Building a National Cyber Information-Sharing Ecosystem

Bruce J. Bakis
Edward D. Wang

May 2017

MITRE

This page intentionally left blank.

Summary

Introduction

This paper provides the authors' recommendations and guidelines for building an unclassified national cyber information-sharing ecosystem around a core of cross-sector regional partnerships for the following purposes:

- To enable widespread sharing of cyber-threat information and defensive measures to improve cyber defense, resilience, and risk management through improved situational awareness and collaboration
- To stimulate regional economies through a collaborative focus on education, workforce development, innovation, and research and development

The recommendations and guidelines are informed by lessons learned in establishing private-sector and public-private partnerships in the United States (U.S.) and by the authors' strategic insights on enabling an information-sharing ecosystem.

Cyber Information-sharing Landscape in the United States

Before summarizing several case studies and offering recommendations, this paper will establish context through an overview of the U.S. unclassified cyber information-sharing landscape. This paper will examine that landscape through a lens that focuses on cross-sector regional exchanges that operate as private-sector or public-private partnerships.

The Department of Homeland Security (DHS) is currently the U.S. Federal Government epicenter of the U.S. cyber information-sharing ecosystem. DHS essentially functions as the clearinghouse, integrator, analysis engine, and national source of cyber-threat information and defensive measures. It is responsible for the government's operational responses to major cybersecurity incidents, analyzing threats, and exchanging critical cybersecurity information with the owners and operators of critical infrastructures and businesses and with trusted partners around the world.

Cyber information sharing first emerged in the U.S. in the late 1990s and early 2000s in response to Federal Government directives calling for the creation of public-private partnerships focused on critical infrastructure protection. The first sectors to form Information Sharing and Analysis Centers (ISACs) were financial services, information technology, electricity, and water. ISACs are generally

organized as non-federal, not-for-profit, private entities that are typically funded by private-sector member fees, federal grants, or a blend of both. In many cases, the information shared by members is provided to the ISACs in anonymous form. The ISACs conduct a value-added analysis and distribute their findings back to the members, and typically federal stakeholders (e.g., DHS), in a form that protects the confidentiality of the data and sources.

Fusion Centers are government partnerships that provide regional cyber situational awareness and analysis at both the state level and major metropolitan level in the U.S.

InfraGard is a regional network of cross-sector, public-private partnerships composed of university, industry, and government entities that share cyber information concerning the security of, vulnerabilities in, and threats to critical infrastructure entities. The U.S. Federal Bureau of Investigation operates more than 80 InfraGard chapters in major urban areas throughout the U.S.

Information Sharing and Analysis Organizations (ISAOs) are the most recent type of partnerships to appear in the U.S. cyber information-sharing landscape. These organizations have the potential to transform the landscape by complementing the current sector-specific sharing model represented by ISACs with a more flexible model that can support a highly distributed, highly diverse, and highly connected sharing ecosystem that is driven by the private sector. The U.S. Federal Government, under a presidential executive order in 2015, directed DHS to encourage the formation of ISAOs. An ISAO is a flexible construct for catalyzing and operating almost any type of cyber information-sharing organization, ranging from informal affinity groups that represent private-private partnerships to formally chartered ISAC-like groups that represent public-private partnerships. The flexibility of an ISAO allows different forms of cross-sector, multidisciplinary, regional sharing, as well as information sharing to help safeguard events, such as major sporting events or conventions. The certification provisions in the executive order will eventually enable ISAO-to-ISAO sharing federations to form for even greater cyber situational awareness within the sharing ecosystem.

While outside the focused view of the U.S. sharing landscape, several other U.S. Federal Government actions and DHS programs are worth noting due to their impact on public-private cyber information sharing. The United States Computer Emergency Response Team (US-CERT) initially formed in 2000, and in 2002, DHS was assigned the responsibility for "responding to major incidents, analyzing threats, and exchanging critical cybersecurity information with trusted partners around the world." As it evolved from an incident "response" team to more of a

proactive defense team, US-CERT became known as the Computer Emergency *Readiness* Team.

Enhanced Cybersecurity Services is a voluntary critical infrastructure protection program whereby DHS shares sensitive and classified cyber-threat information with accredited Communications Service Providers (CSPs) through automated means. The CSPs use the information to block malicious traffic from entering customer networks.

The Cyber Information Sharing and Collaboration Program shares unclassified and anonymized cyber-threat information between DHS and participating private-sector partners.

The DHS National Cybersecurity and Communications Integration Center (NCCIC) is a "cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement."

The DHS Automated Indicator Sharing (AIS) program provides unclassified, bidirectional, machine-to-machine sharing of cyber-threat indicators between the NCCIC and the private-sector, ISACs, ISAOs, public-sector, and international partners and companies. AIS provides cyber information to its subscribers as messages formatted with the Structured Threat Information eXpression (STIX™) language that are transmitted via the Trusted Automated eXchange of Indicator Information (TAXII™) protocol.

The overview of the U.S. cyber information-sharing ecosystem concludes with the Cybersecurity Information Sharing Act (CISA) of 2015. CISA is the federal law that provides various protections to non-federal entities that share cyber-threat indicators or defensive measures with each other or with the Federal Government. CISA removes barriers that were impeding robust cyber information sharing in the U.S.

U.S. Landscape: Key Challenges

Informed by the evolution of the U.S. landscape, the authors provide the top six challenges, expressed as questions, that must be addressed to build a national unclassified cyber information-sharing ecosystem. These questions are listed below and addressed in the main body of the paper.

1. What guides the development of the ecosystem?
2. How balanced is the cyber information-sharing ecosystem?

3. What is predominantly shared?
4. How is automated sharing supported?
5. What will propel the ecosystem?
6. How does the government stimulate sharing?

Case Studies

As previously mentioned, three case studies of cross-sector regional ISAOs in the U.S. are presented in this paper: the Advanced Cyber Security Center (ACSC)—a success story of private-sector sharing; the Northeast Ohio CyberConsortium (NEOCC)—a model of effective public-private sharing; and the National Cyber Exchange (NCX)—a struggling partnership for public-private sharing.

The ACSC is a non-profit consortium, located in the Commonwealth of Massachusetts, that brings together university, industry, and government organizations to address cyber challenges. The primary focus is cross-sector regional collaboration to share unclassified cyber information to better defend against advanced cyber threats. The ACSC is an effective regional information-sharing partnership, but is not without challenges. The ACSC has not adequately invested in the organic resources needed to support its sharing mission or support its other missions pertaining to research and education and to advancing local and national policies and standards. As a cross-sector regional exchange, the ACSC is inherently diverse with respect to the varying levels of sophistication of cyber threats members face. The ACSC has not managed that diversity well, which has diminished the trust of some key members, owing to a perception among sophisticated defenders that less-sophisticated members may inadvertently imperil the value of shared information because of potentially unsophisticated operational security practices. Because the ACSC has not yet effectively addressed both issues, it has not yet reached its full potential, even after more than 5 years of operation.

The NEOCC, centered in Cleveland, Ohio, was launched in 2015 as a cross-sector regional partnership among universities, industries, and the government to share cyber information to improve defenses. The NEOCC is modeled on, but tempered by lessons learned from, the ACSC. As a result, the NEOCC quickly advanced from inception to its current state of effective sharing. Its current value proposition relies almost entirely on the in-kind labor contributions of members, which will need to change as the NEOCC more fully executes its sharing mission and adopts other missions. The NEOCC's effective relationship with the government and law enforcement is especially worthy of emulation.

The third case study is the NCX, which was formerly called the Western Cyber Exchange (WCX). The NCX is a U.S. consortium in Colorado Springs, Colorado, whose objective is to bring together university, industry, and government organizations to address cyber challenges. The NCX is a non-profit, member organization dedicated to improving cybersecurity and protecting critical infrastructure by sharing cyber-threat information, providing education and workforce development as well as technology development, and supporting members' cybersecurity needs. The WCX was established in 2010 as a regional consortium to address the cybersecurity needs of Colorado, Wyoming, and New Mexico. In 2016, the WCX rebranded and expanded its scope as the NCX to align with a state initiative for the University of Colorado at Colorado Springs to house and support a National Cybersecurity Center. A weak trust platform, the lack of shared purpose and operating principles, a highly diverse member base, and inadequate funding ultimately led to the restructuring of the WCX.

Case Studies: Key Challenges

Informed by the case studies, the authors provide the "Gnarly 9" top challenges, expressed as questions, that must be addressed to build a cross-sector regional cyber information-sharing group. These questions are listed below and addressed in the main body of the paper.

1. What is the essence of the consortium?
2. What are the implementation milestones?
3. What information will be shared by members, and how will it be shared?
4. What is the consortium's value proposition?
5. What are the membership criteria and composition?
6. How can members trust the consortium to safeguard their sensitive information?
7. How does the consortium fit into the local, regional, and global cyber ecosystems? What are the roles of government and law enforcement?
8. What is the consortium's leadership and governance?
9. What is the consortium's financial plan?

These challenges devolve to three critical success factors:

1. **Funding:** An ISAO needs adequate financial support to be successful.
2. **Trust:** Low trust crushes effective sharing.
3. **Shared vision and managed growth:** The vision needs to be collaboratively formed with stakeholders and guided by a comprehensive plan.

The Future of Cyber Information-sharing Partnerships

- Cyber information-sharing partnerships will proliferate, especially regionally, and the diversity of the domains and sectors they serve will increase.
- The trend of forming information-sharing organizations will mimic the hype cycle, with the current state being somewhere near the peak between mass-media hype and supplier proliferation. Eventually, there will be some consolidation before trekking up the slope of enlightenment.
- The certification of partnership entities will enable federations and federations-of-federations to form as trust circles organized by region, business domain, and purpose.
- Internet of Things consortia will begin to rapidly form to share cyber information associated with the intersection of device security and safety (e.g., medical devices, autonomous vehicles, on-board avionics).
- ISAO-like models will be repurposed to facilitate sharing within government organizations (e.g., intra-government ISAOs) as public partnerships.
- ISAO-like models will be repurposed for use in non-cyber domains (e.g., elections, fraud prevention).
- Sharing will increasingly occur as machine-to-machine transactions that are managed by trust contracts and chronicled as transactions on blockchain infrastructures.
- Shared information will increasingly incorporate adversary behavior elements and behavioral analytics, which are designed to detect real-time behavioral patterns of an unfolding cyber-attack.

Recommendations

The authors provide 11 recommendations, listed below and detailed in the main body of the paper, as implementation guidelines to building an unclassified national cyber information-sharing ecosystem around a core of cross-sector regional partnerships:

1. Convene workshops to collaboratively develop a strategy and roadmap for an unclassified cyber information-sharing ecosystem.
2. Enact legislation to catalyze the formation of a diversity of sharing centers.
3. Incrementally build the cyber information-sharing ecosystem from a strategic roadmap.
4. Catalyze ecosystem growth with cross-sector regional sharing groups.
5. Articulate the role of the government.
6. Articulate the missions and establish a differentiating value proposition.
7. Develop membership criteria and a governance model.
8. Establish foundations of trust.
9. Share the right data in the right way.
10. Actively manage cyber diversity.
11. Stimulate private-sector participation.

For Potential Further Examination

Several other U.S. ISACs and ISAOs are generally recognized as exemplars that would provide additional insights to the recommendations provided in this paper: the Financial Services ISAC, the National Cyber Forensics & Training Alliance, and the Arizona Cyber Threat Response Alliance.

Acknowledgments

The authors of this paper acknowledge *Australia's Cyber Security Strategy* as a major contributing source from which the cyber information-sharing ecosystem described in this paper emerged.

Contents

Figures

This page intentionally left blank.

1 Introduction

1.1 Purpose

This paper provides the authors' recommendations and guidelines for building an unclassified national cyber information-sharing ecosystem around a core of cross-sector regional partnerships for the following purposes:

- To enable widespread sharing of cyber-threat information and defensive measures to improve cyber defense, resilience, and risk management through improved situational awareness and collaboration
- To stimulate regional economies through a collaborative focus on education, workforce development, innovation, and research and development (R&D)

The recommendations and guidelines are informed by lessons learned in catalyzing private-sector and public-private partnerships in the United States (U.S.) and by the authors' strategic insights on enabling an information-sharing ecosystem.

1.2 Contents

This paper begins with a summary followed by Section 1, this introduction. Section 2 establishes context through an overview of cyber information-sharing models and the framework used to present case studies. Section 2 also provides an overview of the U.S. unclassified cyber information-sharing landscape that focuses on private-sector and public-private partnerships, especially cross-sector regional ones. Section 2 concludes with the authors' perspectives of the key challenges and how those challenges could be addressed.

Section 3 presents three case studies of cross-sector regional cyber information-sharing groups in the U.S.: The Advanced Cyber Security Center (ACSC), the Northeast Ohio CyberConsortium (NEOCC), and the National Cyber Exchange (NCX). Each case study concludes with the authors' impressions of how well the sharing groups operate. Section 3 concludes with the authors' perspectives of the key challenges and how those challenges could be addressed.

Section 4 provides the authors' recommendations on how to best address the challenges to building and operating a national unclassified cyber information-sharing ecosystem and its crucial growth engine—cross-sector regional information-sharing groups. The recommendations in Section 4 are detailed as implementation guidelines. The recommendation and guidelines are informed by the lessons learned for the evolution of the U.S. ecosystem and by the case studies of information-sharing partnerships. The heart of Section 4 provides build plans for the ecosystem and a pilot of a regional sharing group.

In Section 5, the authors provide a highly summarized, broad set of conclusions on how to build a national unclassified cyber information-sharing ecosystem and its core of cross-sector regional information sharing groups.

The first appendix in this paper (Appendix A) provides an overview of The MITRE Corporation's experiences with catalyzing information-sharing and analysis organizations. The appendices that follow (Appendices B through D) provide further context and amplification of key concepts discussed in the paper, including the different type of cyber threats, assembling cyber-threat intelligence for effective sharing, and maximizing the opportunities for sharing cyber information across the cyber-attack life cycle. The last appendix (Appendix E) lists and defines all acronyms and abbreviations used throughout this paper.

1.3 The Authors

The authors of this paper regard cyber partnerships as a crosscutting enabler of the pillars in any country's cybersecurity strategy. The authors believe that cyber partnerships, especially those focused on cyber information sharing, are a key means to achieving the goal of better managing and mitigating cyber risks to improve national, regional, and local cyber defenses.

The MITRE Corporation is a private, not-for-profit organization that manages and operates seven federally funded research and development centers that support U.S. Government sponsors. MITRE applies science, technology, systems engineering, and strategy to complex problems of global significance in the areas of aviation, critical infrastructure, cybersecurity, and defense (refer to Appendix A).

Bruce J. Bakis is the Manager of Cyber Information Sharing Partnerships at The MITRE Corporation. In his "Johnny Appleseed" role, Bakis focuses on cyber information-sharing partnerships and corporate cyber initiatives. Bakis serves on the Core Development Team of the Information Sharing and Analysis Organization (ISAO) Creation Working Group of the ISAO Standards Organization. He also serves on the Executive Committee of George Washington University's Institute for Information Infrastructure Protection. Additionally, Bakis serves on the Steering Committee of the ACSC, a cross-sector ISAO in Massachusetts. Bakis received his B.S. in Mathematics and M.S. in Computer Science from Northeastern University.

Edward D. Wang is a thought leader and regular contributor to the Cyber Information Sharing Partnerships activity at The MITRE Corporation. He specializes in Strategic Enterprise Planning and Execution and Organizational Development, with a focus on cyber information sharing. At MITRE, Wang has worked to establish

best practices for developing these partnerships. He has engaged with multiple domestic and international organizations to guide the growth of the cyber information-sharing partnership ecosystem by applying those best practices in a consistent and effective manner. Wang brings 20 years of industry experience in software development, systems integration, information technology strategy, and cyber information sharing from both the public and private sectors. Wang holds a B.A. in Computer Science from the University of Texas at Austin and an M.B.A. with a focus on Executive Leadership and Strategy from George Washington University.

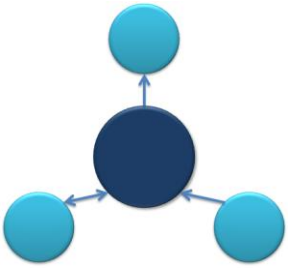
2 Context

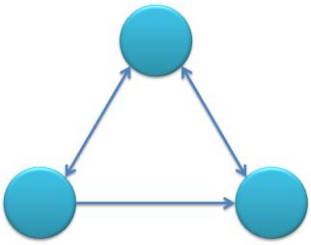
To help establish context and rationale for the recommendations and guidelines provided in this paper, this section contains overviews of cyber information-sharing models, the 10 elements used to frame each of the case studies, and the U.S. unclassified cyber information-sharing landscape. It concludes with the authors' assessment of the U.S. landscape and its near-term and long-term trajectory.

2.1 Cyber Information-sharing Models

Three basic models can be used to characterize cyber-threat information sharing: hub-and-spoke, peer-to-peer (post-to-all), and source-subscriber.[1] [2] Most cyber information-sharing organizations can be characterized as hybrids of these three basic models.

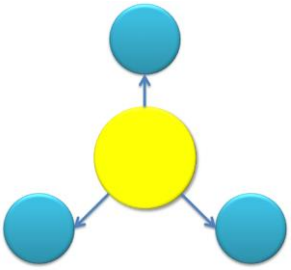
Hub-and-spoke: A central hub receives information from member spokes, operates on it, and distributes it to members. The spokes/members can be consumers or producers of information or both.





Peer-to-peer (post-to-all): Peers/members share directly with each other in a mesh pattern. Peers in the exchange may not always communicate with everyone.

Source-subscriber: A central source sends information to subscribers.



[1] Cyber Information-Sharing Models: An Overview, October 2012, The MITRE Corporation.
[2] Trusted Automated eXchange of Indicator Information (TAXII) - Enabling Cyber Threat Information Exchange, The MITRE Corporation.

2.2 Framework for Catalyzing and Piloting an ISAO

The MITRE framework for catalyzing and piloting an ISAO consists of the following components:

- The top 9 challenges that must be addressed early in the life cycle of an emerging ISAO—"the Gnarly 9"[3]
- Lessons learned[4] from MITRE's experience with helping to form ISAOs and establish and operate public-private partnerships
- A Strategy and Roadmap that guides, tailors, and codifies how challenges will be addressed as informed by lessons learned

Figure 1 illustrates the relationship between the Gnarly 9, lessons learned, the Strategy and Roadmap, and a pilot ISAO. The Gnarly 9 and lessons learned inform both the pilot and the Strategy and Roadmap, which can eventually be transformed into a business plan. The Gnarly 9 provides a useful framework to define the essence of an ISAO and initially address its emerging challenges. The Strategy and Roadmap is informed through the practical lessons learned during the pilot.

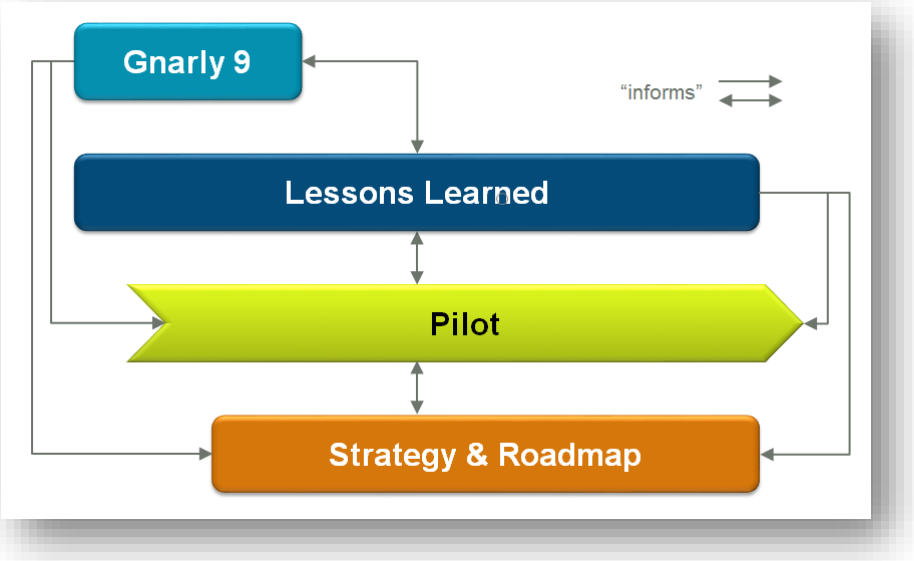


Figure 1. Relationship among Elements in the MITRE Framework

[3] https://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-blog/the-gnarly-nine-how-to-make-sure-your-isao-is

[4] https://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-blog/blueprint-for-cyber-threat-sharing-lessons

The Framework provides a context for exploring alternatives and defining requirements that shape the needed policies, procedures, processes, roles and responsibilities, as well as physical and technical infrastructures for a pilot.

The Strategy and Roadmap[5] has 10 key elements, which were adapted to frame the three regional ISAO case studies presented in Section 3:

1. **Charter:** mission, goals, objectives, principles and values, and value proposition
2. **Participation Agreement (Trust Model):** initial non-disclosure agreement (NDA), final NDA, individual NDA for sensitive information sharing, guest participation agreement, and rules of behavior
3. **Organizational Structure and Interactions:** policies, roles and responsibilities, staffing plan, governance model, intra-organizational interactions, extra-organizational interactions, and federation approach
4. **Membership Structure:** membership criteria and membership levels
5. **Service Offerings:** products and services provided to members/ stakeholders
6. **Financial Plan:** financial plan for the consortium
7. **Operations Plan:** sharing Concept of Operations (CONOPs), including what to share, roles, and how to share; CONOPs for other mission objectives, including Cyber Security Operations Center, synthetic engagement environment, malware analysis lab, and product evaluation and integration testbed; information sensitivity levels; sharing metrics; and strategies for establishing pilot operations, for using standards for secure automated sharing, and for federated sharing
8. **Engagement and Marketing Plan:** strategy for member engagement; external engagement through communications and events; and marketing and advertising, including the web and social media
9. **Infrastructure Plan:** hosting alternatives for technical infrastructure (e.g., outsourced, within consortium, cloud, member-hosted); strategy for application infrastructure (e.g., open source, commercial purchase, software as a service); and high-level requirements for physical, technical, and application infrastructures
10. **Implementation Plan:** strategic roadmap to implement the business plan, and strategic roadmap to develop physical, technical, and application

[5] B. Bakis, I. Lachow, E. Wang, *MITRE Cyber Information Sharing Services*, Public Release 15-1704, July 2015.

infrastructures: prelaunch, launch, piloting and infrastructure builds; transition to full operations; sustainment; and growth

2.3 U.S. Unclassified Cyber Information-sharing Landscape

The authors view the U.S. unclassified cyber information-sharing landscape through a lens that focuses on cross-sector regional exchanges that operate as private-sector or public-private partnerships.

The Department of Homeland Security (DHS) is currently the U.S. Federal Government epicenter of the U.S. cyber information-sharing ecosystem. DHS essentially functions as the clearinghouse, integrator, analysis engine, and national source of cyber-threat information and defensive measures. It is responsible for the government's operational responses to major cybersecurity incidents, analyzing threats, and exchanging critical cybersecurity information with the owners and operators of critical infrastructures and businesses and with trusted partners around the world.

