MID-OHIO REGIONAL
MORPC
PLANNING COMMISSION

111 Liberty Street, Suite 100
Columbus, Ohio 43215
morpc.org

T. 614. 228.2663
TTY. 1.800.750.0750
info@morpc.org

NOTICE OF A MEETING
DATA POLICY NEEDS SURVEY & TOOLKIT WORKING GROUP
MID-OHIO REGIONAL PLANNING COMMISSION

REMOTE MEETING

May 26, 2020 2:30 pm – 4:00 pm

AGENDA

1. **Welcome & Introductions**
2. **Survey Development**
3. **Focus Groups**
4. **Local Government Data Resources –** SharePoint
5. **Other Business**
   - **Public-Private Cyber Intel and Fusion Center**
6. **Next Steps**
7. **Adjourn**

Please notify Lynn Kaufman at 614-233-4189 or LKaufman@morpc.org to confirm your attendance for this meeting or if you require special assistance.

Join Microsoft Teams Meeting
+1 614-362-3056 United States, Columbus (Toll)
(888) 596-2885 United States (Toll-free)
Conference ID: 823 053 00#

The Date and Time of the Next Meeting of the
Data Policy Needs Survey & Toolkit Working Group
is TBD
This Meeting may be held remotely; details to follow.

Creating A More Robust Public-Private Partnership in Information Security Operations

Creating A More Robust Public-Private Partnership in Information Security Operations

This whitepaper discusses the challenges and opportunities for creating a Public-Private Information Security Operations Center ("PP-ISOC") and how to overcome those challenges. In order to succeed in this public-private partnership, challenges relating to reputational harms of participants, liabilities, privacy challenges for the sharing of cyber threat information, improving the quality of information through the PP-ISOC, and others will need to be addressed. The remainder of this white paper discusses the advantages and challenges relating to the PP-ISOC in greater detail. It also proposes various ways some of the challenges can be overcome. However, it does not appear that there are many roadblocks that would prevent such a partnership and operations center from being established.

A. Introduction.

While there are many Information Sharing and Analysis Organizations ("ISAOs") and Information Sharing and Analysis Centers ("ISACs") that are operational, very few operate as real-time information security operations centers. The type of network and personnel integration, protection, and joint response capability that this new information security initiative hopes to create requires a deep level of engagement by participants in both the private and public sectors. When done successfully, such engagement could allow participating entities to establish and maintain security operations in a joint "fusion-center" format that can accommodate multiple operational models while obtaining information from public and private sources and allowing collective responses to cyber threats.

Recently, Indiana University, Northwestern University, Purdue University, Rutgers University and the University of Nebraska-Lincoln created a cyber security operations center that combines real-time security data feeds from the member campuses to identify malicious activity and secure all campuses.[1] A more in-depth approach could allow both public and private entities in close proximity with one another to do the same for both public and private networks, for example in Central Ohio.

Leveraging and expanding the existing Columbus Collaboratory ISAO to create and maintain a joint information security operations center that uses real-time network monitoring, detection, analysis, and response tools and personnel from each of its participants could be useful in providing more efficient and effective responses to evolving information security challenges.

B. Advantages.

A real-time and in-depth collaboration between private and public entities may have various advantages to its participants, including the protection of all of the participants to the PP-ISOC. By enabling state government to partner directly with industry at the security practitioner level, public entities gain access

[1] The Universities created a new, shared cybersecurity operations center called OmniSOC. You may read more about it here.

to practitioners in the private sector who may reside in more mature enterprise environments, and private entities gain access to a larger number of practitioners focused on combating similar threats. Creating a PP-ISOC may also provide opportunities to cost-effectively share important cyber threat intelligence that ultimately results in better protection for both private and public networks. Education and career opportunities may help create a state cyber militia[2] and provide private-sector employment for individuals after the completion of their deployment.[3]

C. Challenges.

There are various challenges with creating and participating in a PP-ISOC, including reputational harms, privacy concerns, liability for sharing threat information, and other items. While these challenges create risks for the private entities participating in the PP-ISOC, it may be possible to mitigate some of these risks with careful planning.

