ELECTIONS, EDUCATION, HEALTH, ETC.)

The mission of an ISAO is to lead cyber-threat exchange and analysis across its membership and related stakeholders. As such, its functions and workflow span the continuum of cyber-threat collection, analysis, and reporting. The outcome of this workflow is increased awareness, resilience, and deployment of defensive measures by members and stakeholders. By pooling this capability, there are cost savings to those members and stakeholders. Accordingly, a state and sub-government offices across the state may choose to establish a distinct budget line item to support ISAO operations in order to obtain the benefits of ISAO operations.

10.3.4 TELECOMMUNICATIONS

Cyber is generally understood to be part of the information and communication technologies (ICT) sector. Telecommunications are most commonly regulated at the federal level; however, public utility commissions, the cable industry, the wireless industry, and other ICT innovations and activities often intersect at state and municipality levels. Various tariff, licensing, and other fiscal mechanisms exist across the states that promote or regulate the ICT industry in ways that benefit the public. A state might consider incorporating ISAOs within this system of administration.

10.3.5 INSURANCE

Cyber insurance has become prevalent in the marketplace. Insurance is often regulated within states by an insurance commissioner. ISAOs present risk-reducing practices and information that could be useful for insurance purposes. As such, insurance commissioners, if properly empowered, could consider deploying fiscal measures to support ISAOs within their jurisdiction. Among them are establishing parameters with respect to the licensing and oversight of insurance carriers and cyber-insurance products.

10.3.6 DEPARTMENT OF REVENUE AND TAXATION

State taxation bureaus present a particularly efficacious ISAO use-case fiscal mechanism. Tax fraud through hacking has become widespread. ISAOs help combat this attack vector by informing members and stakeholders of attack trends and by sharing defensive measures. As such, a taxation authority could, if properly empowered, create fee-based or budgeted allocations to ISAOs that support the protection of tax authorities.

10.3.7 GENERAL TAXATION

A state might consider establishing a tariff, much like exists with telecommunications universal service taxes that are imposed upon all users, whereby the public benefits of ISAOs are partly funded through a taxation regime.

10.3.8 PUBLIC-PRIVATE PARTNERSHIP EXAMPLE

Having discussed the policy implications and benefits of public-private partnering in earlier sections of this document, we note that public-private partnership models offer a variety of differing use cases. In one model, it has come to be characterized by a system of outsourcing a public utility to a private vendor with certain start-up project funding and subsequent revenue-sharing arrangements after the service is offered for sale to the public. Toll roads, for example, have sometimes been created under this approach. A model like this could be established for ISAOs.

By way of example, the state of Wisconsin chose to create a public-private 501 (c)(3) partnership ISAO model with independent state departments having their own memberships as part of the model (e.g., the state CIO and departments under his purview have a single membership and the Wisconsin National Guard has its own membership to the ISAO). Wisconsin's choice was primarily based on legal issues, both financial and liability, regarding a state-directed public-private ISAO using public funds, as well as personnel responsible for running an ISAO. Additionally, the state CIO is prohibited from sharing governmental information with select private-sector partners. However, he is allowed to pay for membership with public funds and share governmental information with an operationally focused third party (e.g., ISAO) as part of a collective network defense initiative.

10.3.9 ECONOMIC DEVELOPMENT AND PRIVATE MARKETS

Information-sharing entities originally were established and operated in the private sector. As the model has matured, some entrepreneurs and leaders have viewed this capability, along with the cyber market more generally, as a valuable economic development initiative for communities. Accordingly, many states have created cyber initiatives that incorporate innovation, jobs programs, and other economic development dimensions. Other programs, both government funded and commercial, offer market-based efforts that could be used to support ISAOs.

States may want to look at these models and collaborate with associated organizations that advance private-sector approaches to establishing ISAOs.

10.3.10 COMPREHENSIVE, FEE-BASED ACROSS SYSTEMS OF ADMINISTRATION

A state may choose to design a fiscal model across all of its systems of administration, if properly empowered, whereby each regime pays a fee to support ISAOs. This would be a model in which the ISAO would universally support all systems of administration, rather than being instituted primarily within one.