Cyber information sharing first emerged in the U.S. in the late 1990s and early 2000s in response to Federal Government directives calling for the creation of public-private partnerships focused on critical infrastructure protection. The first sectors to form Information Sharing and Analysis Centers (ISACs)[6] were financial services, information technology, electricity, and water. ISACs are generally organized as non-federal, not-for-profit private entities that are typically funded by private-sector member fees or atypically funded by federal grants or a blend of both. Initial Financial Services Information Sharing and Analysis Center (FS-ISAC)[7] operations were funded by the government; member funding now primarily sustains operations. ISAC information-sharing sharing operations are a hybrid of hub-and-spoke, peer-to-peer (post-to-all), and source-subscriber models (refer to Section 2.1):

- **Hub-and-spoke:** ISACs serve as a central hub of information that is primarily, but not necessarily, provided by members in anonymous form. ISACs conduct value-added analysis and distribute their findings back to the members, and typically federal stakeholders (e.g., DHS), in a form that protects the confidentiality of the data and information sources.
- **Peer-to-peer (post-to-all):** ISACs typically provide email communications to their members, regularly hold conference calls with virtual online meeting support, and periodically hold face-to-face meetings, events, and conferences.

[6] https://www.dhs.gov/topic/cybersecurity-information-sharing
[7] https://www.fsisac.com/

- **Source-subscriber:** Members are often automatically subscribed to ISAC notifications or tailor them based on profiles (e.g., alerts). ISACs may subscribe to open-source and government cyber-threat intelligence feeds. However, they typically do not receive commercial feeds because licensing to an ISAC entity does not readily accommodate access to the feed by the many member organizations an ISAC.

Fusion Centers[8] are government partnerships that provide regional cyber situational awareness and analysis at both the state level and major metropolitan level in the U.S.

InfraGard[9] is a regional network of cross-sector, public-private partnerships among university, industry, and government entities that share cyber information concerning the security of, vulnerabilities in, and threats to critical infrastructure entities. The U.S. Federal Bureau of Investigation (FBI) operates more than 80 InfraGard chapters in major urban areas throughout the U.S. InfraGard information-sharing operations are a hybrid of hub-and-spoke, peer-to-peer (post-to-all) and source-subscriber models (refer to Section 2.1):

- **Hub-and-spoke:** InfraGard serves as a central hub of information that is primarily, but not necessarily, provided by members in anonymous form. InfraGard conducts value-added analysis and distributes its findings back to chapters and their members in a form that protects the confidentiality of the data and information sources.
- **Peer-to-peer (post-to-all):** InfraGard and its chapters typically provide email communications to their members, regularly hold conference calls, and periodically hold face-to-face meetings, events, and conferences.
- **Source-subscriber:** Members subscribe to InfraGard notifications typically though FBI email lists or RSS feeds.

ISAOs[10] are the most recent type of partnerships to appear in the U.S. cyber information-sharing landscape. These organizations have the potential to transform the landscape by complementing the existing sector-specific sharing model represented by ISACs with a more flexible model that can support a highly distributed, highly diverse, and highly connected sharing ecosystem that is driven by the private sector. The U.S. Federal Government, under a presidential executive

[8] https://www.dhs.gov/state-and-major-urban-area-fusion-centers
[9] https://www.infragard.org/
[10] https://www.dhs.gov/isao

order in 2015,[11] directed DHS to encourage the formation of ISAOs. An ISAO is a flexible construct for catalyzing and operating almost any type of cyber information-sharing organization, ranging from informal affinity groups that represent private-private partnerships to formally chartered ISAC-like groups that represent public-private partnerships. The flexibility of an ISAO allows different forms of cross-sector, multidisciplinary, regional sharing, as well as information sharing, to help safeguard events, such as major sporting events or conventions. As described in the three case studies in Section 3, ISAO information-sharing operations are typically a hybrid of hub-and-spoke, peer-to-peer (post-to-all) and source-subscriber models (refer to Section 2.1).

While outside the authors' focused view of the U.S. regional sharing landscape, several other U.S. Federal Government actions and DHS programs are worth noting due to their impact on public-private cyber information sharing. The United States Computer Emergency Response Team (US-CERT)[12] initially formed in 2000, and in 2002, DHS was assigned the responsibility for "responding to major incidents, analyzing threats, and exchanging critical cybersecurity information with trusted partners around the world."[13] As it evolved from an incident "response" team to more of a proactive defense team, the US-CERT became known as the Computer Emergency *Readiness* Team.

Enhanced Cybersecurity Services[14] is a voluntary critical infrastructure protection program whereby DHS shares sensitive and classified cyber-threat information with accredited Communications Service Providers (CSPs) through automated means. The CSPs use the information to block malicious traffic from entering customer networks.

The Cyber Information Sharing and Collaboration Program (CISCP)[15] shares unclassified and anonymized cyber-threat information between DHS and participating private-sector partners. Authorized partners may be eligible for physical access to the DHS National Cybersecurity and Communications Integration Center (NCCIC),[16] which is a "cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement."

---

[11] https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari
[12] https://www.us-cert.gov/
[13] https://www.us-cert.gov/about-us
[14] https://www.dhs.gov/enhanced-cybersecurity-services
[15] https://www.dhs.gov/ciscp
[16] https://www.dhs.gov/national-cybersecurity-and-communications-integration-center

The DHS Automated Indicator Sharing (AIS)[17] program provides unclassified, bidirectional, machine-to-machine sharing of cyber-threat indicators between the NCCIC and the private sector, ISACs, ISAOs, public sector, and foreign partners and companies. AIS provides cyber information to its subscribers as messages formatted using the Structured Threat Information eXpression (STIX)[18] language and sending them via the Trusted Automated eXchange of Indicator Information (TAXII)[19] protocol. STIX provides a common format for cyber-threat information. TAXII defines a set of protocols for securely exchanging cyber-threat information for real-time detection, prevention, and mitigation of cyber threats. Together, STIX and TAXII enable threat-sharing communities to exchange actionable, structured threat intelligence to promote collective defense.

The authors conclude this overview of the U.S. cyber information-sharing ecosystem with the Cybersecurity Information Sharing Act (CISA) of 2015.[20] CISA is the federal law that provides various protections to non-federal entities that share cyber-threat indicators or defensive measures with each other or with the Federal Government. CISA removes barriers that were impeding robust cyber information sharing in the U.S.

2.4 U.S. Landscape: Key Challenges and Perspectives

The key challenges in building and operating the U.S. national unclassified cyber information-sharing ecosystem are expressed here in the form of questions. The authors provide their perspectives on how those questions were addressed or could be more effectively addressed. The recommendations in Section 4 either answer or provide the context needed to address the questions posed here.

1. **What guides the development of the ecosystem?**
   Rather than guided by a strategic design, the growth of the U.S. cyber information-sharing ecosystem has been directed since the late 1990s by a series of Federal Government mandates and sharing programs in response to an evolving cyber threat.

2. **How balanced is the cyber information-sharing ecosystem?**
   ISACs and the US-CERT emerged from the need to protect critical infrastructures and key government resources. The long-standing prevalence of sharing in that context is now being better balanced with the emergence of ISAOs, which enable sharing in the broader context of better protecting

[17] https://www.dhs.gov/ais
[18] https://stixproject.github.io/
[19] https://taxiiproject.github.io/
[20] https://www.congress.gov/bill/114th-congress/senate-bill/754/text

universities as well as all industries, businesses, and citizens from a wide range of cyber threats.

3. **What is predominantly shared?**
   Cyber defenses in the late 1990s through the early 2000s were predominately intrusion-centric with a focus on perimeter protection and reactive responses to breaches by conventional cyber threats. During that era, ISAC members predominantly shared atomic data elements, such as suspect Internet Protocol addresses, regarding cyber threats. As threat actors became more sophisticated and increasingly began to target key commercial, industrial, and healthcare entities, the need to share contextualized data, referred to as cyber-threat information or intelligence, became apparent in the early 2010s (refer to Section 4.9). Federal Government sharing programs then began to emerge to better supply defenders and cyber analysts with the cyber-threat intelligence needed to fuel more effective, proactive, and resilient defenses.
4. **How is automated sharing supported?**
   The need to coherently share cyber-threat intelligence at a pace that matched the rapid tempo of cyber defensive operations spawned the government-sponsored development of standards—STIX and TAXII—to enable the secure, automated sharing of cyber information. Enabled by those standards, AIS began to provide an unclassified feed of cyber-threat information and defensive measures (refer to Section 4.9 for other automation standards and modes of cyber information exchange).
5. **What will propel the ecosystem?**
   In a prequel to the ISAO executive order in 2015, regional cyber information-sharing groups—like those described in the case studies in Section 3—increasingly began to dot the national landscape. Following that executive order, the pace of ISAO creation, especially cross-sector regional ISAOs, has greatly increased, as evidenced by state ISAO initiatives in Alabama, California, Indiana, Maryland, Texas, and Virginia.

   ISAOs, especially cross-sector regional ISAOs, will strengthen the U.S. national cyber defense ecosystem by necessarily complementing sector-based, critical-infrastructure information-sharing with partnerships that improve the cyber defenses of universities, industry, government, businesses, and citizens not otherwise categorized as critical infrastructures or key resources. Further, these partnerships will provide platforms to help stimulate cyber economies through a collaborative focus on education, workforce development, innovation, and R&D.

ISAO-to-ISAO sharing federations, enabled by the certification provisions in the ISAO executive order, will further propel the ecosystem by enhancing cyber situational awareness.

6. **How does the government stimulate sharing?**
   The U.S. Federal Government stimulates unclassified cyber information sharing among private-sector entities in several ways. First, the ISAO executive order, catalyzing ISAO growth and enabling ISAO-to-ISAO sharing federations to develop. Second, providing protections under CISA that reduce perceived barriers to sharing. And, finally, providing a source of unclassified cyber-threat intelligence through the AIS program that enables secure, standards-based automated sharing. These stimuli, combined with an increased supply of open-source and commercial cyber threat intelligence, provide the needed elements to develop a national cyber information-sharing ecosystem.

   While the Federal Government is the primary driver of cyber information sharing in the United States, there is some state-level stimulus. It typically is provided by state-level commissions and task forces that advocate for cyber information sharing to better defend state ICT assets. However, some states, as discussed above, have stimulated cyber information sharing through ISAO initiatives. For example, the Commonwealth of Virginia has provided funding to catalyze the Virginia ISAO (refer to Appendix A, Section A.5).

Strategically looking ahead, the authors believe that the following will occur:

- Cyber information-sharing partnerships will proliferate, especially regionally, and the diversity of the domains and sectors they serve will increase.
- The trend of forming information-sharing organizations will mimic the hype cycle, with the current state being somewhere near the peak between mass-media hype and supplier proliferation. Eventually, there will be some consolidation before trekking up the slope of enlightenment.
- The certification of partnership entities will enable federations and federations-of-federations to form as trust circles organized by region, business domain, and purpose.
- Internet of Things consortia will begin to rapidly form to share cyber information associated with the intersection of device security and safety (e.g., medical devices, autonomous vehicles, on-board avionics).
- ISAO-like models will be repurposed to facilitate sharing within government organizations (e.g., intra-government ISAOs) as public partnerships.

- ISAO-like models will be repurposed for use in non-cyber domains (e.g., elections, fraud prevention).
- Sharing will increasingly occur as machine-to-machine transactions that are managed by trust contracts and chronicled as transactions on blockchain infrastructures.
- Shared information will increasingly incorporate adversary behavior elements and behavioral analytics, which are designed to detect real-time behavioral patterns of an unfolding cyber-attack (refer to Appendix C) .

3 Case Studies

This section provides three case studies of cross-sector regional ISAOs in the U.S.: the ACSC—a success story of private-sector sharing; the NEOCC—a model of effective public-private sharing; and the NCX—a struggling public-private partnership.

This section concludes with the authors' summary of regional ISAO lessons learned and challenges.

3.1 U.S. Advanced Cyber Security Center[21]

The ACSC[22] is a non-profit consortium located in in the Commonwealth of Massachusetts that brings together university, industry, and government organizations to address cyber challenges. The primary focus is cross-sector regional collaboration to share unclassified cyber information to better defend against advanced cyber threats.

The ACSC has registered as a regional ISAO with the Information Sharing and Analysis Organization Standards Organization (ISAO SO).[23]

3.1.1 Missions and Vision

The ACSC has three missions:

1. **Threat Evaluation/Information Sharing:** operating as a regional ISAO to share and collaboratively analyze unclassified cyber-threat and defensive measures
2. **Research and Education:**
   - Engaging in cyber R&D and providing an innovation bridge to connect cyber R&D, business, and government needs
   - Creating education programs that will address the shortfall in cyber talent
3. **Policy/Legal:**
   - Advancing public policies that will enhance security
   - Developing and advancing standards and metrics for cyber risk management and cyber-threat forecasting

[21] The ACSC Board of Directors has recommended strategic changes to address many of the challenges described herein and has appointed a new Executive Director to reimagine the organization as ACSC 2.0.
[22] http://www.acscenter.org/
[23] https://www.isao.org/information-sharing-groups/

The vision of the ACSC is that it "will be a national leader in cybersecurity, and the major driver to make New England a regional cyber center of excellence."[24]

3.1.2 Trust Model

The ACSC Participation Agreement[25] establishes a foundation of trust among members of the ACSC. The agreement is executed at the corporate level of participating organizations. There is, however, an optional provision for an individual employee NDA (no participating organization has opted for this yet).

The trust foundation supports, and is further enhanced by, regular face-to-face cyber information exchanges (refer to Section 3.1.5).

Occasionally, non-members ask or are invited to participate in Cyber Tuesdays (CTs), during the session when sensitive information is typically shared. Non-members are allowed to participate in that session only with the approval of CT members and only if the non-members execute a special NDA known as the "ACSC Volunteer NDA." The protection requirements in that NDA are like the participation agreement.

In 2011, an initial trust baseline was established by the ACSC Phase I Participation Agreement to provide an initial set of protections to jump-start information sharing. This new agreement was like the current agreement, except that it did not include provisions for ownership rights of derivative products developed from shared information, royalty-free licensing, or highly sensitive information.

3.1.3 Organizational Structure and Interactions

3.1.3.1 Governance

The ACSC is a non-profit organization incorporated in 2012 in Massachusetts under the tax-exempt 501(c)(3) section of the U.S. Internal Revenue Code. It operates at The MITRE Corporation in Bedford, Massachusetts, with the support of Mass Insight Global Partnerships (MIGP),[26] which is the founding organization of the ACSC.

---

[24] The Advanced Cyber Security Center (ACSC) vision is currently articulated in the online job description for the Executive Director position:
http://www.acscenter.org/about/ExecutiveDirector2016.html

[25] http://www.acscenter.org/initiatives/acsc_participation_agreement_january_2014.pdf

[26] Mass Insight Global Partnerships (MIGP) is a Boston-based consulting and research firm that builds strategic pre-competitive alliances among higher education, industry, and government, both regionally and globally.

A Board of Directors (BoD), formed in 2012, provides strategic direction and financial oversight of the ACSC. Since forming, MIGP has chaired the BoD with the Federal Reserve Bank of Boston as vice chair; MITRE served on the BoD until its Chief Security Officer left the corporation. The ACSC Executive Director, first hired in 2012, is responsible for carrying out the general affairs of the ACSC that are subject to the direction and control of the BoD.

In 2008, an informal group of interested participants, led by MIGP, guided the formation of the "Massachusetts IT Security Research Center." In 2009, that informal group was designated as the Advisory Board.

In 2010, a Steering Committee replaced the Advisory Board as the ACSC guiding body.

In 2011, the Steering Committee created three Work Groups to provide specialized guidance: Threat Evaluation/Information Sharing, Research and Education, and Policy/Legal.

In 2012, the Steering Committee was dissolved, but the Work Groups were retained.

Steering Committees convened by the ACSC are now, again, one of governance constructs available to members. For example, a Collaborative Defense steering committee was recently convened by the ACSC to help drive participation in the Annual Conference.[27]

3.1.3.2 Staff and Support

An Executive Director and a Program Support Specialist manage the ACSC operations.

MIGP provides strategic and administrative support services (information and communication technology [ICT], human resources, finance, communications, conference, and strategic development support) under contract to the ACSC.

[27] http://www.acscenter.org/news-events/news_details.html?id=1011

3.1.3.3 Interactions

The clear majority of member interaction is focused on cyber information sharing among cyber defenders and threat analysts.

- **Government:** Typical cyber information-sharing interactions with the Massachusetts state government and the U.S. Federal Government include the following:
  - The Massachusetts Office of Information Technology (MassIT) is the state agency that is the member of the ACSC. Cyber defenders and analysts from MassIT typically interact with ACSC members through CTs and other information-sharing events.
  - Cyber analysts from the Massachusetts National Guard and the Massachusetts State Police who are detailed to the Commonwealth Fusion Center also typically interact with ACSC members through CTs and other information-sharing events.
  - State and U.S. Federal Government agencies (e.g., the DHS) typically interact with the ACSC as invited guests and presenters at ACSC information-sharing events where no sensitive information is disclosed.
  - Some commercial-sector members prefer to not have law enforcement or government members in the ACSC. They believe that law enforcement entities could be compelled to share sensitive information in the context of investigations and legal proceedings that was otherwise shared in confidence among ACSC members in the context of cyber defense. They also believe that government members may not be sufficiently trusted to appropriately safeguard sensitive information.
- **Non-members:** Typical ACSC interactions with non-members include the following:
  - Vendors who are invited to information-sharing events to provide product and service overviews to ACSC members or to serve as panelists at information-sharing events where no sensitive information is disclosed
  - Special guests who are invited to participate in ACSC information-sharing events where sensitive information is typically disclosed. These guests may participate only after they sign an ACSC NDA (refer to the "ACSC Volunteer NDA" described in Section 3.1.2).

3.1.4 Membership

There are currently 21 member organizations in the ACSC. There are two broad categories of membership—Premium and Associate—that are differentiated by service and product packages (refer to Section 3.1.5) and annual membership fees (refer to Section 3.3.10).

3.1.4.1 Composition

Defense
▪ MIT Lincoln Laboratory ▪ MITRE

Financial Services
▪ Eastern Bank ▪ Federal Reserve Bank of Boston ▪ John Hancock Financial Services ▪ Liberty Mutual Group ▪ State Street Corporation

Government
▪ Commonwealth of Massachusetts: Information Technology Division, Fusion Center (State Police), National Guard

Healthcare
▪ Harvard Pilgrim Health Care

Legal
▪ Foley Hoag

Technology
▪ Acquia ▪ Carbon Black ▪ Facebook ▪ RSA/Dell Technologies ▪ Veracode

Universities
▪ Harvard University ▪ MIT
▪ Northeastern University
▪ University of Massachusetts
▪ Worcester Polytechnic Institute

Biotechnology/Pharmaceutical
▪ Vertex

3.1.4.2 Joining and Vetting

The Executive Director and Program and Membership Manager are primarily responsible for member prospecting and vetting. Prospective members may apply to join the ACSC by completing an online application.[28]

Prospective members are typically engaged at the security officer level. Academic members are typically engaged through the security officer or chief information officer.

Prior to participation, member organizations must sign an NDA (refer to Section3.1.2).

[28] http://www.acscenter.org/membership/acsc-application-2014.pdf

3.1.4.3 Onboarding

Member onboarding generally consists of a face-to-face overview briefing given by the ACSC Executive Director with the ACSC staff (refer to Section 3.1.3). Typically, MITRE provides an overview of the ACSC virtual sharing, collaboration, and analysis platforms (refer to Section 3.1.8).

3.1.5 Products, Services, and Events

Products, services, and events support the ACSC's missions and vision.

3.1.5.1 Threat Evaluation/Information Sharing

- **Cyber Tuesdays:** CTs are biweekly, face-to-face cyber information-sharing sessions among cyber defenders and analysts, and are hosted at locations that alternate between MITRE in Bedford, Massachusetts, and the Federal Reserve Bank in Boston, Massachusetts. The 3-hour meeting (9:00 a.m-12:00 p.m.) is facilitated by the Federal Reserve Bank and follows this general agenda:
  - Cyber defense best practices member presentation, which often takes the form of a cyber-threat briefing given by MITRE or another member organization
  - Roundtable discussion of threat indicators and cyber defense best practices
  - Invited vendor presentation on cyber defense tools
- **Collaborative Research Into Threats (CRITs):** CRITs[29] is an open-source repository and analysis platform for cyber-threat information that was originally prototyped by MITRE for its own use. MITRE hosts an ACSC instance of CRITs that is externally accessible by ACSC cyber defenders and analysts.
- **Cyber Portal:** MITRE hosts a web portal (based on JForum,[30] an open-source discussion board system) that is externally accessible by ACSC cyber defenders and analysts to share and discuss cyber threats and defensive measures. The portal serves as the ACSC repository of materials presented at CTs.
- **Group Email List:** MITRE uses its Listserv platform to support a group email list for ACSC cyber defenders and analysts.

[29] https://crits.github.io/
[30] http://jforum.net/index.jsp

- **Handshake Group:** MITRE hosts an ACSC group on Handshake,[31] which is an Elgg[32]-based social networking and collaboration site.
- **ACSC Website:** The ACSC uses a third party to host its website.[33] Most content is developed by MIGP. The website has a members-only sitelet to deploy sensitive content.
- **Cyber Exchange Forums (CEFs):** CEFs are quarterly cyber information-sharing meetings to discuss topics of interest to leaders in the ACSC member organizations. While CTs are geared toward tactical defenders, CEFs are geared toward strategists. The format is generally several morning-long panel discussions among subject matter experts. CEFs are hosted in member conference facilities. Attendance is open to members and invited guests.
- **ACSC Annual Conference:** The Annual Conference[34] is held in November and hosted at the Federal Reserve Bank of Boston. The typical format is several short, morning plenary sessions; breakout sessions in the afternoon, where panels of subject matter experts discuss the breakout topics; a final plenary session; student poster completion; and a concluding reception.
- **Workshops, Meetings, and Events Planning and Facilitation:** This is a core service that the ACSC and MIPG provide to members. Members are key collaborators in planning and presenting at CTs, CEFs, workshops, the Annual Conference, and other ACSC events and meetings.
- **Communications:** This is a core service that the ACSC and MIPG provide to members and the public. Communications are distributed via email and are posted on the ACSC website. Examples of communications include the following:
    - Summary reports of CEFs: *Cloud Computing Cyber Exchange Forum Summary Report*[35] and *Cyber Resiliency Cyber Exchange Forum Summary Report*[36]
    - Summary reports of the Annual Conference: *2015 ACSC Conference Summary Report*[37] and *2014 ACSC Conference Summary Report*[38]
    - Special reports on strategic cyber issues and responses to Requests for Information (RFIs): *The New England Cybersecurity Consortium: A*

[31] https://handshake.mitre.org/
[32] https://elgg.org/
[33] http://www.acscenter.org/
[34] http://www.acscenter.org/news-events/acsc_2016_annual_conference_-_save_the_date/
[35] http://www.acscenter.org/resources/acsc-cef-summary-cloud_computing-may.pdf
[36] http://www.acscenter.org/resources/acsc-cef-summary-resiliency-october.pdf
[37] http://www.acscenter.org/news-events/Newsletter/acsc-conference-summary-121815.pdf
[38] http://www.acscenter.org/resources/2014-acsc-conference-summary.pdf

Paradigm Shift in Education and Workforce Development in Security Fields[39] and *ACSC Rollout Proposal to address the Cyber Challenge*.[40] ACSC members are key collaborators in formulating responses to RFIs.