1. **Reputational harms and potential loss of customers is possible with participation in the PP-ISOC.**
    a. Some companies may be reluctant to share information if government staff are at the table, even with immunities in place. Voluntarily sharing information with the government for what may be viewed as a law enforcement purpose may create issues with some customers given the national dialogue on information privacy issues.
2. **Privacy concerns remain relating to the sharing of personal information of customers of Nationwide, customers of the other private entities participating in the programs, and the public at large, whose personal information may be involved in the information sharing.**
    a. Information shared when government staff are at the table must comply with the restrictions of the Cybersecurity Information Sharing Act (CISA) of 2015 in order for the private entity to continue to enjoy the limitation of liability under CISA. Therefore, entities joining the PP-ISOC will need to ensure that only the information that falls under CISA (cyber threats and defensive measures) is provided to other entities and that the information that is provided is appropriately deidentified in accordance with the Department of Homeland Security and Department of Justice guidance on CISA.[4]

---

[2] There are already some state initiatives to create a state cyber security reserve force, such as Ohio Senate Bill 52. You can read more about those efforts here.

[3] Recently, MasterCard, Microsoft, Workday, and Partnership for Public Service partnered to launch the Cybersecurity Talent Initiative to help recruit and train the next generation of cybersecurity technologists and pay for outstanding student loans. You may read more here.

[4] Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015, by The Department of Homeland Security and The Department of Justice, June 15, 2016, available here. You may find additional guidance from the DHS/DoJ on Privacy and Civil Liberties Final Guidelines here.

3. **Most of the liability for sharing threat information that turns out to be inaccurate has been excluded with CISA.**

    a. Civil or criminal liability for the sharing of cybersecurity information is likely to be one of the most important factors in preventing the sharing of cyber threat intelligence information between private and public entities.[5]

    b. The Cybersecurity Information Sharing Act (CISA) of 2015 largely curbed many of the concerns relating to liability for the sharing of information with federal, state, and other private entities so long as the entities comply with its requirements.[6]

    c. However, CISA's liability limitation mechanism applies only when the sharing or receiving of information is done according to the requirements of the CISA. For example, CISA defines cyber threats and defensive measures and requires that such information be used solely for cybersecurity purposes. Furthermore, it requires that certain personal information be removed prior to sharing this information. Failure to comply with the requirements of the Act could result in the liability limitation not being applicable to the private entity. Furthermore, sharing with the federal government with the privacy protections in place requires that the DHS process be used.[7] This obligation to remove personal information before sharing with the government may take on additional importance for companies that are subject to more strict privacy regulations—such as with respect to the GDPR in Europe.

    d. Participation in the PP-ISOC or sharing of cyber threat information might create additional challenges in regulated industries where there is increasing attention by regulators in cybersecurity. However, CISA has created some exceptions from enforcement by regulators.[8]

4. **Some concerns still exist that sharing of confidential business information with other businesses and the state government will remove the trade secret or other confidentiality protections relating to the information.**

---

[5] For a more thorough examination of these issues, please see Cybersecurity and Information Sharing: Legal Challenges and Solutions by the Congressional Research Service.

[6] CISA allows for the sharing of information between private entities and state entities and also limits liability arising from such sharing so long as the requirements of the Act are complied with (6 U.S.C. § 1503(c)(1)). The law also provides antitrust protections for the sharing of this information (§ 1503(e)(1)). The law exempts from disclosure the open records laws (§ 1503 (d)(4)(B)). Sharing of information should also not result in the waiver of a privilege (§ 1504(d)(1)). The Department of Justice and Department of Homeland security issued additional Guidance on CISA in 2016, available here. DHS and DOJ have published FAQs on CISA and the information sharing provisions, which is available here.

[7] The Department of Justice and Department of Homeland security issued additional Guidance on page 12, available here.

[8] 6 U.S.C. § 1503(d)(4)(c)(i).

a. This concern has been largely alleviated with CISA when the sharing happens to the federal government, specifically using DHS approved methods.[9] However, this protection is not explicitly offered for sharing by a private entity to the state or local governments or other private entities. Therefore, using agreements to govern the confidentiality of information shared between the participants to the PP-ISOC will be important.

5. **There are concerns that shared cyber threat indicators received may not be of good quality.**

   a. Recent reports appear to suggest that cybersecurity threat information sharing with the federal government is limited to only 6 entities providing information to DHS.[10] Other reports appear to suggest that the shared cyber threat information is more focused on quantity instead of quality.[11] For the PP-ISOC to be successful, more participation and more quality information sharing may be crucial. Increasing the number of practitioners and providing some education concerning high quality information sharing – as the Columbus Collaboratory already does - increases both the quality and quality of interactions.