11 FEDERAL RESOURCES

11.1 DHS

The DHS National Protection and Programs Directorate's Office of Cybersecurity and Communications (CS&C) is charged with helping to secure a stronger nation-wide cybersecurity risk posture through capabilities, products, and services. CS&C fosters trusted relationships among homeland security advisors, state-level CIOs, SLTT government officials, and stakeholder associations to better manage cyber risk. CS&C also leads, coordinates, and provides information on efforts that motivate actions to protect SLTT cyber interests, including providing federal government products, resources, and personnel to build partner capacity.

In support of its SLTT ISAO customers, CS&C facilitates connections with information-sharing programs and services. Many of these programs and services use a voluntary, collaborative approach to helping customers understand and manage their cyber risk. CS&C incorporates privacy and civil liberties protections in every product, tool, service, and program it offers.

In further support of information sharing and collaboration, CS&C leverages the functions of the Cybersecurity Framework developed by the National Institute of Standards and Technology: identify, protect, detect, respond, and recover.

11.2 PROGRAMS TO IMPROVE INFORMATION SHARING AND AWARENESS[7]

11.2.1 NATIONAL CYBER AWARENESS SYSTEM

Description: Cyber alerts and advisories. Timely information about security topics and threats via subscription to a mailing list. NCCIC provides current activity, alerts, bulletins, and security tips to stakeholders.

[7] See https://www.dhs.gov/.

11.2.2 HOMELAND SECURITY INFORMATION NETWORK

Description: Collaboration. The NCCIC portal provides stakeholders a platform to securely collaborate and share cybersecurity information, threat analysis, and products within trusted communities of interest.

11.2.3 SYSTEM FOR AUTOMATED INDICATOR SHARING

Description: Cyber threat indicator exchange. Enables real-time bidirectional exchange of cyber-threat indicators at machine speed, with the goal of reducing the number of cyber attacks.

11.2.4 CYBERSECURITY ADVISORS AND PROTECTED SECURITY ADVISORS

Description: Cybersecurity best practices, assessments, and support. Regionally located personnel who engage state and local governments, election crime coordinators, and vendors to offer immediate and sustained assistance, coordination, and outreach to prepare and protect from cyber and physical threats.

11.2.5 INDUSTRIAL CONTROL SYSTEMS ADVISORIES FOR STATE-OWNED CRITICAL INFRASTRUCTURE

Description: Incident advisories and reporting. Industrial Control Systems (ICS) specializes in control system incident alerts, tips, and advisories. Available publications include the *ICS-CERT Monitor*, a newsletter for personnel actively engaged in protecting critical infrastructure assets; joint security awareness reports for the public; and annual reports and white papers.

11.3 EDUCATION AND TRAINING

11.3.1 STOP. THINK. CONNECT TOOLKIT

Description: Educational material. Resources and materials to help promote cybersecurity awareness. Provides a better understanding of cyber threats and empowers people to be safer and more secure online.

11.3.2 FEDERAL VIRTUAL TRAINING ENVIRONMENT

Description: Career development. Online and on-demand cybersecurity training system for federal/SLTT government personnel and veterans. Courses range from beginner to advanced levels. Training is accessible from any Internet-enabled computer.

11.3.3 NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES CATALOG

Description: Career development. Catalog of more than 3,000 cybersecurity-related courses both online and in person from more than 125 different providers

across the nation. Courses are aligned to the specialty areas of the National Cybersecurity Workforce Framework.

11.4 FEDERAL BUREAU OF INVESTIGATION

The Federal Bureau of Investigation (FBI) is the lead federal agency for investigating cyber attacks by criminals, overseas adversaries, and terrorists and has many programs for the SLTT community as well as the private sector and citizens who are focused on improved cyber information sharing, cyber-crime prevention, reporting, and response. The FBI maintains an Office of Private Sector that provides an organized, coordinated, and horizontal approach as to how the FBI engages with the private sector. The FBI is an active participant in various regional InfraGard organizations, which are public/private not-for-profit institutions, that attempt to consolidate and exploit the knowledge bases and experiences of the participants. These are further described below.

11.5 PROGRAMS FOR LAW ENFORCEMENT

The Office of Partner Engagement handles outreach to the law enforcement community. There is a dedicated portal platform, Law Enforcement Online, for collaboration.[8]

11.6 CYBER TASK FORCES

Each field office has a cyber task force (CTF) to help investigate cyber crimes. These critical investigative groups are also involved in outreach to law enforcement and the private sector. When a company has had an incident and it contacts its local law enforcement, the CTF can help with advanced tools and cyber SMEs.