3.1.5.2 Research and Education

- **Research Projects:** In 2012, two "prime-the-pump" small cyber R&D research projects were launched: *Cybersecurity Risk Analysis and Investment Optimization,* and *A Platform for Data-Intensive Cybersecurity Monitoring*.[41] The projects were each funded at $75K (in U.S. dollars [USD]) by a small group of ACSC financial services member organizations.
- **Research Proposals:** The "prime-the-pump" research projects were completed in 2013 and resulted in a research proposal to the U.S. National Science Foundation: *Cybersecurity Risk Analysis based on Financial Engineering and Big-Data Analytics (CRAFA)*.[42] That proposal was not funded.
- **Cyber R&D Platform:** In 2014, the ACSC developed its cyber R&D platform, consisting of the following:
  - Data Sharing Agreement: A data sharing agreement between several members was executed to establish a virtual warehouse in support of big data analytics research.
  - ACSC Research Consortium: The ACSC New England Cyber Security Research Consortium was formed.[43]
- **Academic Resource Guide:** *New England Cyber Security Academic Resource Guide*[44]
- **Intern Job Fairs:** The ACSC hosts job fairs for member companies looking to hire undergraduate and graduate students in cyber and ICT for internships or full-time positions (e.g., ACSC Intern Fair, October 7, 2016[45]).
- **Cyber Poster Competitions:** The ACSC hosts poster competitions for students at its Annual Conference (e.g., *Two winners announced for the ACSC Cybersecurity Poster Session*[46]).

---

[39] http://www.acscenter.org/resources/acscwhitepaper11-12-2012.pdf
[40] http://www.acscenter.org/resources/acsc_rollout_proposal_april_2013.pdf
[41] http://www.acscenter.org/ascsprimethepump_011414.pdf
[42] http://www.acscenter.org/resources/cybersecurity_risk_analysis_summary_(2).pdf
[43] The New England Cybersecurity Consortium: A Paradigm Shift in Education and Workforce Development in Security Fields
[44] http://www.acscenter.org/resources/2015_academic_resource_guide_for_web.pdf
[45] http://www.acscenter.org/news-events/event_details.html?id=982
[46] http://www.acscenter.org/news-events/two_winners_announced_for_the_acsc_cybersecurity_poster_session/

3.1.5.3 Policy/Legal

- **ACSC Participation Agreement** (refer to Section 3.1.2): The trust-related provisions include the following:
  - Confidentiality, safeguarding, and permitted uses of sensitive information
  - Rights of ownership and intellectual property rights of sensitive information and derivative works
  - Background check requirement
  - Non-solicitation of employees
  - Protection of highly sensitive agreement under one or more separate agreements between participants (no participating organizations have opted to do this yet)
- **Summaries of State and Federal Laws on Security and Privacy:** Foley Hoag LLP has developed numerous summaries of state and federal laws on information security and privacy, including the following:
  - *Pending Federal Initiatives to Further Regulate Data Privacy and Cyber Security*[47]
  - *State-By-State Data Security Overview*[48]
  - *Federal and State Laws Regulating Data Privacy and Security*[49]
  - *Federal Statutes Impacting Data Security*[50]
- **Funding Advocacy:** The Policy/Legal Work Group has advocated for Massachusetts state economic development bills to encourage cyber innovation-focused and R&D activities. That advocacy has not yielded any ACSC funding.

3.1.6 Operations

ACSC information-sharing operations can be characterized as a hybrid model of the hub-and-spoke and peer-to-peer (post-to-all) models (refer to Section 2.1):

- **Peer-to-peer (post-to-all):** Most sharing is face-to-face (e.g., CEFs, CTs) and/or via email.

---

[47] http://www.acscenter.org/initiatives/pending_federal_initiative_to_further_regulate_data_privacy_and_cyber_security.pdf

[48] http://www.acscenter.org/news-events/foley_hoag_llp_on_state_data_security_law_table.pdf

[49] http://www.acscenter.org/news-events/foley_hoag_llp_on_current_law_governing_data_security.pdf

[50] http://www.acscenter.org/news-events/foley_hoag_llp_on_federal_data_security_legislation.pdf

- **Hub-and-spoke:** The ACSC serves as a central hub of information (e.g., CRITs, Cyber Portal, ACSC website) and services that are distributed and provided to members (spokes).

Three Work Groups that are aligned with the ACSC missions (refer to Section 3.1.1) focus on ACSC operations: Threat Evaluation/Information Sharing, Research and Education, and Policy/Legal.

In the context of Threat Evaluation/Information, there are two basic levels of cyber information sharing in the ACSC:

- **Strategic (for executives, senior managers, and technical architects):** defense strategies, risks, policies, investment strategies, workforce development, awareness, metrics, and approaches for communicating risk and effectively advocating for cyber defense and resiliency
- **Tactical (for computer network defenders):** cyber observables; indicators; incidents; targets; adversary and defensive tactics, techniques, and procedures (TTPs) (best practices); campaigns; courses of action; cyber actors; analyses; and actionable unclassified intelligence

All information shared is unclassified and typically is not anonymized. Information shared on CTs is uploaded in the Cyber Portal and/or input to CRITs.

3.1.7 Outreach and Marketing

Numerous ACSC products, services, and events provide public outreach and marketing: website, Annual Conference, and communications (refer to Section 3.1.5).

The ACSC Executive Director is primarily responsible for member prospecting (refer to Section3.1.4). The BoD, Executive Director, principals of the Work Groups, and MIGP provide outreach for ACSC advocacy and support within Massachusetts and the U.S. Government.

3.1.8 Infrastructure

3.1.8.1 Physical

The ACSC physical infrastructure and general office space support services (e.g., telecommunications, guest access to the Internet, utilities, and custodial services) are provided by MITRE at its Bedford, Massachusetts, campus. The ACSC currently occupies approximately 600 square feet of office space and an additional

800-1,000 square feet of contiguous common meeting and collaboration space that is shared with other tenants with whom MITRE is incubating or collaborating.

Additionally, MITRE hosts CTs and other ACSC meetings (refer to Section 3.1.5) in a meeting room adjacent to the ACSC office space located outside the MITRE security perimeter (MITRE is a government-approved facility for the stewardship of classified information and systems). CTs are supported through an audio teleconference bridge and virtual online meeting platform to allow remote participation. There are large, high-definition televisions in the CT meeting rooms to display briefing materials. The CT meeting room at MITRE–Bedford supports external Internet-protocol video teleconferencing to non-MITRE locations.

ACSC employees have been approved for 24-hour access to the entire MITRE–Bedford campus, except in controlled-access locations approved for the storage or processing of classified information. This provides ACSC employees with unescorted access to most meeting and conference rooms within the MITRE–Bedford security perimeter.

As discussed in Section 3.1.10.3, the Federal Reserve Bank hosts and supports CTs and other information-sharing events, including the ACSC Annual Conference, in its Boston offices.

3.1.8.2 Virtual

Apart from website hosting, MITRE hosts and supports the entire infrastructure for virtual sharing, collaboration, and analysis, including CRITs, ACSC Portal, ACSC Group Email List, and ACSC Handshake Group (refer to Section 3.1.5.1).

3.1.9 Key Milestones

- In 2007, the kernel of the idea for a cybersecurity center for research and cyber information was formed. In 2008, the Massachusetts IT Security Center was formed.
- In 2009, an Advisory Board was formed and renamed the emerging consortium as the ACSC.
- In 2010, the ACSC first began to regularly share cyber-threat information at MITRE among a very small group of cyber defenders.
- On September 11, 2011, the ACSC held its launch conference at MITRE–Bedford.
- In 2012, the ACSC was incorporated as a 501(c)(3) non-profit organization, an Executive Director was hired, and two small cyber R&D projects ($75K

each and funded by small-group financial services member organizations) were launched

- In 2013, a cyber-threat information repository and analysis platform—CRITs (refer to Section 3.1.5.1)—was adopted, and the small cyber R&D projects were completed.
- In 2014, the ACSC and the Western Cyber Exchange (WCX), now the NCX, exchanged threat information formatted as STIX by using the TAXII protocol (refer to Section A.10 of Appendix A) in an interoperability test of standards-based, secure, automated sharing. The ACSC also formed its cyber R&D platform (refer to Section 3.1.5.2).
- In 2016, the ACSC refocused its cyber R&D agenda on translational research using data sets provided by members.

3.1.10 Financial Plan (USD)

3.1.10.1 Revenue

Annual membership fees are the primary source of funding for the ACSC. The fees are based on a member's annual revenue:[51]

- Premium Member
  - Large Business/Government (annual revenue > $1B): $50K
  - Smaller Business/Non-profit/Academic (annual revenue < $1B): $25K
- Associate Member
  - Mid-size Business (annual revenue = $500M–$1B): $20K
  - Smaller Business/Non-profit/Academic (annual revenue < $500M): $10K

The estimated annual revenue of the ACSC from membership fees is $1M.

When the ACSC launched in 2011, the Massachusetts Technology Collaborative awarded $50K (USD) to MIGP to help establish the ACSC. Prior to and after that, the ACSC was supported as an MIPG corporate initiative with the in-kind and pro bono support of numerous catalyzing future ACSC members.

The ACSC receives some financial support from venture capital firms in the form of sponsorships for events. For example, .406 Ventures[52] and Allied Minds[53] traditionally sponsor the student poster sessions at the ACSC Annual Conferences.

[51] http://www.acscenter.org/membership/11_acsc-memberships-2016.pdf
[52] http://www.406ventures.com/
[53] http://www.alliedminds.com/

The ACSC Sponsorship Program is an additional potential revenue source. Sponsorships for the Annual Conference range from the Platinum Level at $25K to advertisement in the program guide for $1K.

3.1.10.2 Expenses

The estimated major annual expenses are as follows:

- Staffing (two positions): $360K
- Outsourced support (ICT, website hosting, communications, planning, strategic consulting): $500K

3.1.10.3 Member In-Kind/Pro Bono Contributions

MITRE hosts the technical infrastructure to support cyber information sharing and analysis as well as office space and basic support services, at no cost to the ACSC.

Many members support ACSC operations through contributions of labor, products, and services. For example, the Federal Reserve Bank of Boston chairs biweekly CT meetings (refer to Section 3.1.5.1) and hosts every other CT meeting (once per month) in its Boston, Massachusetts, offices. Additionally, the Federal Reserve Bank of Boston hosts the ACSC Annual Conference. Generally, these meeting are hosted at no cost, or at a nominal fee to cover food and beverages. Foley Hoag LLP provides substantial pro bono legal support to the ACSC, as do corporate legal counsel and several other ACSC member organizations.

3.1.10.4 Member Labor Cost to Participate

Labor, travel, and other costs to attend and participate in ACSC information sharing and other events are borne by member organizations. Very roughly, member organizations invest 126 staff hours annually, equivalent to $13K (USD):[54]

- 104 staff hours for one cyber defender/analyst to attend biweekly CT meetings
- 16 hours to attend quarterly CEFs, the Annual Conference, and other ACSC events
- 6 hours to voluntarily prepare two briefings for presentation at CTs, CEFs, or the Annual Conference

[54] Assumptions: 4 hours per CT meeting, including travel with two CTs per month; 4 hours per CEF, including travel with four CEFs per year; and $150K (USD) annual raw salary with an additional 40% fringe benefit rate.

Many members invest considerably more than the hours listed above because more than one cyber defender/analyst and several executives actively engage with the ACSC.

3.1.11 Impressions

- **Overall:** The ACSC is an effective regional information-sharing partnership, but it is not without challenges. The ACSC has not adequately invested in the organic resources needed to support its sharing mission or support its other missions pertaining to research and education and to advancing local and national policies and standards.
- **Missions and Vision:** The ACSC has three primary missions: cyber information sharing, research and education, and policy advocacy. Because of under-investing in all but its information-sharing mission, the ACSC has not gained traction in executing its other missions. Without a dedicated focus and investment to staff its other missions, especially the cyber R&D mission, the other missions are likely to remain aspirational.
- **Trust Model:** The ACSC Participation Agreement has served as a model that has been emulated by many other cyber information-sharing groups. The face-to-face focus of the ACSC has been an effective way to further build member trust to enable engaged and valued cyber information sharing. Nevertheless, the trust baseline and sharing robustness need to increase, as evidenced by the slow growth in cyber indicators of compromise in the ACSC cyber-threat repository. As a cross-sector regional exchange, the ACSC is inherently diverse with respect to the varying expertise of cyber defenders and analysts in organizations that address different kinds of cyber threats (refer to Appendix B). Distrust among defenders in a highly diverse sharing group (further discussed in Section 3.5.2) can arise when information shared by experts is acted upon by less-expert defenders/analysts using relatively unsophisticated operational security practices (e.g., open-source queries on malware samples and other indicators of compromise) that potentially jeopardize the intelligence value of the original shared information (e.g., a command-and-control infrastructure that was established to target a specific victim). Section 4.8 provides recommendations for improving trust to enable more robust cyber information sharing.
- **Organizational Structure and Interactions:** The ACSC has not been adequately staffed, either in number or subject matter expertise, to effectively execute its three missions. Consequently, the value derived from membership in the ACSC often comes from the efforts of the members themselves or other sources of in-kind labor contributions rather than ACSC staff. This staffing challenge has most affected the ability of the ACSC to

execute its cyber R&D mission. In MITRE's experience, a viable cyber research consortium typically needs a full-time, experienced, and well-connected research director and at least two additional full-time staff.

The ACSC is considering several new modes of member interactions, including classified information exchanges and a subgroup of highly capable cyber defenders and analysts.

- **Membership:** Cross-sector regional sharing groups, such as the ACSC, have several advantages over sector-based sharing groups. First, these cross-sector sharing groups can leverage the proximity of members and focus on face-to-face interactions as an effective way to build trust. Second, their cross-sector composition improves more early-warning opportunities (like a canary in a coal mine) than sector-based sharing groups (refer to Section 4.4.1).

  Unfortunately, the diversity within regional sharing organizations can also inhibit effective sharing. Organizations from different sectors often have very different operating modes, hold very different digital assets, face different types of cyber threats, and have different organizational practices. These differences create roadblocks to sharing (refer to Section 3.5.2).

  The face-to-face focus of the ACSC may ultimately limit the size of the membership base. The logistics to accommodate more than 35 to 40 member organizations in regularly occurring face-to-face meetings are difficult to manage effectively. Additionally, the current ACSC trust model, built on in-person interactions, will be difficult to scale with a much larger membership base.

  The membership base of the ACSC has steadily grown from 17 charter members in 2011 to 31 members in 2015. In 2016, there was a decline to 25 members, with some noteworthy departures: a large technology company, a large healthcare provider, a large biotechnology/pharmaceutical company, and the university that originally shaped the emerging ACSC cyber R&D mission in 2009. Within the past 6 months, membership has declined to 21 members.

  As discussed in Section 3.1.3.3, some ACSC members prefer to not have law enforcement or government organizations participate as ACSC members. Consequently, they may be limiting their opportunities to enrich their cyber situational awareness. For example, there is an Air Force cyber-threat intelligence capability at the nearby Hanscom Air Force Base that could add great value to the threat picture. The ACSC is now reconsidering its position on engaged government participation and may pilot an exchange with Hanscom.

- **Products, Services, Events, and Operations:** While the ACSC is best known and valued for cyber information sharing, it is under-delivering on the sharing value proposition because the members themselves are delivering value to each other, while the ACSC is merely providing facilitation services.

  The communications products and services provided by the ACSC are excellent, but they are more useful as promotional materials than as products and services that improve the cyber defenses of member organizations or secure cyber R&D funding.

  The ACSC primarily provides thought leadership, management, guidance, communications, and facilitation services for its members to carry out the three missions of the ACSC. The ACSC does not have the organic resources or subject matter expertise to directly contribute to the execution of its missions.

- **Outreach and Marketing:** As described above, ACSC outreach and marketing are noteworthy and effective.

- **Infrastructure:** The physical and virtual infrastructures that support the ACSC and its members are predominantly provided as in-kind contributions by members. MIGP provides some infrastructure support under contract to the ACSC (e.g., website).

  Electronic sharing of cyber indicators of compromise is accomplished by analysts entering data into a shared threat repository. While there was a proof-of-concept exercise in 2014 between the ACSC and WCX (now the NCX) to electronically share cyber-threat data, the ACSC needs to provide the infrastructure to fully support the automated sharing of cyber-threat information.

- **Key Milestones:**
  - From inception to launch, the ACSC took approximately 5 years. Today, that is a relatively slow pace to form a regional ISAO. One year is now an expected timeframe.
  - From launch to incorporation as a non-profit organization took 2 years. Today, that could be done in 1 year.
  - It has been a little more than 6 years since the first ACSC cyber information-sharing session in 2010. In that amount of time, it is expected that trust would be high enough to support robust sharing of cyber-threat and defensive measure information, and other missions would be well underway. However, trust (further discussed in Sections 3.5.2 and 4.8) is still an issue in the ACSC, the vibrancy and volume of shared cyber information is moderate, and both the cyber R&D and the Legal/Policy missions have struggled to gain traction.

- **Financial Plan:**
  - ACSC finances are fragile:
    - Annual expenses are met by revenue from membership fees only because operational costs have been effectively reduced through in-kind member contributions (e.g., leased space and technical infrastructure). The recently appointed Executive Director is working to reduce operational ACSC cost burdens on the members as well as other ACSC support costs.
  - Annual membership fees are similar to many ISACs but the ACSC provides relatively fewer services:
    - The annual membership fees of a full-service ISAC (e.g., the Financial Services Information Sharing and Analysis Center[55]) are comparable to the ACSC annual fees. However, the ACSC currently provides relatively fewer services to its members.
    - The ACSC is primarily functioning as a facilitator, with most of the value being delivered by members to other members, rather than by ACSC organic staff to members.

3.2 Northeast Ohio CyberConsortium

The NEOCC[56] launched in 2015 as a cross-sector regional partnership among universities, industries, and the government to share cyber information to improve defenses.

The NEOCC is registered with the ISAO SO as a regional ISAO operating in the greater Cleveland, Ohio, region in the U.S.

3.2.1 Missions and Vision

Still in its formative stage, the NEOCC has two missions:

1. **Cyber Information Sharing:** Sharing cyber-threat information and defensive measures to improve the defenses of its member organizations and collective region
2. **Workforce Development:** Addressing the shared workforce development needs of its members

The NEOCC vision is that it will become a center of excellence (CoE) for regional cyber defense and that it will address additional opportunities to strengthen the

[55] https://www.fsisac.com/join
[56] http://www.neocyberconsortium.com/

region's cybersecurity community over time, such as collaborative research, innovation, and industry development.

3.2.2 Trust Model

The NEOCC Executable Charter establishes a trust foundation among founding members through guiding principles, including engaged and meaningful participation and the sharing of actionable cyber information.

A Confidentiality and Privacy Agreement extends the trust foundation to all members as an NDA. The agreement is executed at the corporate level by member organizations, except government and law enforcement participants in the NEOCC. Members have agreed to enter into executive session to excuse government and law enforcement participants when needed.

The trust foundation supports, and is further enhanced by, regular face-to-face and virtual cyber information exchanges (refer to Section 3.2.5).

3.2.3 Organizational Structure and Interactions

The NEOCC is in its formative stage and has not yet incorporated as a legal business entity. Its governance and interactions are those of a well-organized and disciplined affinity group.

3.2.3.1 Governance

The NEOCC Executable Charter establishes guidelines for governance as the consortium forms. The NEOCC leadership team is comprised of four organizing partners: Case Western Reserve University,[57] Cleveland Clinic,[58] Federal Reserve Bank of Cleveland,[59] and the U.S. Attorney's Office for the Northern District of Ohio.[60] This Steering Group is supported by the following committees:

- **Governance:** responsible for establishing governing constructs
- **Technical Operations:** responsible for leading the development of the infrastructure and platforms needed to support NEOCC operations
- **Funding, Development, and Marketing:** responsible for securing funding to support the NEOCC

[57] https://www.case.edu/
[58] http://my.clevelandclinic.org/
[59] https://www.clevelandfed.org/
[60] https://www.justice.gov/usao-ndoh

- **Workforce and Economic Development:** responsible for establishing NEOCC programs to support cyber workforce and economic development

3.2.3.2 Staff and Support

Most of the support for catalyzing the NEOCC is provided by the voluntary labor of members. Recognizing that meaningful progress at a purposeful pace requires more of a dedicated effort than the members could provide, Case Western Reserve University and the Cleveland Clinic co-funded a consultant as a part-time program manager.

3.2.3.3 Interactions

Following the NEOCC launch in November 2015, most member interaction has focused on establishing their cyber information-sharing mission. Members engage through the various organizing committees with the facilitation and support of the NEOCC program manager. The NEOCC instituted regularly occurring cyber information-sharing sessions (refer to Section 3.2.5) in March 2016. Over the next 8 months, the NEOCC added asynchronous platforms (Listserv and SharePoint) to support sharing, as well as forums for deeper technical sharing at a greater frequency.

The NEOCC is modeled on the ACSC (refer to Section 3.1). The greatest difference between the two groups is the level of government participation. Government participation in the ACSC, except from the cyber defenders of the Commonwealth of Massachusetts information technology infrastructure, is light, whereas government participation in the NEOCC is significant and highly engaged. State and U.S. Federal Government agencies are key partners and participants in the NEOCC:

- **U.S. Attorney's Office:** a NEOCC organizing partner, on the Governance Committee, and regularly attends, and occasionally presents at, the monthly sharing sessions
- The **Federal Bureau of Investigation** and the **U.S. Department of Homeland Security**, including the **Secret Service:** regularly attend, and occasionally present at, monthly sharing meetings. For example, the Secret Service gave a cyber situational awareness and readiness briefing to NEOCC members just prior to the 2016 Republican National Convention in Cleveland.

3.2.4 Membership

The Steering Group organized a 1-day conference as a launch event in October 2015. The conference included an additional 12 sponsoring organizations. Membership

has grown organically to 31, based on informal dissemination of information in the region's business community.

3.2.4.1 Composition

Membership includes many of the region's Fortune 1000 and larger mid-market companies, as well as major academic, healthcare, and civic institutions. All of the region's leading industries—including manufacturing, financial services, insurance, real estate, and utilities—are represented.

3.2.4.2 Joining and Vetting

While in its formative stage, the NEOCC currently has no formal membership requirements or member vetting process, other than referrals from the current membership. The NEOCC Leadership Team (Steering Group and Committee Chairs) has instituted a policy to limit the induction of new members pending the development and approval of a business plan and membership model that will provide ongoing sustainability for the activity.

The Steering Group is composed of chief legal officers. These officers typically engage with prospective members through their counterparts.