6. **Concerns that private information stored in government databases will become discoverable through freedom of information laws requests have been largely alleviated.**

   a. This concern has been largely alleviated with CISA in that information shared with the State should be exempt from freedom of information laws.[12]

7. **Concerns under Electronic Communications Privacy Act (ECPA) of 1986 and wiretap laws have largely been alleviated.**

   a. Concerns relating to ECPA have been largely alleviated through the limitation of liability provisions of CISA.[13] Nevertheless, monitoring of the networks and sharing of those entities' data pursuant to agreements may help alleviate some of the concerns that may arise from the participants' network.

   b. However, hacking back is not permitted under CISA; therefore, the PP-ISOC will be limited in that the definition of defensive measures excludes any activity that violates the Computer Fraud and Abuse Act.[14]

8. **Concerns around the sharing of classified information have work arounds.**

   a. A concern with government entities sharing cyber threat information that includes private information is the limitation relating to classified information. CISA appears to take this into

[9] 6 U.S.C. §§ 1504(d)(1) and (2).
[10] Report available here.
[11] Report available here. According to the DHS biennial report, available here, the Inspector General report stated that "one agency representative told us that although DHS provided 11,447 cyber threat indicators in 2016, only 2 or 3 of these indicators were found to be malicious and related to cyber incidents."
[12] 6 U.S.C. § 1504(d)(1).
[13] 6 U.S.C. § 1505(b).
[14] See FAQ 16 here and exclusions to defensive measures under § 1501(7).

consideration and alleviates some of the concerns by stating that sharing should take place with appropriate security clearances,[15] other information may be declassified and shared with private entities,[16] and the sharing itself does not affect the use of classified information by the federal government.[17]

D. **Overcoming Challenges.**

1. Resourcing the PP-ISOC.

To create a truly valuable information sharing forum – one that is well differentiated from the plethora of formal and informal fora already available – the PP-ISOC will need to be resourced to provide effective governance, facilitation, tools, primary source intelligence, management, and legal support. Additionally, a physical facility may be required to create a true joint/fusion-center environment.

2. Creating immunities for liability challenges.

a. Liability for incorrect reports or intelligence shared within the PP-ISOC may be the most important challenge to the success of better integrated data security operations.

b. The sharing of information may subject all of the participants to lawsuits, including class action lawsuits in the event of a data breach or a security response.[18]

c. CISA has addressed many, but not all, of the challenges for sharing of cyber threat information. For example, the sharing of cyber threat information with state governmental entities and related limitations of liability are not addressed under CISA—while the sharing with federal governmental entities and the DHS is.

d. Furthermore, these liability protections may not be available to state entities under CISA because they can only be invoked by private entities (and public entities that are utilities).[19]

e. On the other hand, we were unable to find any examples of any lawsuits that resulted directly from sharing of cyber threat information or defensive measures under CISA. Therefore, some of the concerns relating to the sharing of this information may be more perceived than actual.

f. Passing a state law that would allow the sharing of cyber threat information with state entities and related limitations of liability would help foster additional sharing of

[15] 6 U.S.C. 1502(a)(1).
[16] 6 U.S.C. 1502(a)(2).
[17] 6 U.S.C. 1507(c)(1).
[18] For example, in 2017, following reports of a Chrysler vulnerability that allowed some of the functions of an automobile to be remotely taken over, the Auto-ISAC was served with a subpoena, though a court ultimately quashed it. A quick search did not reveal other instances of when ISACs were involved in a lawsuit or references to CISA.
[19] See FAQ 17 here.

information with state entities. However, this effort would require a 50-state effort, given that an immunity created by statute in Ohio may not apply in Indiana.

3. **Addressing privacy concerns with public engagement and recourse.**

    a. Addressing privacy concerns from civil liberties and privacy advocates may be the second most important challenge in the success of the PP-ISOC. Civil liberties advocates[20] have generally been opposed to the indiscriminate sharing of cyber threat intelligence between public and private entities due to the possible violations of constitutional rights as well as the possible abuses of the information by public or private entities.

    b. It may be possible to overcome some of the privacy concerns with additional transparency, prior and frequent public engagement, education, and marketing efforts.

