NOTICE OF A MEETING
REGIONAL DATA ADVISORY COMMITTEE
MID-OHIO REGIONAL PLANNING COMMISSION

REMOTE MEETING

June 2, 2020, 1:00 pm – 2:30 pm

AGENDA

1. **Welcome & Introductions**
2. **2020 Census Update** – *Aaron Schill*
3. **MORPC Staff Updates** – *Aaron Schill*
   a. COVID-19 Hub
   b. Regional Housing Strategy
4. **Public-Private Cyber Intel and Fusion Center** – *Kirk Herath & Nathan Wymer, Nationwide*
5. **Regional Public Policy Update** – *Joe Garrity*
6. **Working Group Reports**
   a. Regional Information & Data Group – *Charlie Burks*
   b. Sustainability Dashboard – *Rick Stein*
   c. Data Policy Needs Survey & Toolkit – *Doug McCollough*
   d. Regional Municipal Fiber Strategy – *Gene Oliver*
   e. Central Ohio GIS User Group – *Cheri Mansperger*
7. **Next Steps**
8. **Other Business**
9. **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: 977 305 713#

The next RDAC Meeting will be
September 1, 2020, 1:00 pm

Mid-Ohio Regional Planning Commission

Remote Meeting

Regional Data Advisory Committee
Meeting Notes

June 2, 2020, 1:00 pm

Members Present

Charlie Burks, Columbus Metropolitan Library
Chair Brad Ebersole, Consolidated Electric Cooperative, Inc.
Shoreh Elhami, City of Columbus
Vice Chair Jung Kim, One Columbus
Doug McCollough, City of Dublin
Jonathan Miller, Delaware County Regional Planning Commission
Gene Oliver, City of Worthington
Tom Reed, Educational Service Center of Central Ohio
Theresa Seagraves, Franklin County Public Health
Rick Stein, Urban Decision Group

Public Present:

Brandon Brown, City of Dublin
Christina Drummond, Educopia
Rick Frantz, City of Dublin
Kirk Herath, Nationwide
Justin Milam, City of Upper Arlington
Katie Phillips, OSU CURA
Christian Selch, City of Columbus
Dan Sowry, Ohio EPA
Lawrence Ware
Nathan Wymer, Nationwide

MORPC Staff Present

Joe Garrity
Shawn Hufstedler
Natalie Hurst
Lynn Kaufman
Cheri Mansperger
William Murdock
Aaron Schill
Brian Shang
Liz Whelan
Brandi Whetstone

Meeting Called to Order at 1:05 pm.

2020 Census Update

Census Timeline:

June 1, 2020	Field offices began opening, and data collection will begin, specifically group quarters and the homeless count.
July 31, 2020	Self-response period ends.
August, 2020	Non-response follow-up by enumerators will begin.
October 31, 2020	Data collection period ends.
Spring 2021	Apportionment counts are delivered to the President and Congress.
July 2021	State and local redistricting data is released.

Participant Statistical Areas Program (PSAP)

MORPC has finished the review and validation of the PSAP program, the redrawing of census tracts and block groups – non-jurisdictional boundaries for the Census. The Cities of Dublin, New Albany, Grove City, Westerville, and Hilliard had tracts split due to increased population, as well as other parts of Delaware, Union, Licking and Fairfield Counties. The City of Columbus Downtown census tracts were revised, and now only reflect the actual downtown area, which is an important change that will help anyone doing population analysis and projection.

Response Rate Tracking
Aaron Schill directed the members' attention to the Census Bureau's Response Rate Page. MORPC has created a tableau dashboard for response rate tracking and comparison. The dashboard is fed daily, and can be accessed via MORPC's open data website, M.O.O.D. The dashboard will help with targeted marketing and show trends for tracts. MORPC staff created the dashboard based on feedback from community leaders who asked for simple way to view response rate data.

MORPC Staff Updates
COVID-19 Hub
MORPC staff created the COVID-19 Hub in March to meet needs expressed by local governments for accurate, timely COVID-19 information. Staff has recently added re-opening strategies, a survey to gauge the impact of the stay at home order on municipalities, other mapping resources, and links to other resources.

Regional Housing Strategy
Data collection and analysis is done, and the process is transitioning into implementation strategies, investment strategies, and other recommendations. Staff will use ESRI's open data program to create a Regional Housing Strategy resource hub, similar to the COVID-19 Hub. So far, findings show that the local housing market is tight, with high pressure in the affordable market. Developers have not been building enough housing to keep up with the need; this gap was hidden by the slow housing market during the recent recession.

Broadband (Digital Inclusion)
Since the stay-at-home order went into effect, broadband has become critical to everyone. MORPC and key partners are addressing the immediate broadband access needs of communities to come up with long-term solutions to access for tele-working and remote learning. Funds from the philanthropic community and COVID-19 funds may be deployed to address these issues.

MORPC is partnering with non-profit PCs for People which distributes low-cost computers to income-eligible households with K – 12 children. MORPC staff participated in an event on May 19 where 300 – 400 devices were distributed, with another distribution event scheduled for Thursday, June 4. These distribution events are planned for every other week through the end of the summer. The local offices of PCs for People and MORPC are looking for public- and private-sector partners for this program.