3.2.5 Products, Services, and Events

- **Monthly Technical Operations Meetings:** First held in March 2016, these face-to-face meetings bring together senior managers and tactical defenders to collectively build advocacy and demonstrate the value of cyber information sharing. The information shared at these meetings is leveled more at strategists than at tactical defenders. The 1.75-hourlong format generally starts with a threat landscape briefing provided by a member organization, followed by presentation(s) by other member(s) of their cybersecurity programs and initiatives. These meetings are hosted in member conference facilities on the third Friday of the month and are facilitated by the hosting organization. Attendance is open only to members.
- **Twice-Monthly Analyst and Defender Sharing Sessions:** First held in November 2016, these twice-monthly sessions bring together tactical defenders and cyber analysts (but do not exclude senior managers) to share actionable cyber-threat information and the details of defensive measures. The 1-hourlong format generally starts with a series of short threat briefings provided by the participating members, which is accompanied by discussions of defensive TTPs. These sessions occur on the first and third Fridays of the month and dovetail with the Monthly Technical Operations (TechOps) Meeting. When held in conjunction with the TechOps Meeting, the tactical

sessions are face-to-face with teleconferencing support; otherwise, they are held as teleconferences. Attendance is open only to members.

- **Cyber Portal:** MITRE hosts a SharePoint site that is externally accessible by NEOCC members. The portal serves as the repository and virtual collaboration platform for the NEOCC.
- **Group Email List:** MITRE uses its Listserv platform to support group email lists for the NEOCC.
- **Website:** The NEOCC uses a third party to host its website. The current content pertains to the NEOCC cyber resiliency conference, at which the NEOCC was launched. The website will be updated to serve as the consortium's public interface.
- **Communications:** Group email lists are used to redistribute threat alerts and reports from government agencies and to disseminate NEOCC status reports and announcements to members. The portal serves as the repository for those reports and announcements as well as for meeting materials.

3.2.6 Operations

Like ACSC sharing operations (refer to Section 3.1.6), NEOCC information sharing has the following characteristics:

- A hybrid model of the hub-and-spoke and peer-to-peer (post-to-all) models
- Two fundamental levels of cyber information sharing: strategic and tactical
- Unclassified information sharing that is not anonymized

3.2.7 Outreach and Marketing

The NEOCC Steering Group, supporting committees, and members provide outreach for advocacy, support, and member recruitment for the NEOCC.

3.2.8 Infrastructure

- **Physical:** Still in its formative stage, the NEOCC has not established a physical footprint. All support for face-to-face meetings is provided by the members.
- **Virtual:** MITRE hosts the NEOCC SharePoint site and the group email lists. Teleconferencing support is currently provided by the member organizations that host face-to-face meetings.

3.2.9 Key Milestones

- Chief legal officers from Case Western Reserve University, Cleveland Clinic, and Federal Reserve Bank of Cleveland, along with the Office of the U.S. Attorney—Northern District of Ohio, begin discussions in 2014 regarding a collaborative approach to cybersecurity.
- In early 2015, planning begins for a cybersecurity conference in Cleveland, Ohio. Cleveland business leaders visit both MITRE and the ACSC in Bedford, Massachusetts, to discuss conference planning and the ACSC cyber information-sharing model.
- On October 14, 2015, the NEOCC launch conference (Cyber Resilience Conference) is held in Cleveland, Ohio.
- On March 4, 2016, the NEOCC holds its first monthly cyber information-sharing session.
- On November 18, 2016, the NEOCC holds its first biweekly cyber information-sharing session for cyber defenders and analysts.

3.2.10 Financial Plan

MITRE drafted an initial straw man business plan that projects financial stability resulting from a combination of start-up grants and membership annual dues. Until securing those grants, the NEOCC operates only with member in-kind labor and other pro bono contributions (e.g., application hosting and facilities use) and the support of a part-time program manager.

Labor, travel, and other costs to participate in NEOCC information-sharing sessions are borne by member organizations. Very roughly, members invest 80 staff hours annually, equivalent to $8K (USD):[61]

- 26 hours for one cyber defender/analyst to attend each biweekly sharing session
- 48 hours to attend monthly sharing sessions
- 6 hours to voluntarily prepare two briefings for presentation at sharing sessions

[61] Assumptions: 2 hours per biweekly sharing session including travel with 26 sessions per year, 4 hours per monthly sharing session including travel with 12 sessions per year, $150K (USD) annual raw salary with an additional 40% fringe benefit rate.

3.2.11 Impressions

- **Overall:** The NEOCC is modeled on, but tempered by, lessons learned from the ACSC. Thus, the NEOCC quickly advanced from inception to its current state of effective sharing. Its current value proposition relies almost entirely on the in-kind labor contributions of members and will need to change as the NEOCC more fully executes its sharing mission and adopts other missions. The NEOCC's effective relationship with government and law enforcement is especially worthy of emulation.
- **Missions and Vision:** The NEOCC has focused its energy and resources on its information-sharing mission and plans to expand its missions only as resources become available. Its strategy around workforce development is to explicitly focus on collaborations with well-positioned partners (e.g., academic institutions for talent acquisition at the entry level, and professional organizations for mid-career talent development) to identify and execute activities that are low-cost and high-value for the members.
- **Trust Model:** The NEOCC has established a strong trust model to support its current cyber information-sharing mission. However, the NEOCC will need to strengthen the trust model when highly sensitive information is shared and as high-trust subgroups inevitably emerge.
- **Organizational Structure and Interactions:** The NEOCC has established an effective interim structure and operation to support the ramp-up of its cyber information-sharing activities. The NEOCC will need to evolve its essentially all-volunteer model to more of a funded hub-and-spoke sharing model to deliver on its value proposition to members.
- **Membership:** The NEOCC has steadily grown and will need to tailor its products and services to accommodate a growing membership that will be increasingly characterized as highly diverse regarding its cyber defense capabilities (refer to Appendix B), especially as more small and mid-sized businesses join the coalition.
- **Products, Services, Events, and Operations:** The NEOCC now operates as an affinity group that facilitates cyber information sharing at no cost to its members. That is not a sustainable model for a group that wishes to provide highly valued and differentiated products and services to its members.
- **Outreach and Marketing:** The highly collaborative nature of the greater Cleveland area aided the rapid formation and growth of the NEOCC. To improve the regional coverage of the NEOCC, especially with the increased participation of small to mid-sized businesses, the NEOCC will need more concerted outreach and marketing activities.

- **Infrastructure:** All infrastructure to support the NEOCC is provided pro bono by members. That is not a viable approach as the NEOCC grows and increasingly provides additional and more valuable products and services to its members.
- **Key Milestones:** The NEOCC has progressed at a rapid pace, but it risks leveling off, unless it can fund additional valued operations.
- **Financial Plan:** Ideally, the NEOCC would secure a seed grant or matching grant to sustain its current operations and to fuel an operational ramp-up. The NEOCC should plan for self-sustained long-term operations.

3.3 National Cyber Exchange

The NCX, formerly the WCX, is a consortium in Colorado Springs, Colorado, whose objective is to bring together university, industry, and government organizations to address cyber challenges. The NCX "is a non-profit, member organization dedicated to improving cybersecurity and protecting critical infrastructure by sharing cyber-threat information, providing education and workforce development, technology development, and supporting member cybersecurity needs."[62]

The WCX was established in 2010 as a regional consortium to address the cybersecurity needs of Colorado, Wyoming, and New Mexico. In 2016, the WCX rebranded and expanded its scope as the NCX to align with a state initiative for the University of Colorado at Colorado Springs to house and support a National Cybersecurity Center(NCC).[63] The current relationship between the NCX and NCC is best characterized as an aspirational functional merger.

3.3.1 Missions

The NCX has three primary missions:

1. **Cyber Threat Sharing and Analysis:** operating as an Information Sharing and Analysis Organization (ISAO)[64] to share and analyze unclassified cyber-threat information derived from members, open sources, and the DHS cyber information-sharing programs

[62] http://nationalcyber.org/wcx-rmta
[63] https://www.nationalcybersecuritycenter.org/
[64] https://www.dhs.gov/isao

2. **Workforce Development:** partnering with academies and universities to provide students with hands-on experience and opportunities to participate in exercises and training events, and providing cyber awareness and certification training
3. **Technology Development and Research:** serving as a capacity center and technical resource to its members

3.3.2 Trust Model

The NCX NDA[65] establishes a foundation of trust among members of the NCX. The agreement is executed at the corporate level of participating organizations. The trust foundation is reinforced by the NCX Membership Agreement,[66] which is executed by all individuals who access NCX services.

3.3.3 Organizational Structure and Interactions

3.3.3.1 Governance

The NCX is governed by an NCX Executive Committee established by the Rocky Mountain Technology Alliance (RMTA),[67] which is a non-profit organization incorporated in 2006 in the state of Colorado under the tax-exempt 501(c)(6) section of the U.S. Internal Revenue Code. The NCX and RMTA operate at Imprimis Incorporated,[68] a small for-profit technology consulting firm in Colorado Springs, Colorado. The NCX functionally operates as a committee of RMTA. Several subcommittees operate under the NCX Executive Committee: Operations, Fund Raising, Membership, and Economic Development.

The NCX evolved from an RMTA initiative in 2010—the Center for Information Age Transformation (CIAT)—which became the WCX in 2011. The WCX then rebranded as the NCX in 2016.

3.3.3.2 Staff and Support

The NCX is mostly a virtual organization staffed and supported by Imprimis through in-kind labor contributions.

---

65 https://static1.squarespace.com/static/569945cda2bab8378c7d4056/t/580509b559cc684e436364ef/1476725174890/NCX+NDA+Template.pdf

66 https://static1.squarespace.com/static/569945cda2bab8378c7d4056/t/580509ce59cc684e43636653/1476725202254/NCX+Membership+Agreement+Template.pdf

67 http://www.rmtech.org/

68 http://imprimis-inc.com/

3.3.3.3 Interactions

The current NCX interactions are focused on reestablishing the WCX as an ISAO that provides valued products and services to its member organizations.

Members primarily share cyber-threat and defensive-response information through automated, rather than face-to-face, means.

- **Members and Local Government:** The peak of WCX cyber information sharing occurred during an 18-month period in 2011 and 2012, when there were approximately 30 organizations participating in periodic, face-to-face technical exchanges known as Information Technology (IT) Users Forums. The participating organizations were primarily small and mid-sized technology companies in Colorado Springs and representatives from local government departments of utilities. An initial trust model was developed, but was not universally adopted by all participants because of concerns that there could be disclosures of shared information compelled under Colorado Sunshine Laws that govern public meetings. A tension between the needs of the government participants to conduct meetings and exchanges in accordance with bureaucratic requirements and the wishes of the small technology companies to informally conduct information-sharing meetings contributed to the demise of regular, face-to-face WCX information sharing. A series of devastating wildfires, the Waldo Canyon Fire in 2012 and the Black Forest Fire in 2013, diverted the focus of many members and ultimately led to the collapse of regular sharing. In 2013 and 2014, the WCX hosted numerous meetings and seminars, but the meetings and seminars were not well attended by the waning membership. In 2014, the WCX reassessed its value proposition and began to strengthen its original vision as a capacity center focused on technology as a core platform for improving the individual and collective defenses of its members. As discussed below, the WCX supplemented its vision through participation in Federal Government sharing programs to provide timely delivery of actionable cyber-threat indicators to its members through its technology platforms.
- **Federal Government:** The role and participation of the government in the WCX/NCX greatly changed in 2015, when the WCX executed a special agreement—a Collaborative Research and Development Agreement (CRADA)[69]—with DHS to participate in some of its public-private cyber information-sharing programs (refer to Section 3.3.5).

[69] https://www.dhs.gov/science-and-technology/technology-transfer-mechanisms

3.3.4 Membership

The NCX has a multi-tiered membership structure that includes followers, students, individuals, cyber professionals, non-profits, small companies, and larger companies. The levels are differentiated by service and product packages (refer to Section 3.3.5) and annual membership fees (refer to Section 3.3.10).

3.3.4.1 Composition

The NCX is targeting a membership base that consists of entities operating the following sectors and domains: public utilities, energy, technology, IT, cybersecurity, academia, and digital health. These sectors are similar to the ones that WCX previously targeted.

3.3.4.2 Joining and Vetting

Prospective members apply for membership online by completing the NCX NDA and NCX Membership Agreement (refer to Section 3.3.2) and submitting credit-card payment. Followers, students, and individuals do not execute the Membership Agreement. Followers do not execute the NDA.

The corporate status, where applicable, is verified.

3.3.5 Products, Services, and Events

Products, services, and events support the NCX's missions.

3.3.5.1 Cyber Threat Sharing and Analysis

- **Cyber Threat Center:** a member-facing portal for access to NCX information-sharing and analysis platforms and threat feeds
    - DHS Cyber Information Sharing and Collaboration Program (CISCP):[70] In CISCP, DHS and participating companies share information about cyber threats, incidents, and vulnerabilities, and have access to the NCCIC[71]—the DHS hub and cybersecurity operations center to increase awareness of vulnerabilities, incidents, and mitigations.
    - DHS Automated Indicator Sharing (AIS):[72] a program for secure, standards-based, automated sharing of threat indicators
    - Soltra Edge:[73] an open-source cyber-threat information repository and platform for secure, standards-based, cyber information sharing

[70] https://www.dhs.gov/ciscp
[71] https://www.dhs.gov/national-cybersecurity-and-communications-integration-center
[72] https://www.dhs.gov/ais
[73] https://github.com/Soltra

  - CRITs:[74] CRITs is an open-source repository and analysis platform for cyber-threat information, originally prototyped by MITRE for its own use. Imprimis hosts an NCX instance of CRITs that is externally accessible by NCX cyber defenders and analysts.
  - Analysis Tools: Suricata,[75] an open-source tool for analyzing packet-capture information, and Cuckoo,[76] an open-source malware analysis tool

- **Secure Email:** NCX email accounts are encrypted using Absio Dispatch.[77]
- **NCX Website:** The NCX uses a third party to host its website. Most content is developed by Imprimis.
- **Member Forum:** The NCX website has a members-only forum to deploy content to members.
- **Mobile Application:** WCyberX Forum[78] provides a mobile-device interface to the Member Forum.
- **Communications:** This is a core service that the NCX and Imprimis provide to its members. Communications are distributed via email and posted to the Member Forum. Examples include Newsletters, Alerts, and Event Notices.

3.3.5.2 Workforce Development

- **Workshops, Meetings, and Events Planning and Facilitation:** This is a core service that the NCX and Imprimis provide to it members. Examples include the NCX Annual Meeting and the Health IT Cybersecurity Summit.
- **Training Exercises:** Examples include an annual tabletop exercise with utilities operating in the Colorado Springs area.
- **Cyber Citizen Training:** This is a 2-hour training in the basics of cybersecurity.
- **Certification Training:** This is provided as needed.

[74] https://crits.github.io/
[75] https://suricata-ids.org/
[76] https://cuckoosandbox.org/
[77] https://www.absio.com/dispatch/
[78] iPhone: http://www.appszoom.com/iphone-app/wcyberx-forum-mrpxs.html; Android: http://www.appszoom.com/android-app/wcyberx-portal-lyrly.html

3.3.5.3 Technology Development and Research

- **Technical Resource Register:** a registry of member vendors and cybersecurity product and service catalogues
- **Voluntary Collaborative Incident Response:** a volunteer Cyber Brigade of members and partners

3.3.6 Operations

The NCX information-sharing operations can be characterized as a hybrid model of the hub-and-spoke and peer-to-peer (post-to-all) models (refer to Section 2.1):

- **Hub-and-spoke:** The NCX serves as a central hub of information and services that are distributed and provided to members (spokes).
- **Peer-to-peer (post-to-all):** The NCX provides face-to-face and email communications.

The information shared falls into two general categories:

- **Strategic (for executives, senior managers, and technical architects):** defense strategies, risks, policies, investment strategies, workforce development, awareness, metrics, and approaches for communicating risk and effectively advocating for cyber defense and resiliency
- **Tactical (for computer network defenders):** cyber observables; indicators; incidents; targets; adversary and defensive TTPs (best practices); campaigns; courses of action; cyber actors; analyses; and actionable unclassified intelligence

All information shared is unclassified and typically anonymized when provided by members to the NCX through the Cyber Threat Center Portal.

3.3.7 Outreach and Marketing

The NCX Executive Committee and Membership subcommittee provide outreach and marketing in conjunction with NCX website content. With the functional merger of the NCX with the NCC, increased outreach and marketing services can be inherited from the NCC.

3.3.8 Infrastructure

- **Physical:** The current NCX physical footprint is provided by Imprimis. Support for face-to-face meetings is currently provided by Imprimis and members. The new NCC/NCX facility is being constructed and will be occupied in the second half of 2017. With the planned functional merger of the NCX with the NCC, the combined facility will include a Security Operations Center, data center, showcase, cyber exercise facilities, training facilities, and the ability to provide incident response support.
- **Virtual:** Imprimis hosts, either directly or through commercial hosting services, the entire NCX technical infrastructure.

3.3.9 Key Milestones

- In 2010, RMTA formed CIAT.
- In 2011, CIAT transformed into the WCX, and information sharing began as an IT Users Forum.
- In 2012, the WCX established CRITs as an information repository and analysis platform.
- In 2014, the WCX exchanged a threat formatted as a Structured Threat Information eXpression with the Advanced Cyber Security Center via the Trusted Automated eXchange of Indicator Information protocol, and added the Member Forum and mobile application to communicate with member organizations.
- In 2015, the WCX self-identified as an ISAO; signed a CRADA with DHS, participated in DHS CISCP, added Soltra Edge, and hosted a utility-sector tabletop exercise.
- In 2016, the WCX was approved to consume DHS AIS feeds, hosted a digital health summit, and rebranded as the NCX. The NCX obtained approval to merge with the NCC to provide nationwide functional support.

3.3.10 Financial Plan

3.3.10.1 Revenue

Annual membership fees are the primary source of funding for the NCX. The fees were initially structured as follows:

- Follower: no fee
- Student: $25

- Member: $50
- Cyber Professional: $250
- Non-profit: $250
- Small Business (1–49 employees): $500
- Larger Business (50+ employees): $1,000

However, the rate structure for when the NCX functionally merges with the NCC has not been finalized. The new rate structure is expected to follow the NCX membership levels in form, but with somewhat higher fees that are tempered for smaller businesses.

Membership levels, services, and fees are related as illustrated in Figure 2.[79]

Benefit & Annual Dues (Green = member receive benefits, # = no. of staff receiving benefit, % = discount)	Corp. L2	Corp. L1 (< 50 Employees)	Non-Profit	Cyber Professional	Member	Student Member*	NCX Follower
Annual Dues	$1,000	$500	$250	$250	$50	$25	$0
▪ Newsletter							
▪ Notice of all NCX events							
▪ Cyber Threat Center (CTC) information sharing / Alerts							
▪ Member Forum for information exchange					Public Threat Alerts		
▪ NCX TRR (Technical Resource Register) at reduced member rates							
▪ Training – Cyber Citizen- (2 hr. Class)	10	5	1	1	1	1	
▪ Discount on NCX Training & Certification	10%	10%	10%	10%	10%	Scholarships	
▪ Annual Events – Admission for …	5	2	1	1			
▪ NCX E-Mail Account with Absio Dispatch License	5	3	1	1			

* Students may volunteer in lieu of Dues & Event Fees, will be eligible for Scholarships

Figure 2. Membership Levels, Services, and Fees

When the NCX and NCC functionally merge, additional benefits of membership will be inherited and will include access to the NCC Cyber Institute and Cyber Education, Training, and Research Center.

3.3.10.2 Expenses

The expenses are not known, but are probably low due to offsets provided through in-kind support from Imprimis, sponsors, and members.

[79] http://nationalcyber.org/membership

3.3.10.3 Member In-kind/Pro Bono Contributions

Imprimis hosts the entire technical infrastructure to support cyber information sharing and analysis, as well as office space and basic support services, at no cost to the NCX.

Sponsors and many members support NCX operations through contributions of labor, products, and services. The combined NCX/NCC business model is intended to substantially increase available funding sources.

3.3.11 Impressions

- **Overall:** A weak trust platform, the lack of shared purpose and operating principles, and the failure to effectively manage a diverse member base ultimately led to the restructuring of the WCX. In the early years of WCX operation, a tension developed between public and private participants over the formality of sharing processes and operations. That tension stemmed from two fundamentally opposing beliefs regarding how to best conduct sharing operations: (1) as an altruistic social exercise that can be achieved informally versus (2) as business transactions that are governed by bureaucracy and conducted using formal processes. Regarding the first belief, some participants felt that the WCX governing body was using the WCX as a marketing platform. The ill will from this perception dampened enthusiasm and trust, which ultimately had a chilling effect on effective sharing. While the focus on greater private-sector participation and the aspirational merger with the NCC may help address the original shortcomings and tensions, the NCX faces another challenge. As the NCX reinvents itself as a delivery platform for automated information exchange of cyber indicators, it may risk the embracement of one of its key value propositions: in an environment dominated by small and mid-sized businesses that face basic cyber threats, how actionable and useful will cyber-threat indicators of sophisticated attacks be to those businesses?
- **Missions and Vision:** To differentiate themselves from regional ISAOs that serve large, mid-sized, and small business, the NCX missions and vision should be more sharply focused on small and mid-sized businesses that would benefit more from sharing best practices and basic defenses against conventional cyber threats than from consuming automated feeds of sophisticated threat information that they will struggle to process and use. The NCX workforce development mission aligns very well with that of most of its potential members.

- **Trust Model:** The NCX sharing model has moved away from face-to-face cyber information sharing during the WCX era to more of an automated model. This shift will likely slow the building of trust that is needed for vibrant, high-value sharing.
- **Organizational Structure and Interactions:** Ideally, an ISAO with missions like the NCX's missions would be operated by a public-interest organization that is trusted, independent, non-profit, and free of any perceived conflicts of interest.
- **Membership:** The NCX levels of membership are nicely stratified and well-suited for an economic ecosystem that is dominated by small and mid-sized businesses. The national reach of the NCX seems premature; the NCX might consider waiting to first be a smashing success in its own backyard before expanding to a national stage.
- **Products, Services, Events, and Operations:** The NCX service offerings appear to be helpful and useful.
- **Outreach and Marketing:** Testimonials and case studies may be effective tools for marketing and outreach to disseminate via the NCX website.
- **Infrastructure:** All infrastructure to support the NCX is provided pro bono by Imprimis, partners, and members. That is not a viable approach as the NCX grows and fully executes its value proposition.
- **Key Milestones:** The NCX has been a work in progress for 6 years and has reimagined itself several times. Until 2015 its progress was slow and labored because it appeared to be taking on too many missions, with too few resources and too little buy-in by members. However, its progress in 2015 and 2016 is impressive. Nevertheless, with too few resources, the aspiration for national outreach seems to be too much, too soon.
- **Financial Plan:** The current membership dues are so low that sufficient revenue to fund NCX services would seemingly have to be fueled by a very large membership base. Growing very large, very quickly is very difficult. However, if the NCX functionally merges with that of the NCC, then additional funding to sustain operations may be available through state and federal funding and grants.

3.4 Case Studies: Key Challenges and Perspectives

The key challenges in building and operating an ISAO like those described in the cases studies are expressed here in the form of questions (refer to the Gnarly 9 in Section 2.2). The authors provide their perspectives on how the questions could be addressed. The recommendations in Section 4 either answer or provide the context to address the questions posed here.