4. **Creating incentives for sharing quality cyber threat information.**

    a. Additional funding for a cyber security center and a pilot program for the deployment of network sensors may also be helpful to establish and maintain the PP-ISOC. A new bill in the Senate has a pilot program for the installation of network sensors.[21] Funding and deploying a new pilot program in a state program could help standardize the network sensor and monitoring technology used by the participants to the PP-ISOC.

5. **Creation of a simple and accessible method for being removed from threat lists.**

    a. It may also be possible to create a prompt and effective recourse mechanism for individuals whose personal information has been inadvertently involved in the information shared through the PP-ISOC.[22]

6. **Signing cooperative research and development agreements.**

    a. Given that ISACs and ISAOs have established mechanisms for membership and are also generally protected as private entities under CISA, the PP-ISOC should follow a similar mechanism for membership and operation, for example, by using agreements that govern membership. It may also be advisable to follow available NIST documentation in this area.[23]

---

[20] See ACLU's complaints (and here) relating to the Cyber Information Sharing Act of 2015.

[21] Efforts in the 116th Congress include Senate Bill 1846, which would allow DHS's 24-hour cyber situational awareness and incident response center called National Cybersecurity and Communications Integration Center (NCCIC) to provide (in coordination with Multi-State Information Sharing and Analysis Center) guidance and training if requested by state and local governments to help them combat cyber threats. This bill would also create a pilot program deploying network sensors capable of utilizing classified indicators for identifying and filtering malicious network traffic.

[22] One approach may be to use examples such as the SpamHaus project, which was created for the blocking of spam emails.

[23] See NIST SP 800-150, available here.

b. For example, these agreements between contributing entities should cover issues to confidentiality, non-disclosure, non-attribution, trade secrets, and privilege issues—to the extent possible.[24]

7. New state legislation modeled after federal legislation and possibly expanding the scope of CISA.

a. It may be helpful to pass additional state legislation to encourage the sharing of information with state entities. In fact, given the slow pace of information sharing with federal entities, and the free-rider problem, it may be an opportune time to examine the possibility of passing state legislation that requires the sharing of cybersecurity information with private and public entities.

b. Given some of the ambiguities and limitations present in CISA, it may also be helpful to pass additional federal laws to clarify the liabilities and confidentiality protections.

E. Additional Materials.

For additional reading regarding the cybersecurity arena and related risks, please refer to the following materials:

1. CISA, which provides many protections to private entities for sharing information with the federal government and other private entities, is available here, here, and at 6 U.S.C. § 1501.

2. Executive Order 13691 Promoting Private Sector Cybersecurity Information Sharing, which established ISAOs, is available here.

3. Presidential Decision Directive/NSC-63 on Critical Infrastructure Protection, which established ISACs, is available here.

4. NIST SP 800-150 Guide to Cyber Threat Information Sharing is available here.

5. Cybersecurity Update: Heightened Concerns, Legal and Regulatory Framework, Enforcement Priorities, and Key Steps to Limit Legal and Business Risks, Paul Weiss, September 30, 2015, available here.

6. Cybersecurity and Information Sharing: Legal Challenges and Solutions, Andrew Nolan, Congressional Research Services, March 16, 2015, available here.

7. MITRE, Building a National Cyber Information-Sharing Ecosystem, May 2017, available here.

8. Collaborative Cyber Defense, Barriers and Best Practices for Strengthening Cyber Defense by Collaborating Within and Across Organizations, May 2018, available here.

9. Information Sharing: Economic Analysis, by N. Eric Weiss, Congressional Research Services, June 3, 2015, available here.

[24] The FS-ISAC agreement is available here and the DHS Automated Indicator Sharing Terms of Use is available here. ISAO standards organization also generates many standards relating to ISAOs, available here.

10. Biennial Report on DHS' Implementation of the Cybersecurity Act of 2015, Office of the Inspector General, The Department of Homeland Security, November 1, 2017, available here.

11. Efforts in the 116th Congress include Senate Bill 1846, which would allow DHS's 24-hour cyber situational awareness and incident response center called National Cybersecurity and Communications Integration Center (NCCIC) to provide (in coordination with Multi-State Information Sharing and Analysis Center) guidance and training if requested by state and local governments to help them combat cyber threats. This bill would also create a pilot program deploying network sensors capable of utilizing classified indicators for identifying and filtering malicious network traffic.