11.7 PROGRAMS FOR STATES, BUSINESSES, AND CITIZENS

11.7.1 THE INTERNET CRIMES COMPLAINT CENTER

The mission of the Internet Crime Complaint Center is to provide the public with a reliable and convenient reporting mechanism to submit information to the FBI concerning suspected Internet-facilitated fraud schemes and to develop effective alliances with law enforcement and industry partners. Information is analyzed and disseminated for investigative and intelligence purposes to law enforcement and for public awareness.

[8] For additional details, see https://www.fbi.gov/resources/law-enforcement.

This can be helpful to state and local entities when prioritizing what cyber crimes to focus on in terms of allocating budget resources for education and prevention.[9]

11.7.2 INFRAGARD

InfraGard is a partnership between the FBI and the private sector. It is an association of people who represent businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States.[10]

11.7.3 DOMESTIC SECURITY ADVISORY COUNCIL

The Domestic Security Alliance Council (DSAC) is a security and intelligence-sharing initiative between the FBI, the Department of Homeland Security, and the private sector. Created in 2005, DSAC enables an effective two-way flow of vetted information between the FBI and participating members to help prevent, detect, and investigate threats affecting American businesses.[11]

11.7.4 FBI CYBER DIVISION

The FBI Cyber Division is dedicated to getting cyber information into the hands of the field offices and subsequently to the private sector as well as SLTT entities. It focuses on disseminating strategic threat information on topics such as business email compromise and ransomware. Another key function of this group is to partner with government agencies, nonprofits, private industry, and academia to exchange detailed cyber information and indicators at all levels of classification to facilitate improved situational awareness and operations.[12]

11.7.5 NATIONAL CYBER TRAINING AND FORENSICS ALLIANCE

The National Cyber Training and Forensics Alliance (NCFTA)—created in 1997 and based in Pittsburgh—has become an international model for bringing together law enforcement, private industry, and academia to build and share resources, strategic information, and threat intelligence to identify and stop emerging cyber threats and mitigate existing ones.

The FBI Cyber Division's Cyber Initiative and Resource Fusion Unit (CIRFU) works with the NCFTA, which draws its intelligence from the hundreds of private-sector NCFTA members, NCFTA intelligence analysts, Carnegie Mellon University's Computer Emergency Response Team, and the FBI's Internet Crime Complaint Center. This extensive knowledge base has helped CIRFU play a key

[9] For more information, see https://www.ic3.gov/default.aspx, including annual reports located here: https://www.ic3.gov/media/annualreports.aspx.
[10] For more details, see https://www.infragard.org/.
[11] See https://www.dsac.gov/.
[12] See https://www.dsac.gov/.

strategic role in some of the FBI's most significant cyber cases in the past several years.[13]

11.7.6 DEPARTMENT OF HEALTH AND HUMAN SERVICES

This past year, the Department of Health and Human Services convened a cyber task force to develop recommendations on how to improve our cyber defenses for healthcare.[14]

11.7.7 NATIONAL INSTITUTE FOR STANDARDS AND TECHNOLOGY

The National Institute for Standards and Technology (NIST) is the creator of the Cyber Security Framework, a widely used benchmark on cyber hygiene.[15]

The NIST Cyber Center of Excellence is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges.[16]

12 CONCLUSION

Through this document, we have attempted to describe how ISAOs can be an effective mechanism in the national effort to combat the increasing cybersecurity threat that this nation will continue to experience, one that threatens our national security; the safety and dependability of our institutions, resources, and public services; and our personal, financial security. We have offered a variety of mechanisms for public-private cooperation within the ISAO movement, particularly directed at involving and telescoping the resources of the states to work synergistically with their private-sector counterparts. In doing so, we have described a number of approaches, structures, and existing state-level resources, as well as other federal adjuncts, that state, local, tribal, and other public entities might employ to work effectively within, or simply with, ISAOs. Current cybersecurity exigencies, coupled with severe state budgetary realities, compel this cooperative effort.

[13] For more information, see http://www.ncfta.net/.
[14] To view the report, see https://www.phe.gov/preparedness/planning/cybertf/documents/report2017.pdf.
[15] For additional resources, see https://www.nist.gov/cyberframework/industry-resources.
[16] To view a variety of projects and use cases, see https://www.nccoe.nist.gov.