1. **What is the essence of the consortium?**
   Identify the consortium's short-term, mid-term, and long-term missions. For example, the short-term mission may be sharing cyber-threat indicators and defensive measures. The mid-term mission may be conducting R&D collaboratively, and the long-term mission may be engaging in regional economic development.
2. **What are the implementation milestones?**
   Develop a high-level plan—Strategy and Roadmap (refer to Section 2.2)—that matches up with the missions and that includes specific milestones at each phase.
3. **What information will be shared by members, and how will it be shared?**
   Determine what information will be shared by whom, for whom, and for what purposes. Other considerations include defining the appropriate level of sensitivity, whether the information will be attributed or anonymous, and whether it will be used for tactical defense or strategic decision making.
4. **What is the consortium's value proposition?**
   Establish a value proposition that sets the consortium apart to encourage potential members to commit resources, time, and effort. Determine what services the consortium will provide for its members.
5. **What are the membership criteria and composition?**
   Decide if membership will be based on location, sector, event, or type of threat. For example, will it be capped or unlimited? Is there a vetting process for membership? What are the roles of law enforcement and the government?
6. **How can members trust the consortium to safeguard their sensitive information?**
   Look for a trusted, independent third party to manage operations. Determine the appropriate controls. Create platforms and mechanisms for building trust among members, such as institutional and individual NDAs.

7. **How does the consortium fit into the local, regional, and global cyber ecosystems? What are the roles of the government and law enforcement?**
   Determine who has access and under what circumstances information can be shared or used outside the consortium, and define the consequential obligations.
8. **What is the consortium's leadership and governance?**
   Identify key stakeholders and their roles. Consider the benefits of organizing as a non-profit, trusted, independent third party. Develop a plan for selecting a board of directors, for creating steering and subcommittees, and for staffing.
9. **What is the consortium's financial plan?**
   How you address the other 8 questions will drive your financial plan, and your financial plan will affect how you address those questions. Explore seed funding and grants to get started; without them, you must start small, lean heavily on member in-kind contributions, or boost membership fees. Determine the fee structure for founding members and other membership categories, including sponsors.

3.5 Critical Success Factors

Three critical success factors emerge from the case studies and the key challenges:

1. **Funding:** An ISAO needs adequate financial support to be successful.
2. **Trust:** Trust is a prerequisite for effective sharing.
3. **Shared vision and managed growth:** The vision needs to be collaboratively formed with stakeholders and guided by a comprehensive plan.

These success factors, as well as the challenges outlined in Section 3.4, drive the recommendations in Section 4.

3.5.1 Funding

In each of the case studies, funding was a critical success factor. The lack of sufficient revenue affected the ACSC's ability to staff operations capable of delivering substantial value to members. Consequently, that responsibility fell to the members. With annual fees as high as those of the FS-ISAC, the value proposition was increasingly regarded as unattractive, resulting in a shrinking membership base. The lack of sufficient revenue also shifted the responsibility for infrastructure support to the membership, which is not sustainable in the long term.

Since its launch in 2015, the NEOCC has relied mostly on in-kind labor contributions from members to sustain operations and deliver value to members. There are currently no membership fees. The value proposition is attractively simple: what members get from the NEOCC is driven by what members provide to the NEOCC. Currently, some members provide more support than others, which is not sustainable in the long term. The NEOCC will eventually need to evolve its essentially all-volunteer model to a fee-for-service model that relieves members from responsibilities that they may regard as too burdensome.

The NCX low-fee membership and low-growth prospects do not appear to be adequate to sustain effective long-term valued operations. Consequently, the NCX may need to shift responsibilities for value delivery onto its members and risk what may be regarded as too great a burden for members to bear in the long term.

Section 4.11 provides recommendations to address the funding-related critical success factor.

3.5.2 Trust

Trust is the enabler of valued cyber information sharing. Without it, sharing is often anemic and low value. The regional ISAOs in the case studies established adequate trust baselines in several ways. The first way was through NDAs. While necessary, these agreements are not sufficient to establish a deep-enough trust relationship among cyber defenders that enables the sharing of valuable, highly useful cyber information. The second way that a baseline level of trust was established was through the referent trust provided by the non-profit, trusted, independent third parties who were responsible for catalyzing and operating the ISAOs.

Both the ACSC and the NCX are non-profit formal corporations, while the NEOCC currently operates less formally as a consortium under a charter. MITRE—in its capacity as a non-profit, trusted, independent third party—hosts sharing infrastructure components for the ACSC and the NEOCC.

At its inception, the NEOCC had more of a jump-start on trust than the ACSC and the WCX did. Prior to launching the NEOCC, founding members and early adopters were already connected through long-standing business trust circles in the Cleveland, Ohio, vicinity. Clevelanders were already predisposed to collaborate and share. Following the NEOCC launch, initial sharing interactions were, consequently, more robust than the early interactions in the ACSC, which did not have a pre-existing trust network.

The three ISAOs were effective in building additional trust through regular face-to-face interactions afforded by regional proximity. However, each ISAO faces the same fundamental challenge to further building trust. Because their membership bases encounter a wide range of cyber threats, from conventional to advanced (refer to Appendix B), cyber-defense expertise varies greatly within the membership base of each ISAO. Consequently, distrust can arise if the cyber-threat information shared by experts is improperly treated by less-expert defenders/ analysts whose operational security practices (e.g., open-source queries on malware samples and other indicators of compromise) can potentially jeopardize the intelligence value of the shared information (e.g., a command-and-control infrastructure that was established to target a specific victim organization). While there are no known instances of this happening in any of the three ISAOs in the case studies, some cyber defenders have had their cyber intelligence "burned" by unsophisticated sharing partners. That indelible experience has resulted in more cautious sharing in groups that are not bound by very strong trust.

Unequal sharing is another common phenomenon that affects diverse sharing groups and can ultimately diminish robust sharing. In diverse groups, experts often dominate sharing with less-expert defenders who consume information but are able to offer little in return. Over time, this imbalance can lead to resentment and can reduce the volume and value of what advanced practitioners are willing to share.

Mainly because it has operated longer than the other regional ISAOs, the ACSC has most strongly felt the ill effects of untreated cyber diversity. Robust sharing has waned over the past several years, and the membership has contracted approximately 30%.

Section 4.8 addresses the aspects of trust and provides a model of inter-personal trust that rationalizes the observations and assertions made in this section. Section 4.10 provides cyber diversity management recommendations.

3.5.3 Shared Vision and Managed Growth

An ISAO's vision, mission, value proposition, and growth plan—codified as a comprehensive Strategy and Roadmap, like the one described in Section 2.2—need to be collaboratively formed and adopted by engaged stakeholders and potential members and participants, rather than being exclusively formed by the entity that is catalyzing the ISAO. Without this, an ISAO risks committing to goals and plans that may not be readily achievable or fully supported.

Only the NEOCC has effectively engaged with key stakeholders in this process. The ACSC and WCX visions and initial plans were more exclusively formed and were

driven by the business interests of their single-founder entities. However, the NCX (the next generation of the WCX) and ACSC 2.0 (next generation of the ACSC) are now more broadly engaging with their stakeholders as they re-invent themselves.

Sections 4.1 provides recommendations for collaboratively developing strategies and roadmaps.

3.6 For Potential Further Examination

Several other U.S. ISACs and ISAOs are generally recognized as exemplars that would provide additional insights to the recommendations provided in this paper, including the FS-ISAC (refer to Section 2.3), the National Cyber Forensics & Training Alliance,[80] and the Arizona Cyber Threat Response Alliance.[81]

[80] https://www.ncfta.net/
[81] http://azinfragard.org/?page_id=8

4 Recommendations and Implementation Guidelines

The authors provide 11 recommendations, further detailed as implementation guidelines, that address the top challenges in building an effective unclassified national cyber information-sharing ecosystem around a core of cross-sector regional partnerships to (1) improve the individual and collective cyber defenses of university, industry, and government entities, as well as citizens, through greater situational awareness and more-informed risk-management decisions; and (2) stimulate regional economies through a collaborative focus on education, workforce development, innovation, and R&D that is informed by the challenges facing cyber defenders and is fueled by research data sets.

The recommendations, which are listed below, and the implementation guidelines that follow are informed by lessons learned in establishing regional sharing centers and other public-private partnerships in the U.S., and by the authors' strategic insights on enabling an information-sharing ecosystem.

1. Convene workshops to collaboratively develop a Strategy and Roadmap for an unclassified cyber information-sharing ecosystem.
2. Enact legislation to catalyze the formation of a diversity of sharing centers.
3. Incrementally build the cyber information-sharing ecosystem from a strategic roadmap.
4. Catalyze ecosystem growth with cross-sector regional sharing groups.
5. Articulate the role of the government.
6. Articulate the missions and establish a differentiating value proposition.
7. Develop membership criteria and a governance model.
8. Establish foundations of trust.
9. Share the right data in the right way.
10. Actively manage cyber diversity.
11. Stimulate private-sector participation.

4.1 Convene Workshops to Develop a Strategy and Roadmap for an Unclassified Cyber Information-sharing Ecosystem

Rather than evolving the information-sharing ecosystem from emerging government needs over decades, as in the U.S. (refer to Section 2.4), a national strategy that is collaboratively developed through a public-private partnership among university, industry, and government stakeholders would guide the development of the ecosystem. An ISAO would be established to convene and manage the workshops and to lead the development of the strategy. The ISAO would be operated by a trusted not-for-profit, independent third party.

Two key products would emerge from the national workshops:

- A Strategy and Roadmap for the whole ecosystem
- A Strategy and Roadmap for ISAOs

Those products, initially shaped by the Gnarly 9 and the 10 Strategy and Roadmap elements described in Section 2.2, would initially guide the evolution of the ecosystem (described in Section 4.3) and the development of a cross-sector regional ISAO (described in Section 4.4). The Strategy and Roadmap documents would be periodically updated by lessons learned as the ecosystem evolved and as the ISAO was piloted.

The Strategy and Roadmap for ISAOs would provide a general blueprint that cross-sector regional ISAOs would tailor to their needs, environment, and local culture.

Recommendation drivers appear in the following sections: Section 2.4 (#1), Section 3.4 (#1), and Section 3.5.3.

4.2 Enact Legislation to Catalyze the Formation of a Diversity of Sharing Centers

A myriad of U.S. Government policies and federal laws and regulations govern cyber information sharing.[82] The overwhelming majority of them pertain to critical infrastructure protection. As discussed in Section 2.4, two Federal Government actions stand out as enablers of the vigorous growth in private-sector and public-private partnerships for cross-sector regional sharing and other domain-based sharing: CISA and the ISAO executive order.

[82] https://www.dhs.gov/publication/ci-threat-info-sharing-framework and https://www.isao.org/products/isao-600-2-us-government-relations-programs-and-services/

Together, these U.S. Federal Government actions have enabled the formation of many ISAOs, including state-level ISAOs in Alabama, California, Indiana, Maryland, Texas, and Virginia. Because of their success as catalysts of cyber information sharing, especially at the regional level, the authors of this paper recommend that similar government policies and federal laws and regulations be established or tailored.

Recommendation drivers appear in the following section: Section 2.4 (#6).

4.3 Incrementally Build the Cyber Information-sharing Ecosystem from a Strategic Roadmap

The Strategy and Roadmap developed through the national collaboration described in Section 4.1 would provide the blueprint to build the ecosystem. Rather than taking more than 15 years, as in the U.S., a national cyber information-sharing ecosystem could be established within several years, if there was an effective baseline (described in Section 4.3.1) already in place to build upon. Sections 4.3.2 through 4.3.6 illustrate and describe a recommended series of incremental builds to establish a national unclassified cyber information-sharing ecosystem.

4.3.1 Build 0 (Baseline): Sharing in the Context of Emergency Response and Critical Infrastructure Protection

Figure 3 illustrates the key entities and the primary cyber-information flows in an unclassified national cyber information-sharing ecosystem that supports emergency response (CERTs); critical infrastructure protection (ISACs); and secure, standards-based, automated sharing.

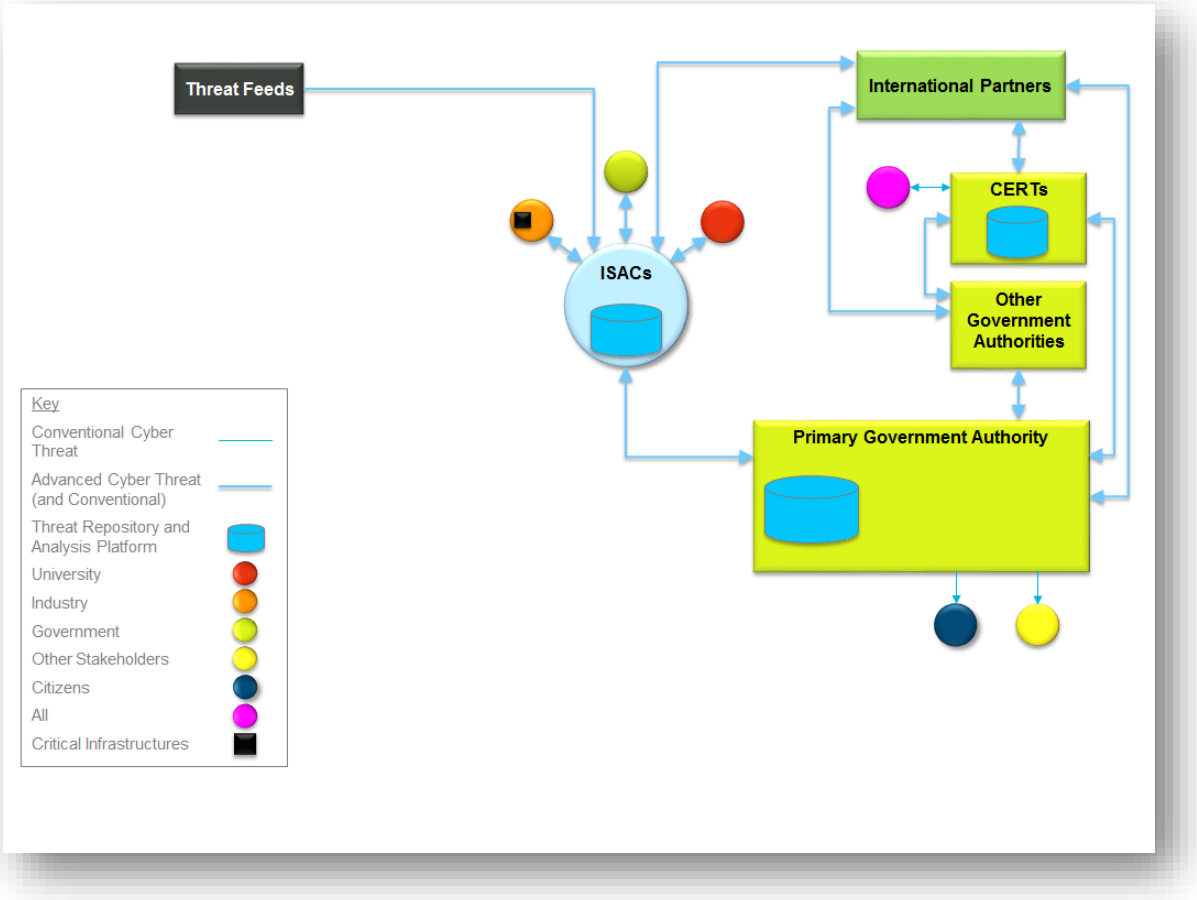


Figure 3. Sharing in the Context of Emergency Response and Critical Infrastructure Protection

The entities shown in Figure 3 are summarized below.

- **Primary Government Authority:** In this baseline, a primary government authority—like DHS in the U.S. (refer to Section 2.3)—is the epicenter of the ecosystem. This government authority functions as an unclassified clearinghouse, integrator, analysis engine, and national source of cyber information pertaining to both conventional and advanced cyber threats and defensive measures. This authority is shown as the intermediary for the CERTs, but the sharing with ISACs could be direct.
- **Threat Repository and Analysis Platform:** A database of unclassified cyber-threat and defensive-response information, and a platform for threat analysis

- **Conventional Cyber Threat:** Threats with the motivational intent of vandalism or incursion (refer to Appendix B)
- **Advanced Cyber Threat:** Threats with the motivational intent of breach, disruption, or warfare (refer to Appendix B)
- **CERT:** The national CERT is responsible for responding to major incidents, analyzing threats, and exchanging critical cybersecurity information with the owners and operators of critical infrastructures and with trusted partners around the world. The national CERT is often operated by the Primary Government Authority.
- **Other Government Authorities:** Organizations external to the Primary Government Authority that play roles in a nation's cyber-defense mission. Examples include law enforcement and intelligence entities to prevent, detect, and respond to cybercrime and other malicious cyber activity.
- **ISACs:** Sector-based, public-private partnerships among owners and operators of critical infrastructures for sharing cyber-threat information and defensive measures. ISAC sharing operations are characterized as a hybrid of hub-and-spoke, peer-to-peer (post-to-all), and source-subscriber sharing models (refer to Section 2.1).
- **Critical Infrastructures:** Assets, such as banking, power generation, and water, that are vital for a functioning society and national economy
- **University, Industry, and Government:** The unclassified cyber information collected or developed by government entities is generally shared broadly with ISACs and their stakeholders.
- **Threat Feeds:** Open-source and commercial feeds of cyber-threat and situational-awareness information. Threat feeds introduce a source-subscriber model into the sharing ecosystem (refer to Section 2.1).
- **International:** The national cyber information-sharing ecosystem has international reach and a global impact. Most nations share cyber information with international law enforcement and intelligence entities to collaboratively prevent, detect, and respond to cybercrime and malicious cyber activity. Additionally, most nations share cyber information with international partners and stakeholders, typically CERTs, in the context of incident response.
- **Citizens:** Citizens who are given access to unclassified cyber information that is provided by government entities
- **Other Stakeholders:** Small and mid-size businesses and other entities that do not directly participate in ISACs or in other structured sharing groups

- **All:** Universities, industry, government, citizens, and other stakeholders interacting with the CERT in the context of emergency response
- **Secure, Automated, Standards-based Sharing:** While not specifically shown in this or any other figures, the ecosystem must support secure, standards-based automated sharing (e.g., STIX and TAXII) (refer to Section 2.3).

Recommendation drivers appear in the following sections: Section 2.4 (#2, #3, #4) and Section 3.4 (#3, #8).

4.3.2 Build 1: Establish Cross-sector Regional Sharing and Other ISAOs

4.3.2.1 Growth Catalyst of the Ecosystem

Figure 4 introduces cross-sector regional ISAOs, as well as other ISAOs, into a national unclassified cyber information-sharing ecosystem. This figure also introduces unclassified, government-provided cyber-threat information feeds. For Figure 4 through Figure 9, each figure successively builds on the previous figure (e.g., Figure 4 builds on Figure 3, Figure 5 build on Figure 4). In each figure, the newly introduced entities and flows are accentuated with color, while those inherited from the previous "build" (i.e., previous figure) are lowlighted (grey).

Because of its importance as an ecosystem growth catalyst, Section 4.4 provides a development approach for piloting a regional ISAO.

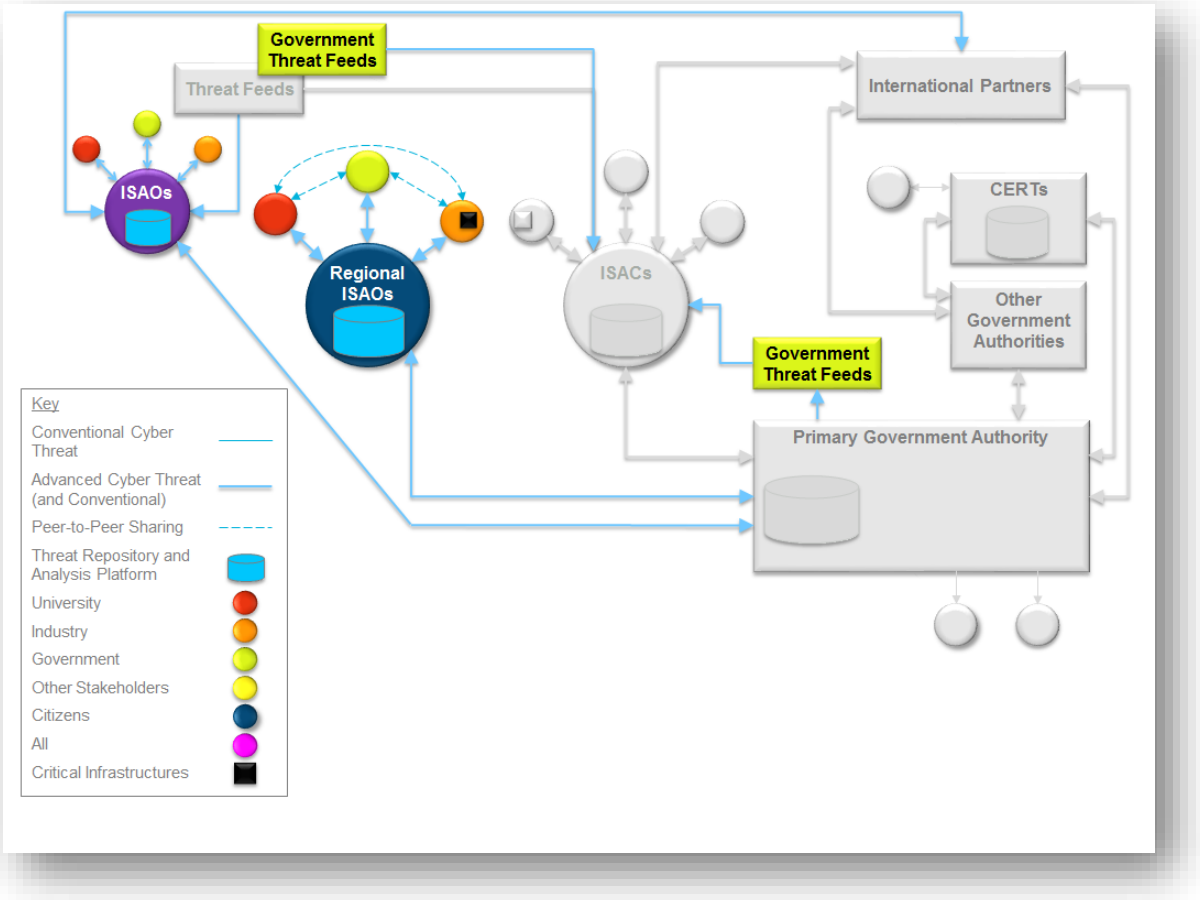


Figure 4. Introduce ISAOs and Cross-sector Regional ISAOs

Figure 4 introduces the following additional entities:

- **Regional ISAOs:** As described in the case studies in Section 3, these are regional partnerships among university, industry, and government entities that are focused on cross-sector cyber information sharing to improve stakeholders' and regional defenses. Cross-sector regional ISAOs are an essential complement to the sector-based critical infrastructure protection provided to ISACs. Regional ISAOs and other ISAOs generally operate as a hybrid of hub-and-spoke, peer-to-peer (post-to-all), and source-subscriber sharing models (refer to Section 2.1).
- **Peer-to-Peer Sharing:** Regular face-to-face sharing afforded by regional ISAOs is a key element in building trust among stakeholders, which is essential for effective cyber information sharing.

- **ISAOs:** These are the most recent type of cyber information-sharing partnerships to appear in the U.S. cyber information-sharing landscape (refer to Section 2.3). ISAOs will catalyze the growth of a highly distributed, highly diverse, and highly connected sharing ecosystem that is driven by the private sector.
- **Government Threat Feeds:** Feeds of cyber situational awareness from the Primary Government Authority, like DHS' AIS program in the U.S. (refer to Section 2.3)

Recommendation drivers appear in the following sections: Section 2.4 (#2), Section 2.5 (#5), Section 3.4 (#6), and Section 3.5.2.

4.3.3 Build 2: Establish Unclassified Clearinghouse and Federated Sharing

Figure 5 shifts the epicenter of the ecosystem from a government entity to a trusted, independent third party that functions as the steward of an unclassified clearinghouse of cyber information. The clearinghouse is fed by, and feeds to, ISAOs, ISACs, and a Primary Government Authority. That Authority would be responsible for breaking the gridlock that often occurs in releasing unclassified versions of cyber threat information. Figure 5 also introduces federated sharing among ISACs and ISAOs.

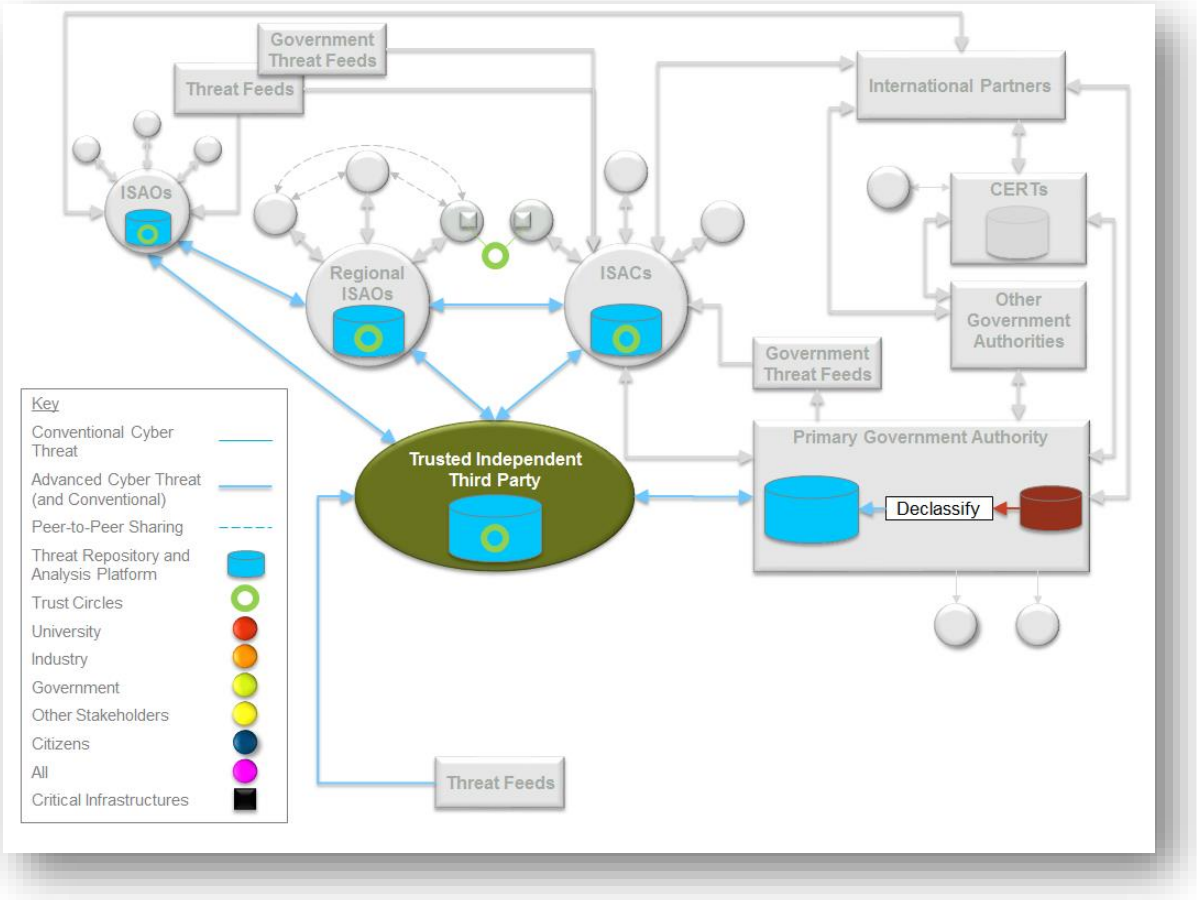


Figure 5. Introduce Trusted, Independent Third Party and Federated Sharing

Figure 5 introduces the following additional entities:

- **Trusted, Independent Third Party:** The epicenter of the ecosystem shifts from a Primary Government Authority to a trusted, not-for-profit third party that functions as a clearinghouse, integrator, analysis engine, and steward of a virtual national repository of unclassified cyber-threat and defensive-response information. This shift is crucial to establishing the trust needed for robust, effective sharing in the ecosystem. Rather than being literally centralized, the repository of cyber information would be distributed through conventional replication, clustering, and mirroring technologies, but eventually may reside and be shared in a highly decentralized blockchain infrastructure.

- **Primary Government Authority:** This government authority is additionally responsible for providing, to the trusted, independent third party, unclassified cyber-threat and defensive measures that are derived and downgraded from classified sources.
- **Trust Circles:** These are trusted enclaves that participants in cyber information-sharing groups may form with other cyber information-sharing groups (i.e., a group-of-groups referred to as a sharing federation). Trust circles enable secure, standards-based, automated, federated sharing among clusters of ISAOs and ISACs. Future trust circles may be established through trust contracts that execute on a blockchain infrastructure.

Recommendation drivers appear in the following sections: Section 3.4 (#6) and Section 3.5.2.

4.3.4 Build 3: Introduce a National Portal and Regional Citizen Centers

Figure 6 introduces a national portal and regional citizen centers to engage with citizens and small businesses that are not otherwise served by ISACs or ISAOs.

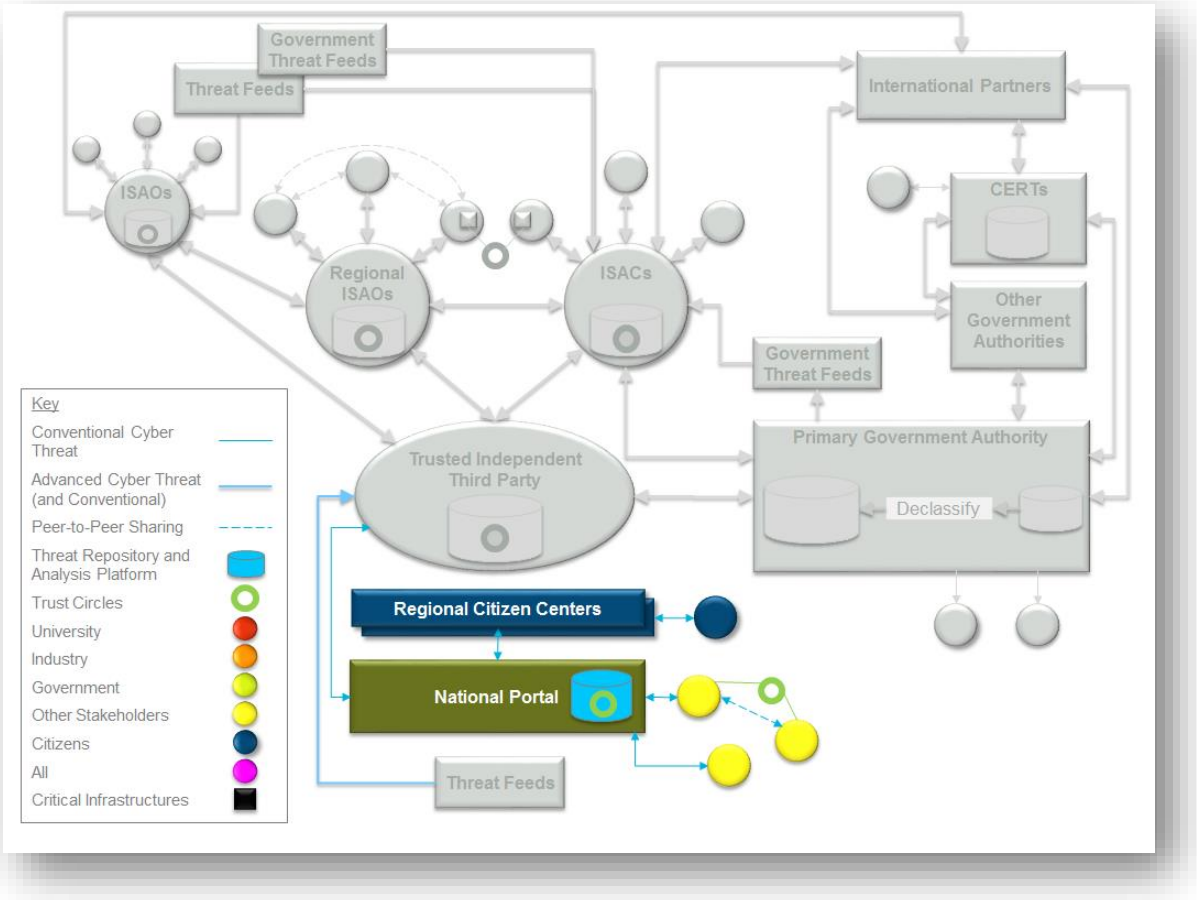


Figure 6. Introduce Cyber Innovation Centers and Academic Centers of Excellence

Figure 6 introduces the following additional entities:

- **National Portal:** A shared repository of cyber-threat information regarding conventional cyber threats fed by the trusted, independent third party and regional ISAOs (not shown in Figure 6). The portal is a national resource for reporting cyber incidents as well as sharing cyber threats and best practice defenses for citizens and other stakeholders.
- **Regional Citizen Centers:** The public would engage with the national ecosystem through a regional view provided by a National Portal. Citizens, and other entities not formally engaged with ISAOs, would use the portal for incident reporting as well as cyber situational awareness and defensive measures tailored to be helpful and useful for them. The Centers would be physically co-located with the regional ISAOs and would provide cyber-awareness and best-practice seminars.

Build 3 represents an ecosystem that enables widespread sharing of cyber-threat information and defensive measures to improve cyber defense, resilience, and risk management through improved situational awareness and collaboration. Cyber information sharing that helps catalyze regional cyber economies is addressed in Build 4.

Recommendation drivers appear in the following section: Section 2.4 (#2, #5).

4.3.5 Build 4: Support Regional Economic Development

Figure 7 introduces innovation centers and academic cyber CoEs to support regional economic development.

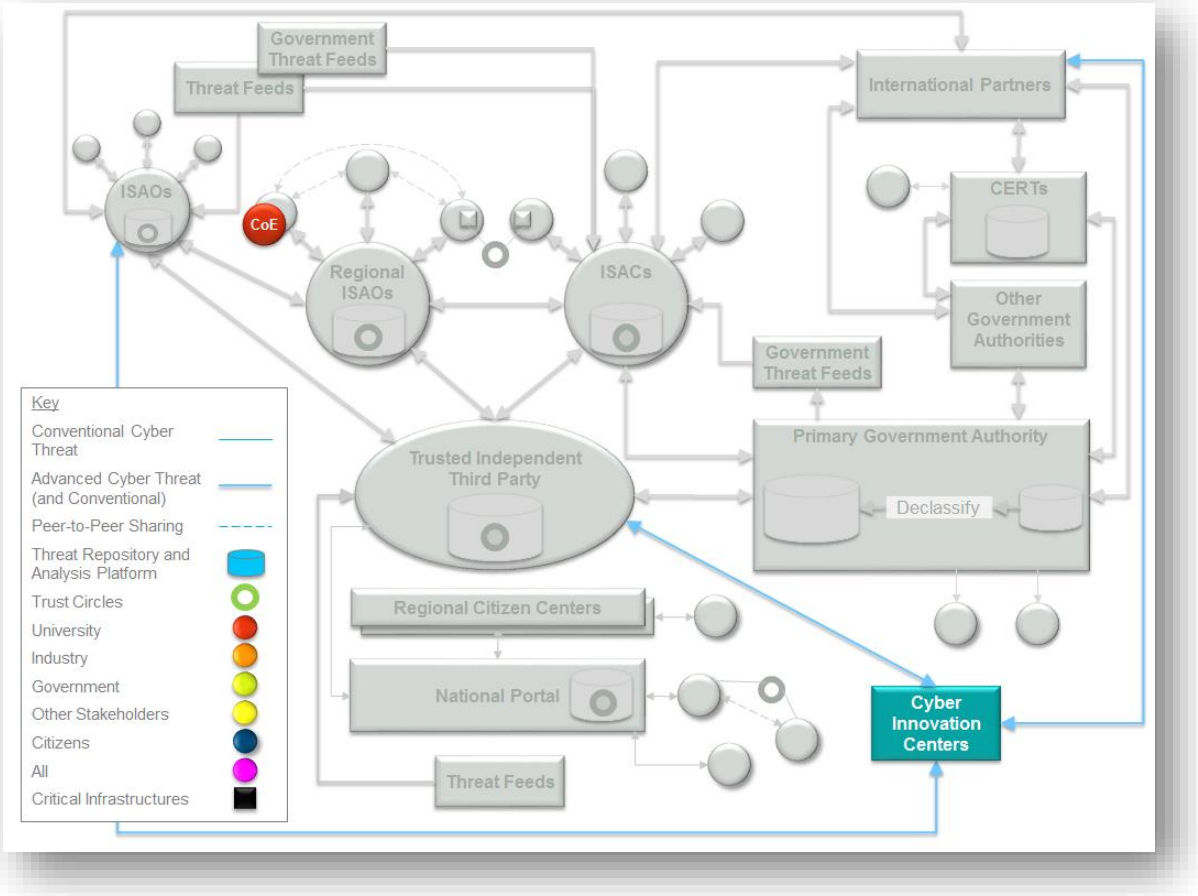


Figure 7. Introduce Cyber Innovation Centers and Academic Centers of Excellence

Figure 7 introduces the following additional entities:

- **Cyber Innovation Centers:** These are regional platforms for catalyzing and facilitating the growth of regional cyber economies through a focus on education, workforce development, innovation, and R&D. The Centers would connect with the ecosystem through ISAOs, regional ISAOs (not shown in Figure 7), and the trusted, independent third party, which would provide research data sets and identify cyber defense challenges faced by their members/stakeholders to help fuel R&D and innovation. The Centers would also collaborate with International Partners.
- **Cyber CoEs:** Academic cyber CoEs at universities that connect with the ecosystem through the ISAOs and regional ISAOs (not shown in Figure 7), which would provide research data sets and identify cyber defense challenges faced by their stakeholders to help fuel cyber R&D, innovation, and workforce development

Recommendation drivers appear in the following section: Section 2.4 (#5).

4.3.6 End-State: National Unclassified Cyber Information-sharing Ecosystem

Figure 8 represents the end-state of a national unclassified cyber information-sharing ecosystem that is developed in four successive builds atop a baseline sharing capability enabled by CERTs and ISACs. The ecosystem is a federation of meshed entities that employ the three fundamental modalities of cyber information sharing—the hub-and-spoke, peer-to-peer (post-to-all), and source-subscriber models (refer to Section 2.1).

The ecosystem enables the secure, standards-based, automated sharing of cyber-threat information and defense measures for the purposes of improving national, regional, local, and citizen cyber defense as well as catalyzing a cyber economy through innovation, R&D, and workforce development.

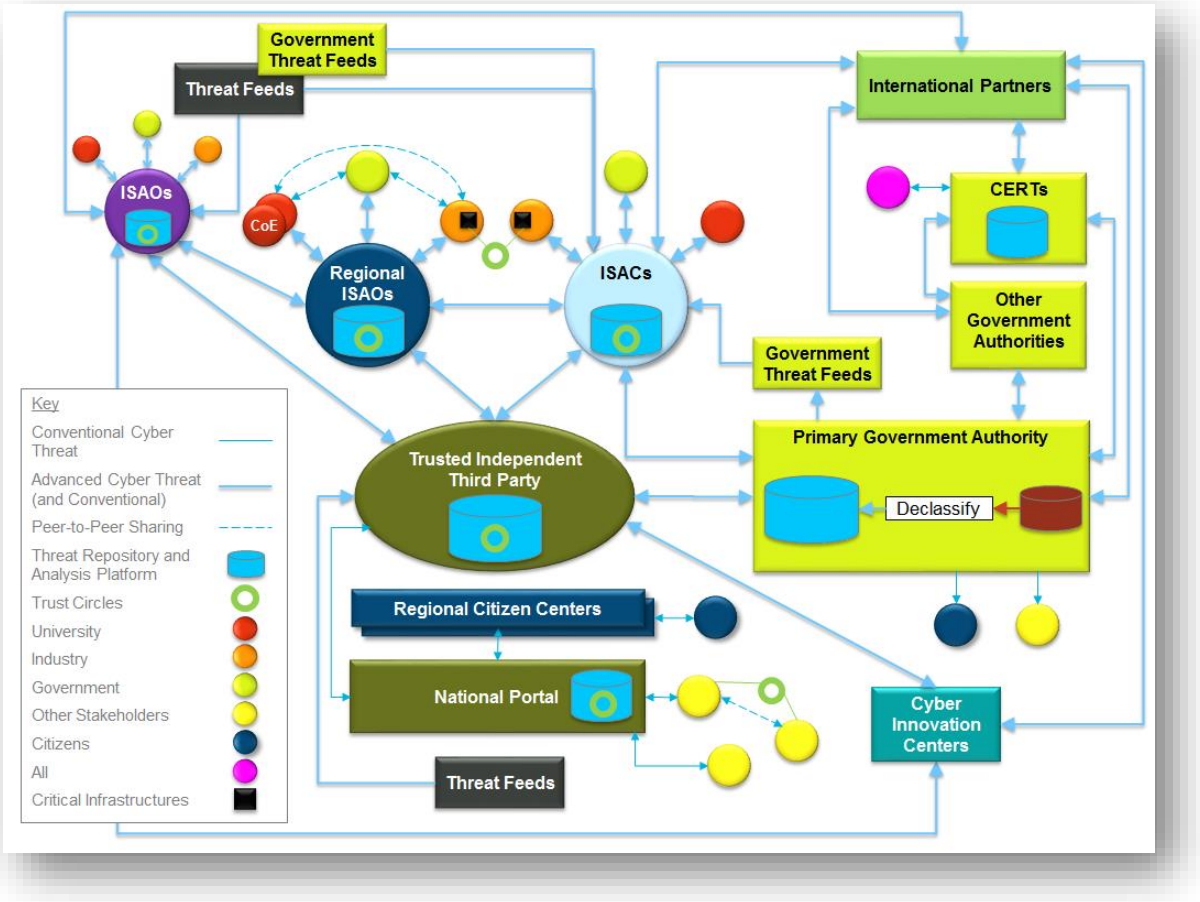


Figure 8. End-state: National Unclassified Cyber Information-sharing Ecosystem

4.3.7 Timeline for Establishing an Ecosystem

4.3.7.1 U.S.

The baseline ecosystem described in Build 0 took more than 15 years to establish in the U.S. Build 0 continues to evolve as ISACs more fully adopt the secure, standards-based, automated sharing that is enabled by STIX and TAXII.

As described in Build 1, the introduction of ISAOs, including cross-sector regional ISAOs like the ones described in the case studies in Section 3, into the U.S. cyber information-sharing ecosystem started more than 5 years ago. ISAOs will increasingly emerge over the next several years. They are the catalyst for ecosystem growth.

Although STIX and TAXII are the enablers of federated sharing among ISACs and ISAOs, there is no known, well-established instance in the U.S. of federated sharing like that described in Build 2; it is likely to take several years before that is a noteworthy occurrence.

There have been discussions in the last several years about the potential need for, and value of, a government-sponsored, unclassified clearinghouse in the U.S. like the one described in Build 2. At least another 6 to 8 months of continued discussion is likely to occur before that kind of clearinghouse concept becomes more than a potentially good idea. There is, however, a private-sector clearinghouse-type concept emerging in the U.S.: CyberUSA.[83]

Currently, a national portal and regional citizen centers, like the ones described in Build 3, are mostly the objects of entrepreneurial aspiration in the U.S.

Cyber innovation centers and academic cyber CoEs abound in the U.S., but they are not currently connected or integrated as envisioned in Build 4.

4.3.7.2 Accelerating Ecosystem Development

Three accelerants would reduce the time to build a national, unclassified, cyber information-sharing ecosystem:

1. Drive the development through a public-private national Strategy and Roadmap, as described in Section 4.1.
2. Stimulate private-sector participation, as described in Section 4.10.
3. Skip and/or combine some of the 4 builds (1–4). For example, skip the trusted, independent third party in Build 2, but maintain the Build-1 connection between ISACs, ISAOs, and regional ISAOs and the Primary Government Authority; then, combine Builds 3 and 4 and rewire the ecosystem to connect the Primary Government Authority (and/or CERTs) to the National Portal and cyber innovation centers.

This ecosystem acceleration results in 2 builds, rather than 4 builds. Figure 9 illustrates what the new Build 2 would look like.

[83] http://www.cyberusa.us/

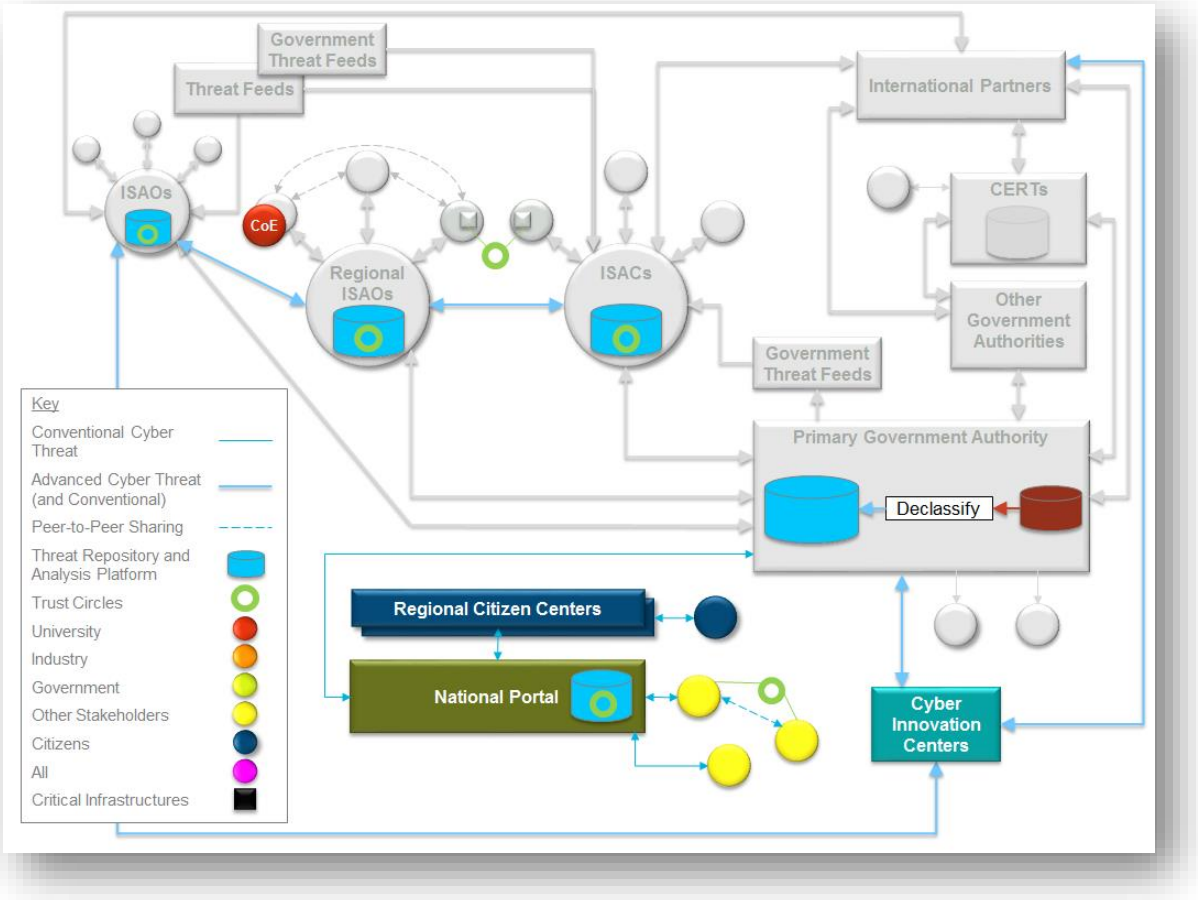


Figure 9. Eliminating and Merging Builds

4.4 Catalyze Ecosystem Growth with Cross-sector Regional Sharing Groups

4.4.1 Value to the Ecosystem

Cross-sector information-sharing partnerships, including regional exchanges, are regarded by the authors as a necessary complement to a national ecosystem that initially focuses on sector-specific, critical-infrastructure-based cyber information sharing.

Cross-sector cyber information-sharing partnerships can provide more early warning opportunities (like a canary in a coal mine) than sector-based sharing partnerships. As offered in the *Verizon 2015 Data Breach Investigations Report*, "We need more cross-sector sharing." Additionally, "It follows that our standard practice

of organizing information-sharing groups and activities according to broad industries is less than optimal. It might even be counterproductive."[84]

4.4.2 Incrementally Pilot a Cross-sector Regional ISAO

The authors of this paper recommend that the ecosystem be initiated around a 24-month pilot of a regional ISAO in the context of the accelerated ecosystem development discussed in Section 4.3.7.2 and illustrated in Figure 9. While the Strategy and Roadmap drafted through the national workshops described in Section 4.1 would guide the pilot, the authors provide the implementation guidelines that follow.

The regional ISAO would be established by a trusted, independent third party as a non-profit consortium located in a major city that brings together a variety of institutions, such as university, industry, and government organizations, to share unclassified cyber-threat information and defensive measures. The regional ISAO would be initially connected with the Primary Government Authority (refer to Figure 9) to provide shared, national cyber situational awareness with regional and critical infrastructure views of the threat landscape.

The regional ISAO would be piloted as a series of incremental builds of increasing capabilities. The first 12 months of pilot operations would include the following major functional capabilities:

- Face-to-face sharing
- Teleconferencing and web conferencing
- An online capability that serves both as a repository of cyber-threat information that supports the secure, standards-based, automated exchange of cyber information and as a collaborative cyber-threat analysis platform. This platform provides the enabling technical infrastructure to support widespread sharing of cyber information within the national ecosystem (federation) and with international entities (global federation).
- Synchronizing and de-duplicating elements in the cyber-threat repositories maintained by the regional ISAO and other entities in the sharing ecosystem
- Anonymous or attributed information submission
- Tagging information with sensitivity

[84] http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report_2015_en_xg.pdf

- Tagging information to allow and control fine-grained access and sharing within trust circles
- A common taxonomy of terms, but also a Rosetta Stone translation key to identify equivalent cyber-threat campaigns
- Real-time direct messaging among participants

The lessons learned during the pilot would be used to inform the initial regional ISAO Strategy and Roadmap (i.e., the "blueprint") developed under the national initiative described in Section 4.1.

The 24-month pilot would be conducted as follows:

- **The Focus:** The first 18 months would focus on effective cyber information sharing to better manage cyber risks and to improve cyber defenses. After 18 months, the sharing focus would open to support regional economic development through innovation, R&D, and workforce development.
- **Near-term (first few months):** Leverage existing social networking, collaboration, and sharing platforms to jump-start sharing and collaboration.
- **Mid-term (4–6 months):** Select and transition to sharing and collaboration platforms that will sustain pilot activities for the remainder of the first year of the pilot.
- **Long-term (6–12 months):** Integrate into the pilot a collaborative threat analysis platform that enables the secure, standards-based automated sharing of threat intelligence. Expand the pilot to include a National Portal and Regional Citizen Centers (refer to Section 4.3.7.2 and Figure 9). The Portal and Center would be piloted as a series of incremental builds with the following functional capabilities:
    - Public-facing
    - Business-facing
    - Feeds of cyber situational awareness from the government as well as commercial and open sources
    - Feeds of cyber situational awareness between the National Portal, the regional ISAO(s), and other government platforms
- **Transition (12–18 months):** Begin to transition the initial operational capability developed during the first year of the pilot to full-scale operations.
- **Longer Term (18–24 months):** Conduct a 6-month readiness trial of full operations, during which lessons learned will be used to inform future ongoing full-scale operations. Begin to engage with academic cyber CoE and cyber innovation centers by sharing research data sets derived from the

regional ISAO and/or provided by its members/stakeholders. Begin to shift the epicenter of the cyber information-sharing ecosystem from the government to a trusted, independent, not-for-profit third party.

Recommendation drivers appear in the following section: Section 2.4 (#5), Section 3.4.2, and Section 3.5.3.

4.5 Articulate the Role of the Government

For an effective exchange of information between the government and an ISAO, members need to believe that the benefits gained by sharing information with the government outweigh the risks (e.g., unauthorized disclosure of personal information). Because the value proposition is often not compelling enough from the perspective of the private sector, the private sector rarely initiates two-way sharing with the government. One way to improve the value proposition, from the perspective of the private sector, is through one-sided sharing, where the only information shared comes from the government. One practical way to achieve this is through an electronic feed of cyber-threat information from the government to the ISAO.

If there is reciprocal sharing of cyber information between the ISAO and the government, then the ISAO would need to provide an anonymous sharing capability. However, anonymous sharing can diminish the potential value of information (refer to Section 4.9).

Recommendation drivers appear in the following section: Section 3.4 (#7).

4.6 Articulate the Missions and Establish a Differentiating Value Proposition

Focus and articulate the ISAO's short-term, mid-term, and long-term missions. For example, a short-term mission would be sharing actionable cyber-threat information and defensive measures to improve collective regional defenses through greater situational awareness and more-informed risk -management decisions. A mid-term mission would be conducting R&D collaboratively, and a long-term mission would be engaging in regional economic development.

Establish a value proposition that sets the ISAO apart from other cyber information-sharing groups to encourage potential members/stakeholders to commit resources, time, and effort.

Determine the service offerings provided by the ISAO, which, beyond sharing, may include analyses of cross-sector threat migration; a collaborative analysis of threats;

a collaborative or managed incident response; and shared resources, such as product evaluation testbeds, a cybersecurity operations training facility, and a synthetic environment for engaging cyber adversaries. The selected service offerings should be directly aligned with both the value proposition and the stated missions.

Recommendation drivers appear in the following section: Section 3.4 (#1, #4).

4.7 Develop Membership Criteria and a Governance Model

Initially address the following three elements of membership and governance:

1. Develop criteria for membership/participation in the ISAO, including eligibility, qualifications, vetting, and whether it will be capped or unlimited.
2. Develop levels of membership/participation.
3. Develop a governance model for the ISAO and the cyber information-sharing ecosystem.

The strength of the trust framework that is used to admit and cohere members should dictate the maximum size of an ISAO. A high-trust framework (described in Section 4.8) can sustain a large membership. However, because trust relationships do not scale well, there is a practical upper limit to the number of high-trust members that a regional ISAO can effectively manage (30 to 50 member organizations). A regional ISAO can scale beyond that upper limit by surrounding its high-trust core membership with an outer ring of additional member organizations (as many as 50 to 100) that primarily participate through virtual interactions in venues where high trust is not required.

The governance model for an ISAO that is a public-private partnership among university, industry, and government entities needs to be especially well-crafted to balance the inherent tension between the needs of government participants to conduct meetings and exchanges in accordance with bureaucratic requirements and the wishes of the small companies to conduct more-informal information-sharing exchanges. The governance model also needs to be dynamic to accommodate the maturing of sharing operations over time. In its formative stages, the ISAO governance model can be lightweight and informal. As the ISAO moves through its pilot stage of operations and gathers lessons learned, additional layers and components of governance can be added; but only as needed, keeping the burden of bureaucracy to a minimum. Having an agreed-upon governance structure will facilitate the collaboration and trust-building among ISAO members. The impact of this is that the cohesiveness of the membership and the overall direction of the organization are appropriately managed and maintained in the face of change.

Recommendation drivers appear in the following section: Section 2.4 (#8), and Section 3.3.3.

4.8 Establish Foundations of Trust

Blomqvist and Ståhle "…propose that there is both inter-personal and inter-organizational trust, but it is always people in the organization that trust."[85] Because trust is a key enabler of effective cyber information sharing, both types of trust must be established among the entities in an ISAO.

To establish an inter-organizational foundation of trust, an ISAO should be operated by a not-for-profit, trusted, independent third party that operates in the public interest, is free of commercial conflicts of interest, and can effectively steward and safeguard sensitive information. To further build inter-organizational trust, member organizations should be required to execute corporate-level non-disclosure agreements (NDAs). Trust would be further built through strong vetting of candidate member organizations.

The U.S. ISAO construct, as discussed in Section 2.3, has provisions for certification that are intended to establish ISAO trustworthiness that would be needed to enable widespread ISAO-to-ISAO sharing in a national ecosystem. Trust certification of regional (and other) ISAOs should be similarly considered.

Charles Green's Trust Equation[86] identifies four components that affect interpersonal trust: credibility, reliability, intimacy, and self-orientation, where the first three components increase trust, while the last (self-orientation) diminishes trust. While some individual credibility and reliability are inherited from a parent organization, they can be strengthened through individually executed NDAs to increase trust. Interpersonal trust is strengthened by the intimacy built through face-to-face interactions, especially afforded by the close proximity of members in a regional ISAO. Interpersonal trust is further built through rigorous member vetting that increases an individual's credibility and reliability. Additionally, adherence to rules of behavior that address engaged participation and information safeguarding requirements for different levels of information sensitivity (e.g., the Traffic Light Protocol[87]) can increase interpersonal trust by further increasing credibility and reliability and reducing self-orientation.

---

[85] Kirsimarja Blomqvist and Pirjo Ståhle, *Building Organizational Trust*, 2000, page 4 (http://www.impgroup.org/paper_view.php?viewPaper=37)

[86] http://trustedadvisor.com/why-trust-matters/understanding-trust/understanding-the-trust-equation

[87] https://www.first.org/newsroom/releases/20160831

Recommendation drivers appear in the following sections: Section 2.5.1, Section 3.4 (#6), and Section 3.5.2.

4.9 Share the Right Data in the Right Way

Sharing the right data in the right way is important for two main reasons: to help develop trust within the sharing organization and to ensure that value can be derived from sharing. The level of trust among the participants in an ISAO and the risk tolerance of individual participants and their parent organizations generally dictate the sensitivity of the information that is shared. As trust is initially being developed, the ISAO should focus on sharing information that is not sensitive, which generally means shying away from information about incidents and vulnerabilities. Besides being sensitive, this information is often not actionable by other participants. The ISAO should initially focus on sharing intrusion-attempt information (i.e., information about incidents, regardless of actual intrusions). As trust develops, more-sensitive and contextual information, or cyber threat intelligence, can be shared, including indicators of compromise, threat campaign characteristics, detection tools and techniques, and behavioral analytics (refer to Appendix C).

As discussed in Section 2.4, what is typically shared has changed over time, from cyber threat data often with little context to fully contextualized data, or information, referred to as cyber threat intelligence. The volume, diversity, and delivery speed of cyber threat data, information, and intelligence has grown tremendously over the past decade, to the point of taxing the ability of cyber defenders and analysts to process it into actionable information in a timely manner. To best deal with this challenge, an understanding and alignment is needed of what kind of information is suitable and actionable for ISAO members based on their operational needs and the threats they face (refer to Section 4.10).

A nation should balance reactive, incident-based cyber information sharing with the more-proactive sharing of information derived from the earlier stages of the Cyber-attack Life Cycle (refer to Appendix D) of advanced cyber adversaries. This balance of reactive and proactive sharing has greater potential to reduce the overall cost of cyber defenses by better avoiding the relatively high costs of breach containment and recovery.

An ISAO should encourage data attribution and fidelity, whereby organizations would not anonymize or sanitize data to hide the identities of those providing data and would not desensitize the data before sharing it with members/stakeholders or with the government. Anonymizing and desensitizing data prevents others from

following up with the source organization for amplification or context. Data has a far greater potential value when it has attribution and fidelity.

Cyber threat information is exchanged in several different ways, including face-to-face, virtual conferencing, electronic feeds, and email. When shared through electronic means, cyber information should be encapsulated and transmitted securely using standards-based formats and protocols. There are several proprietary and open standards for encapsulating and securely transmitting cyber information, such as STIX and TAXII (refer to Section 2.4 and Section A.10 in Appendix A), Incident Object Description and Exchange Format (IODEF), IODEF for Structured Cyber Security Information (IODEFSCI), Real-time Inter-network Defense (RID), Vocabulary for Event Recording and Incident Sharing (VERIS), and Open Indicators or Compromise (OpenIOC).[88]

Recommendation drivers appear in the following sections: Section 2.4 (#3 and #4) and Section 3.4 (#3).

4.10 Actively Manage Cyber Diversity[89]

The advantage of sector-based threat-sharing groups, such as the U.S. FS-ISAC, is that members are all in the same business sector, and thus face similar threats. Regional threat-sharing groups, on the other hand, are cross-sector and collectively face a broad range of threats, from conventional cyber threats to advanced cyber threats (refer to Appendix B). The advantages of regional sharing are not necessarily in shared threats, but are in the opportunity to meet face-to-face, build trust, collaborate on shared concerns, and offer fresh ideas and approaches that are not necessarily conceived by a sector-based approach.

Because the motivations and goals of attackers are different for conventional and advanced cyber threats, the cyber information-sharing requirements to manage risks, defenses, and responses are also different. To achieve effective, risk-based threat sharing among regional partners, the regional partners must fundamentally change the way they organize. Instead of a single structure in which all members share cyber information based on their own view of the threat, which may overwhelm some members with irrelevant information or use mechanisms that are not shared by all, organizing around operational preparedness to address different cyber threats (refer to Appendix B) would potentially achieve a better outcome.

---

[88] G. Farnham (SANS Institute InfoSec Reading Room), *Tools and Standards for Cyber Threat Intelligence Projects*, October 2013.

[89] S. Sundar, D. Mann, *Effective Regional Cyber Information Sharing*, Public Release 16-4620, to be released in 2017.

Recommendation drivers appear in the following section: Section 2.4, Section 3.1.11, and Section 3.5.2.

4.11 Stimulate Private-sector Participation

The government—especially at the federal level but also at the state and city levels—should stimulate private-sector operation and participation in ISAOs, as well as engagement in the design and development of the sharing ecosystem, in several ways:

- Providing ownership through engaged collaboration in developing a Strategy and Roadmap (refer to Section 4.1)
- Offering safe harbor protection from inadvertent disclosures of protected privacy information (refer to Section 4.2)
- Providing relief from regulatory burdens
- Fully or partially funding ISAO operations

Regarding relief from regulatory burdens, the U.S. Food and Drug Administration issued guidance in 2016, stating that it did not intend to enforce certain reporting requirements related to the disclosure and remediation of certain medical-device vulnerabilities if the manufacturer was actively involved in an ISAO and adhered to another recommended guidance.[90]

Regarding the government funding of ISAO operations, the recommended approach for establishing and sustaining ISAO operations, especially for the piloting a cross-sector regional ISAO (refer to Section 4.3), is for the government to initially fund operations, with ISAOs eventually transitioning to self-sustaining operations that are funded by their members/stakeholders. This is consistent with the approach for catalyzing the first ISACs in the U.S. (e.g., the FS-ISAC discussed in Section 2.3).

This funding approach would allow resources to be dedicated to piloting the first regional ISAO and would thereafter reduce barriers to adding regional nodes to the sharing ecosystem. Without start-up funding, regional sharing groups tend to make very slow progress in executing their missions and delivering on their value propositions.

Recommendation drivers appear in the following section: Section 2.4 (#6).

---

[90] *Postmarket Management of Cybersecurity in Medical Devices, Guidance for Industry and Food and Drug Administration Staff,* Food and Drug Administration, January 22, 2016, https://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm482022.pdf

5 Conclusions

Supported by case studies, tempered by lessons learned and top challenges, and informed by their strategic insights, the authors provide a highly summarized, broad set of conclusions on how to effectively build a national unclassified cyber information-sharing ecosystem and its core of cross-sector regional information-sharing groups.

- **A national unclassified cyber information-sharing ecosystem and its key elements—such as cross-sector regional ISAOs—need to evolve from a strategic plan—Strategy and Roadmap—that is collaboratively developed by university, industry, and government stakeholders.**
- The "ownership" of the ecosystem should not be dominated by the government; rather, it should be co-owned by the stakeholders.
- The epicenter of a national cyber information-sharing ecosystem should be led by a non-profit, trusted, independent third party, rather than by the government, as the government can be perceived as less trustworthy.
- A vital ecosystem is heavily driven by ISAOs that are catalyzed and operated by the private sector. Cross-sector regional ISAOs are a vital growth engine of an ecosystem.
- Every ISAO is different and needs to be catalyzed and operated under a Strategy and Roadmap that is tailored to its mission, environment, and local culture.
- The government needs to stimulate participation in the ecosystem through stakeholder buy-in, legal encouragement and protection, and relief from regulatory burdens.
- The government needs to create tear lines on classified information and get high-value, actionable cyber information into the unclassified domain of trusted recipients.
- The ecosystem needs to simultaneously support and adapt to information sharing that addresses old, new, and anticipated threats.
- The ecosystem needs to support secure, standards-based, automated sharing.
- The ecosystem needs to supply cyber information that is helpful and useful to anyone, especially small and medium-size businesses, as well as citizens.
- Whatever the purposes for information sharing are, adhere closely to each purpose by appropriately investing and assigning resources.

- Unless there a good reason not to, make information sharing for cyber defense effective before making it a catalyst for economic development.
- **Low trust crushes effective sharing.**
- **Unless carefully managed, highly diverse sharing groups, in the context of wide-ranging cyber defense expertise, can erode trust and consequently dampen sharing.**
- There are typically many more takers than givers in a sharing group. Givers needs to guard against resentment, and takers need to find a good way to return something of value.
- Vital sharing in a new group will take much longer than expected.
- Rainmakers catalyze ISAOs, but expertise, commitment, and value delivery make them successful.
- A regional ISAO is a special kind of business that needs to be effectively run like a special kind of business, so seek the guidance of subject matter experts.
- **The start-up costs that are needed to deliver valued services to ISAO members are often so high that funding early operations solely through membership fees becomes very challenging. Government funding can overcome this challenge. A realistic financial plan is critical.**
- Low-value delivery from an ISAO will eventually be recognized and will result in rapidly shrinking participation.
- Ecosystems and ISAOs are complex; build them in steps.
- If you are not sure if an element of an ecosystem or an ISAO will work well, then pilot it and learn from it.

Appendix A. The MITRE Corporation

The MITRE Corporation[91] is a private, not-for-profit organization that manages and operates seven federally funded research and development centers (FFRDCs) that support United States (U.S.) government sponsors. FFRDCs serve as long-term strategic partners to the government, providing objective guidance in an environment free of conflicts of interest. MITRE operates the nation's first FFRDC that is solely dedicated to cybersecurity; it supports the National Cybersecurity Center of Excellence's goal of accelerating the adoption of secure technologies to address today's most pressing cybersecurity challenges.

Founded in 1958, MITRE initially focused on supporting the U.S. Air Force's air-defense mission. Since then, MITRE has distinguished itself as a national asset by applying science, technology, systems engineering, and strategy to complex problems of global significance in the areas of aviation, critical infrastructure, cybersecurity, and defense.

MITRE's goal is to build a safer, more secure nation and world. MITRE currently provides expertise to the international community in the areas of aviation, defense, cybersecurity, judicial reform, fiscal transparency, financial and healthcare fraud detection, and technical and data standards.

MITRE has substantial experience as a trusted, independent third party providing secure stewardship, sharing, and transformational analyses of sensitive information. For example, MITRE operates the Aviation Safety Information Analysis and Sharing (ASIAS) platform for the Federal Aviation Administration (FAA). ASIAS is an information exchange that focuses on the sharing of data from airlines to improve air safety. In that model, MITRE acts as a hub that receives information from multiple airlines and the FAA. MITRE collects, anonymizes, and analyzes this information and provides reports to all participants on the key issues that affect airline safety (refer to Section A.1).

Additionally, MITRE has created several Information Sharing and Analysis Organizations (ISAOs) like ASIAS, but in the healthcare domain:

- Healthcare Fraud Prevention Partnership (HFPP) (refer to Section A.2)
- National Health Safety Analytics Partnership (refer to Section A.3)

[91] https://www.mitre.org/

MITRE has also helped create ISAOs in the cybersecurity domain, including the Advanced Cyber Security Center (ACSC)—a New England-based non-profit consortium of industry, government, and academic organizations engaged in cyber-threat information sharing, cybersecurity research and development (R&D), and the creation of educational programs that help protect the region's public and private information technology infrastructure (refer to Section A.4).

Presently, MITRE is helping to form several other regional ISAOs similar to the ACSC, including the Mid-Atlantic Cyber Center (MACC) (refer to Section A.5) and the Northeast Ohio CyberConsortium (NEOCC) (refer to Section A.6).

MITRE also brings its perspective to bear as a long-standing, highly participative member of numerous ISAOs (refer to Section A.7). MITRE is highly experienced in the cyber-threat analysis and cyber standards domains. For example, MITRE staff developed the open-source threat-sharing analytic tool called Collaborative Research Into Threats (CRITs) (refer to Section A.8), as well as a set of open-source computer network defense tools that integrate with CRITs. MITRE has also developed a model, framework, and repository for describing and sharing the actions a cyber adversary may take while operating within an enterprise network (refer to Section A.9). Additionally, MITRE has developed cyber automation standards under the sponsorship of the U.S. Department of Homeland Security (DHS) that enable secure, automated sharing of cyber information (refer to Section A.10). Additionally, MITRE participates in the Information Sharing and Analysis Organization Standards Organization (ISAO SO) (refer to Section A.11).

A.1 Aviation Safety Information Analysis and Sharing

MITRE developed and implemented the ASIAS system to share data from airlines to improve air safety. As previously mentioned, MITRE acts as a hub that receives information from multiple airlines and the FAA. Members do not directly share information with each other; instead, each participant sends its data, which is often highly sensitive, to MITRE, and then MITRE works diligently to ensure that each member's data is kept confidential. MITRE gathers and analyzes this information and then provides reports to all participants on the key issues that affect airline safety. The growth of ASIAS, from 10 to 31 members in just a few years, and its continued government sponsorship are testaments to the value of this effort and to members' confidence in the process.

A.2 Healthcare Fraud Prevention Partnership

Under U.S. Government sponsorship, MITRE developed and operates the HFPP—a voluntary public-private partnership between the Federal Government, state officials, law enforcement, private health insurance plans and associations, and

healthcare anti-fraud associations. The HFPP aims to foster a proactive approach to detect and prevent healthcare fraud through data and information sharing; data analytics; and training, outreach, and education. MITRE provides the infrastructure and resources to gather and analyze healthcare information and then provides reports on suspected fraud to HFPP participants, while preserving the privacy of sources.

A.3 National Health Safety Analytics Partnership

MITRE created a collaborative and voluntary public-private national partnership to develop and share predictive analytics to systematically reduce medical errors and other harm to patients. The National Health Safety Analytics Partnership will improve patient safety through the sharing and integration of public and private-sector information regarding the indicators of precursors to "near miss" events. The initiative will yield transformational (order of magnitude) reductions in the occurrence of selected safety issues and will begin a national conversation across the health sector to address safety in a new, systematic, data-driven manner. In short, the goal of this partnership is "to take patient safety to the next level."

A.4 U.S. Advanced Cyber Security Center

The ACSC is a New England-based non-profit consortium that brings together university, industry, and government organizations to address advanced cyber threats. The primary focus is cross-sector collaboration to share cyber-threat information to better defend against advanced cyber threats, to engage in next-generation cybersecurity R&D, and to create education programs that protect the region's public and private information assets. Section 3.1 of this paper provides a detailed case study of the ACSC.

MITRE developed and hosts the technical infrastructure for the ACSC that enables the secure sharing of sensitive but unclassified cyber-threat information. This includes a secure sharing portal and a cyber-threat repository, as well as the MITRE-created CRITs threat repository and analysis platform (refer to Section A.8).

MITRE has been a key contributor to most of the activities that created the ACSC and now sustain its operations. These activities include work on the ACSC non-disclosure agreement; the 2011 launch of the ACSC at MITRE's Bedford, Massachusetts, location; hosting of collaboration space at MITRE–Bedford; and the sharing and collaboration constructs that enable face-to-face interactions, such as Cyber Tuesdays and Cyber Exchange Forums.

A.5 Mid-Atlantic Cyber Center

MITRE has been funded by the Commonwealth of Virginia to establish the Virginia Information Sharing and Analysis Organization (VA-ISAO) as a cross-sector, public-private partnership initially focused on sharing and analyzing cyber-threat information and defensive-response practices to better protect Virginia's cyber ecosystem.

The VA-ISAO is being established as part of a broader MITRE initiative to pilot a regional ISAO: the MACC. During the 2-year piloting of the MACC, MITRE will help expand the MACC's missions to include collaborative incident response, resource sharing, product/service evaluation, workforce development, federation with other ISAOs, cyber R&D, regional economic development, and citizen engagement and awareness.

A.6 Northeast Ohio CyberConsortium

"The Northeast Ohio CyberConsortium (NEOCC) is a cross-sector regional Information Sharing and Analysis Organization. This Consortium has been organized to become a Northeast Ohio center of excellence for cyber defense, formed to address and mitigate escalating cyber threats across various industries. The NEOCC aims to build platforms and develop services to enable more effective information sharing and analysis among members on cyber threats. "With a focus on the Northeast Ohio region, the NEOCC strengthens the community of corporate and institutional cybersecurity professionals in the region."[92] Section 3.2 of this paper provides a detailed case study of the NEOCC.

A.7 MITRE as an ISAO Member

In addition to its membership in the ACSC, NEOCC, and MACC, MITRE is a member of multiple Defense Industrial Base information-sharing exchanges. Some exchanges follow the hub-and-spoke model, while others use a post-to-all model. Thus, MITRE has firsthand experience with participating in different types of information-sharing collectives (refer to Section 2.1 of this paper). MITRE has gathered lessons learned from its participation in these exchanges and continuously evaluates what works and what needs to be improved in these groups.

[92] https://www.isao.org/information-sharing-groups/

A.8 Collaborative Research Into Threats

A strong threat-based defense strategy relies on an intelligence-based approach that can successfully anticipate, detect, prevent, and respond to threats. Numerous observations of threat characteristics need to be collected, chronicled, shared, and analyzed over time. To fill this need, MITRE created CRITs—a sophisticated threat information management tool that can both manage vast volumes of data and provide the analytic sophistication needed to discover patterns and trends. Tracking and leveraging threat characteristics can reduce the likelihood of success of future attacks.

CRITs is unique in the way it pulls together the disconnected pieces of a threat puzzle and allows its users to share information among different groups within the organization or community. When used in a consortium, CRITs provides sharing partners with critical threat information that they typically would not have access to when working alone. Sharing through CRITs enhances network defense and improves the return on investment by leveraging partner organizations' cyber-threat experiences and investments.

CRITs software was licensed to more than 100 government and private organizations, many of which are testing and learning from the prototype to help provide future requirements of the tool. CRITs is now available as open-source software.[93]

A.9 Adversarial Tactics, Techniques, and Common Knowledge and Cyber Analytics Repository

A high-level view of an adversary's life cycle is important to understand the phases a cyber adversary goes through to compromise an environment and work toward an objective, but is not enough to understand the common actions they perform and how those actions can be effectively mapped to defenses within an enterprise network. MITRE created the ATT&CK™[94] model and methodology for deconstructing an adversary's life cycle and representing the information in a way that helps defenders better understand the context surrounding adversarial behaviors. Empirical evidence of persistent threat behavior documented in open source threat reporting served as the basis of ATT&CK to keep the model grounded. ATT&CK has since expanded to incorporate research from security researchers, red teams, and attacker methods that are likely to be incorporated into an adversary's arsenal of techniques.

[93] https://crits.github.io/
[94] https://attack.mitre.org/wiki/Main_Page

The ATT&CK threat model is in use across government and industry to better define and understand adversary behavior. The most common use cases include developing behavioral analytics, adversary emulation, threat hunting, defensive gap analysis, training, and evaluation of security products.

MITRE developed the Cyber Analytics Repository (CAR)[95] to complement ATT&CK. CAR is a collection of post-exploit behavioral analytics based on the behaviors described ATT&CK that MITRE shares with the cyber-defense community (refer to Appendix C).

A.10 Cyber Standards

MITRE is the developer and custodian of multiple cybersecurity standards, including Common Vulnerabilities and Exposures (CVE®)[96] and Open Vulnerability and Assessment Language (OVAL®).[97] In this role, MITRE is sponsored by the U.S. Government to lead the development of industry collaboration standards.

MITRE continues leading the effort on two initiatives for sharing cyber-threat information: TAXII[98] and STIX,[99] which are both sponsored by DHS. TAXII defines a set of protocols for securely exchanging cyber-threat information for real-time detection, prevention, and mitigation of cyber threats. STIX provides a common format for cyber-threat information. Together, TAXII and STIX will enable threat-sharing communities to exchange actionable, structured threat intelligence to promote collective defense. MITRE is currently working with the Organization for the Advancement of Structured Information Standards (OASIS) to further develop and transition DHS specifications for TAXII and STIX to OASIS open standards.[100]

MITRE also collaborates in similar community efforts for vulnerability management, software assurance, application security, asset management, enterprise reporting, malware protection, configuration management, event management, and remediation.

A.11 Information Sharing and Analysis Organization Standards Organization

MITRE is a key contributor to the ISAO SO,[101] which is sponsored by DHS to establish best practices in establishing and operating ISAOs. MITRE participates in

[95] https://car.mitre.org/wiki/Main_Page
[96] https://cve.mitre.org/
[97] https://oval.mitre.org/
[98] https://taxiiproject.github.io/
[99] https://stixproject.github.io/
[100] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti
[101] https://www.isao.org/

the ISAO SO's Working Groups and Core Development Teams to collaboratively develop specific standards and guidelines for the creation and functioning of ISAOs.

Appendix B. Cyber Threats[102]

Figure 10 illustrates two major types of cyber threats—conventional cyber threats and advanced cyber threats—and how these threat types decompose into five threat subtypes based on adversarial intent, capability, and effect. This figure pairs each of the five threat subtypes (top row) with the needed defensive posture (bottom row) to address the respective threat subtype.

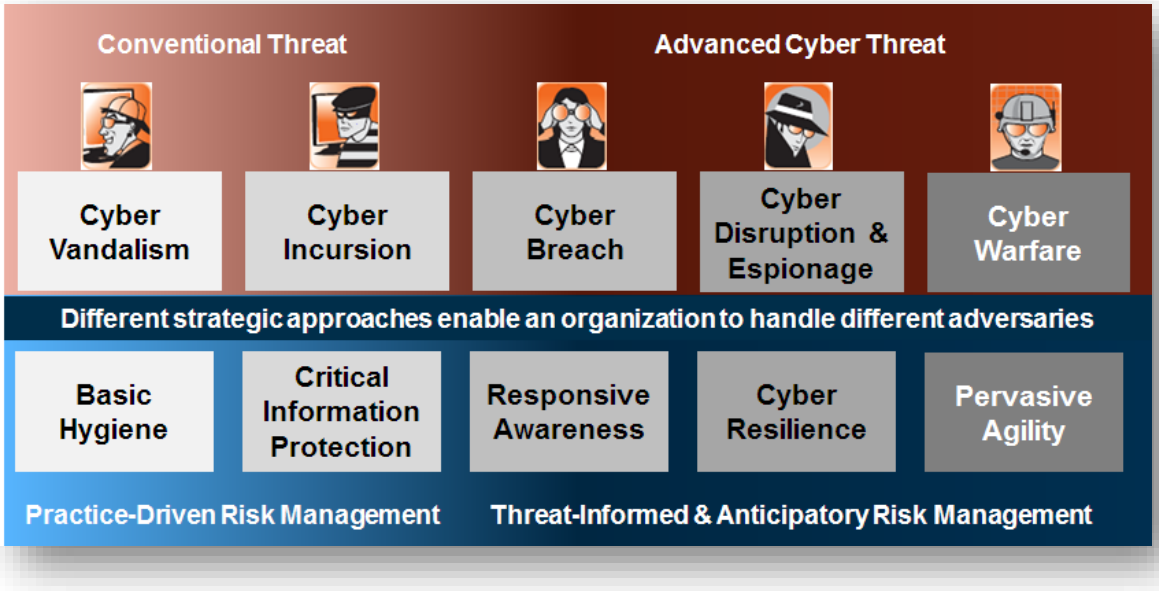


Figure 10. Cyber Threat Types

[102] https://www.mitre.org/publications/technical-papers/how-do-you-assess-your-organizations-cyber-threat-level

This page intentionally left blank.

Appendix C. Threat Intelligence

An effective approach for sharing cyber-threat information among partners is based on analyzing a cyber-attack "campaign." A cyber campaign consists of two parts: (1) intrusion attempts and (2) tactics, techniques, and procedures (TTPs), as shown in Figure 11. Together, these parts reveal the adversary's method of attack. TTPs are the methods and approaches that a cyber attacker uses repeatedly over a series of related intrusion attempts. TTPs include target lists and how they are compiled; the tools that are used; the infrastructure components, entities, and accounts that are targeted; and how these elements are sequenced and used across the Cyber-attack Life Cycle (refer to Appendix D) to conduct a series of related intrusion attempts.

An intrusion attempt consists of the distilled parts and telltale signs of a cyber-attack. This can include the domains that are used to launch attacks and host command and control channels, the email sources that are discernible, and the intelligence that can be obtained from the malware samples used in the attack.

Because information about attempted intrusions does not reveal an organization's vulnerabilities, it can generally be shared with partners to provide them with defensive value at a modest level of risk and effort.

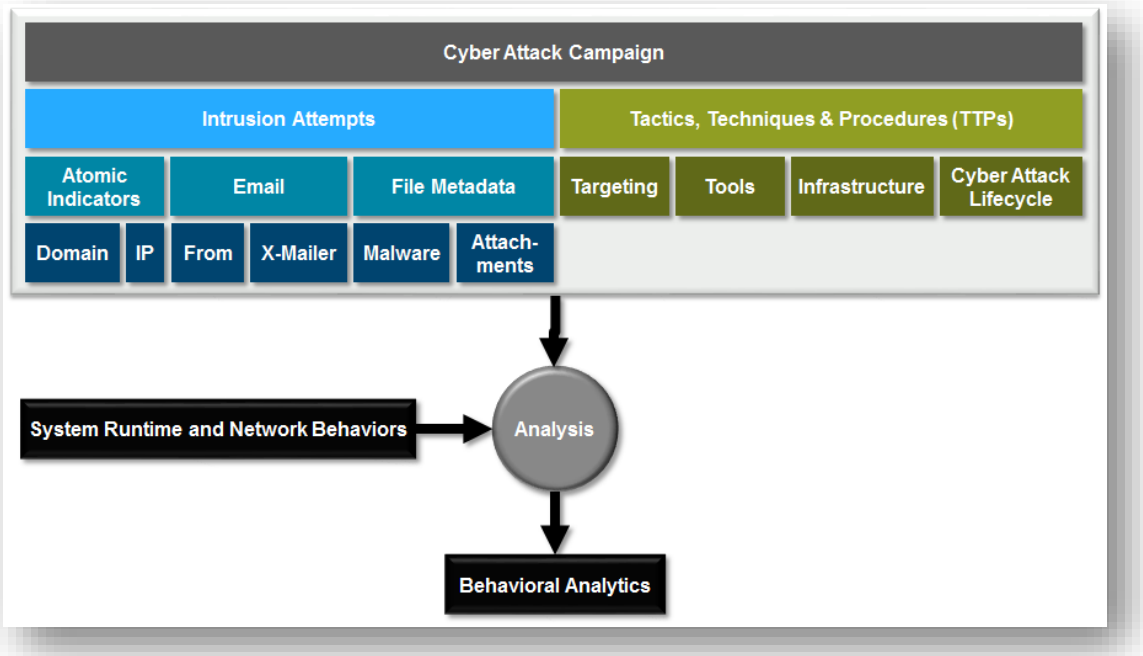


Figure 11. Cyber-attack Campaign

Behavioral analytics are designed to detect detailed patterns of adversary behavior derived from observed and reported adversarial actions and tools. Adversarial behavior should be viewed as a subset of TTPs that may leverage benign system and network functionality that is used for malicious purposes. CAR is a collection of post-exploit behavioral analytics based on known adversarial behaviors described in the ATT&CK model. The behavioral analytics in CAR can be used to dramatically improve detection of adversary activity patterns by focusing on common actions performed across many different campaigns.

Sharing TTPs and behavioral analytics provides far greater defensive value to members, but it puts the contributing partner at greater risk if it reveals the organization's threat-based defensive capabilities. In addition, TTPs require a greater level of effort to produce because large volumes of data must be collected over time, followed by sophisticated analyses. Similarly, behavioral analytics require many types of data, including telemetry from endpoint systems, and the ability to proactively test and refine analytics to effectively derive adversarial behavior patterns within an environment. Analytics may be developed for a particular security information and event management platform, so having access to the adversary behavior, either through direct observation or sharing, will allow an organization to develop and tune a detection analytic specific to their environment through adversary emulation.

Common terminology, automation, and security are needed to accomplish effective sharing of cyber-threat information among organizations. Central to this are robust cyber standards, including the taxonomy, hierarchy, and structures defined by the Structured Threat Information eXpression, as well as the secure, real-time, automated transmission of information defined by the Trusted Automated eXchange of Indicator Information protocol.

Appendix D. Active Defense[103]

Cyber-attacks from advanced actors are growing in scope and frequency. These attacks are successful because current defensive strategies are not well-suited to mitigate prolonged and determined attackers who are leveraging advanced techniques. Most organizations continue to focus on preventing zero-day exploits by relying on commercial security products, such as patching and blocking bad domain names and Internet Protocol addresses.

While these approaches are effective against some types of threats, they fail to stop advanced attacks and provide no knowledge of what an adversary does once the network has been penetrated. A more effective framework for thinking about cyber defense is the Cyber-attack Life Cycle, as shown in Figure 12, which was originally conceived by Lockheed Martin as the Cyber Kill Chain.[104]

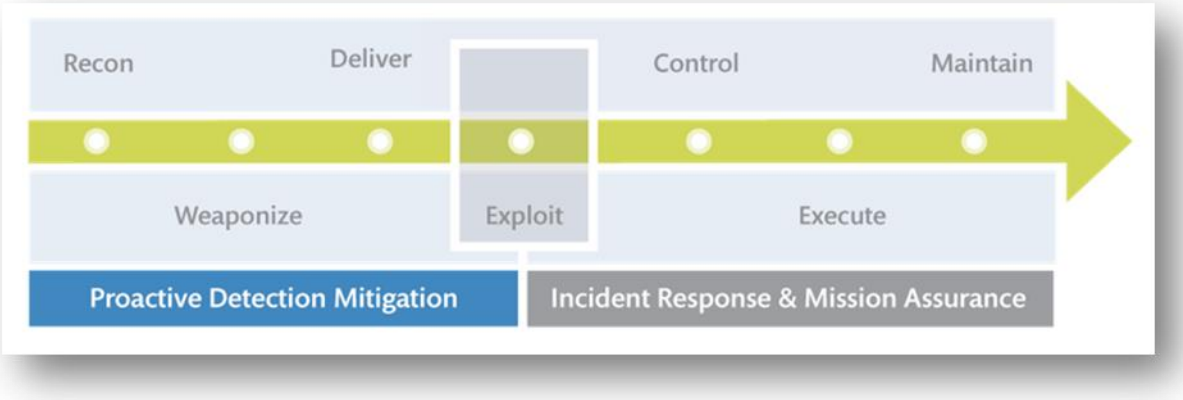


Figure 12. Cyber-attack Life Cycle

The Cyber-attack Life Cycle shown in Figure 12 depicts the 7 phases of a cyber-attack:

- Phase 1: Recon—the adversary develops a target.
- Phase 2: Weaponize—the attack is put in a form to be executed on the victim's computer/network.
- Phase 3: Deliver—the means by which the vulnerability is weaponized.
- Phase 4: Exploit—the initial attack on the target is executed.

[103] https://www.mitre.org/publications/technical-papers/active-defense-strategy-for-cyber
[104] http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

- Phase 5: Control—mechanisms are employed to manage the initial victims.
- Phase 6: Execute—leveraging numerous techniques, the adversary executes the plan.
- Phase 7: Maintain—long-term access is achieved.

The early steps of the Cyber-attack Life Cycle (before Phase 4: Exploit) represent an opportunity to proactively detect and mitigate threats before the adversary establishes a foothold. After Phase 4: Exploit, incident detection/response can be exercised along with the assurance of mission-critical assets. To best leverage the opportunity for active defense, it is necessary to perform a retrospective analysis of threat characteristics across the entire Cyber-attack Life Cycle and correlate the results to produce telltale indicators.

By understanding an adversary's Cyber-attack Life Cycle, the defenders have more opportunity to discover and respond to an attack. Phases 1 through 7 of the Cyber-attack Life Cycle can be employed as strategies for defense:

- **Recon:** Mine and analyze open resources to provide indicators and warnings of intrusion attempts.
- **Weaponize:** Analyze artifacts to create high-fidelity signatures to detect malicious activity.
- **Deliver:** Understand adversaries' tools and techniques for delivering messages in order to intercept them early.
- **Exploit:** Leverage anti-exploitation and exploit-detection techniques to find zero-day attempts.
- **Control:** Employ robust intrusion-detection signatures and tools to detect newly installed implants.
- **Execute:** Instrument and configure internal networks to detect existing internal compromises.
- **Maintain:** Deploy advanced host analysis to detect hidden implants and abnormal activity.

Active defense that leverages the adversary's Cyber-attack Life Cycle requires detailed cyber intelligence. This intelligence is best created through information sharing with peer organizations. Defenders can generate a robust set of adversary TTPs only by understanding the adversaries' behavior against a range of targets over a period of time. By sharing information on TTPs, defenders gain valuable insights into an attacker's overall campaign plans and strategies. This, in turn, improves the defenders' ability to predict attacker behavior and create more

dynamic defenses. However, scaling the sharing process across multiple organizations requires the parties involved to develop and/or use common security standards (such as Structured Threat Information eXpression and Trusted Automated eXchange of Indicator Information, described in Section A.10 of Appendix A) and to employ trust models that enable genuine collaboration. A federation of sharing communities, each with its own trust circle (refer to Section of this paper) among its members using common sharing standards, will enable the most effective active defense strategy.

This page intentionally left blank.

Appendix E. List of Acronyms and Abbreviations

ACSC	Advanced Cyber Security Center
AIS	Automated Indicator Sharing
ASIAS	Aviation Safety Information Analysis and Sharing
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
BoD	Board of Directors
CAR	Cyber Analytics Repository
CEF	Cyber Exchange Forum
CERTs	Computer Emergency Response/Readiness Teams
CIAT	Center for Information Age Transformation
CISA	Cybersecurity Information Sharing Act of 2015
CISCP	Cyber Information Sharing and Collaboration Program
CoE	Center of Excellence
CONOPS	Concept of Operations
CRADA	Collaborative Research and Development Agreement
CRAFA	Cybersecurity Risk Analysis based on Financial Engineering and Big-Data Analytics
CRITs	Collaborative Research Into Threats
CSP	Commercial Service Provider
CT	Cyber Tuesday
DHS	Department of Homeland Security
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FFRDC	Federally Funded Research and Development Center
FS-ISAC	Financial Services Information Sharing and Analysis Center
HFPP	Healthcare Fraud Prevention Partnership
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization

ISAO SO	Information Sharing and Analysis Organization Standards Organization
ICT	Information and Communication Technology
IT	Information Technology
MACC	Mid-Atlantic Cyber Center
MassIT	Massachusetts Office of Information Technology
MIGP	Mass Insight Global Partnerships
NCC	National Cybersecurity Center
NCCIC	National Cybersecurity and Communications Integration Center
NCX	National Cyber Exchange
NDA	Non-disclosure Agreement
NEOCC	Northeast Ohio CyberConsortium
OASIS	Advancement of Structured Information Standards
R&D	Research and Development
RFI	Request for Information
RMTA	Rocky Mountain Technology Alliance
STIX	Structured Threat Information eXpression
TAXII	Trusted Automated eXchange of Indicator Information
Tech Ops	Technical Operations
TTPs	Tactics, Techniques, and Procedures
U.S.	United States
US-CERT	United States Computer Emergency Readiness Team
USD	United States Dollar
VA-ISAO	Virginia Information Sharing and Analysis Organization
WCX	Western Cyber Exchange