ESRI Urban
ESRI Urban is a platform for 3D modeling and scenario planning. It will give MORPC the ability to 3D model all the buildings and landscape in Franklin County, to start with. It will also allow MORPC and partners to research different development scenarios and the impact of zoning changes and land use changes. MORPC will be the home of the regional instance of the platform, and all the local communities will be able to take advantage of it. Staff and ESRI are working through the contract process with the intention to start using ESRI Urban July 1.

Public-Private Cyber Intel and Fusion Center, a presentation by Kirk Herath & Nathan Wymer, Nationwide
Click here to see the full presentation.

Regional Public Policy Update – Joe Garrity
Click here to see Joe Garrity's presentation.

Working Group Reports
Regional Information & Data Group (RIDG)
The RIDG user group met virtually on April 22, with 32 attendees. Discussion centered on the 2020 Census, beta testing the Sustainability Dashboard, and showcase presentations from members describing their work around COVID-19. Attendees also participated in five breakout sessions on Long Term Impacts of COVID-19, Remote Working, Lessons on Data Governance in a Crisis, Metadata Woes, and Efficient Data Sharing.

The RIDG Working Group is preparing for the Q3 RIDG meeting, which will be in July; the exact date is still to be determined. The meeting will focus on clarifying participants' understanding of the Census Differential Privacy Standards, and will include expert presentations and facilitated breakout sessions.

The Working Group is developing a six-month plan to transfer leadership of RIDG to the participants (with continued support from MORPC staff). The goal is to have a small group of volunteer representatives form a Steering Committee, with a staged plan for transferring complete oversight of the group to the Steering Committee by early 2021.

Sustainability Dashboard
The Working Group was on track to release the Dashboard in Spring 2020, but the COVID-19 crisis slowed progress. Adam Porr and his team at OSU CURA are working tirelessly on the project, continuing to add enhancements to the tool. Invitations for the second round of user testing will be sent very soon; RDAC members among others will receive that invitation. The Working Group hopes to have the Dashboard ready for public release in Late Summer/Early Fall 2020.

Data Policy Needs Survey & Toolkit
The Working Group's progress is going well. The survey development was slowed down a bit due to COVID-19, but most of the slowing has been to refine the survey questions. Working Group members are taking time to tailor the survey to many different municipalities and jurisdictions.

Regional Municipal Fiber Strategy
The Working Group was again slowed due to COVID-19. Members are focusing on defining a Minimum Viable Product (MVP) for the network. The Working Group will meet again on June 16 to continue moving forward with the design of the MVP. Members are also in the process of creating a Non-Disclosure Agreement about fiber assets.

Central Ohio GIS User Group (COGUG)
COGUG met on May 20, with 47 attendees. ESRI staff gave a presentation regarding new hub templates. The meeting featured six breakout sessions, facilitated by MORPC, Dublin, Westerville and Marysville staff.

Adjourned at 2:33 pm.

Mid-Ohio Regional Planning Commission
111 Liberty Street
Columbus, Ohio 43215

Regional Data Advisory Committee
Meeting Notes

March 3, 2020, 1:00 pm

Members Present

Charlie Burks, Columbus Metropolitan Library
Chair Brad Ebersole, Consolidated Electric Cooperative, Inc.
Shoreh Elhami, City of Columbus
Vice Chair Jung Kim, One Columbus
Tom Kneeland
Jonathan Miller, Delaware County Regional Planning Commission
Gene Oliver, City of Worthington
Theresa Seagraves, Franklin County Public Health

Members Calling In

Rick Stein, Urban Decision Group

Public Present:

Christian Selch, City of Columbus

MORPC Staff Present

Joe Garrity
Natalie Hurst
Lynn Kaufman
Cheri Mansperger
William Murdock
Aaron Schill
Brandi Whetstone

Meeting Called to Order at 1:05 pm.

Welcome & Committee Administration

Members and staff introduced themselves.

2020 Census Update

MORPC staff has developed a one-page fact sheet specifically for local governments and targeted toward elected officials and local leaders. The document is intended to give those leaders basic information for frequently asked questions from the public. It explains how the census data will be used.

Census Timeline:

February & March 2020	Invitations to participate are distributed.
April 1, 2020	Census Day is observed nationwide. By this date, every home will have received an invitation to participate in the 2020 Census.
May - Summer 2020	The Census Bureau will follow up with those who have not responded.
December 2020	Apportionment counts are delivered to the President and Congress.
March 31, 2021	State and local redistricting data is released.

MORPC Staff Updates

Regional Housing Strategy

Work on the Regional Housing Strategy began in summer 2019. Housing affordability and supply has been an ongoing issue for communities throughout the region. MORPC is partnering with the public sector, the private sector and the social sector to research the current and anticipated needs for housing in the region. Through data collection and analysis, staff and consultants will explore affordability issues and how to address them. Staff is currently reviewing recommendations and investment/policy strategies for the region and will tailor those recommendations to particular community types. There will be Local Housing Action Plans created so that each community can customize the Action Plan for their own community and their own purposes, to address the housing needs of their communities.

MORPC staff is working with Enterprise Community Partners, a large national nonprofit organization that works in both housing development and housing consulting.

Scope of Work

- Equip the region with a unified vision for housing investments
- Expand the regional housing toolbox
- Provide a strategic roadmap with measurable actions
- Consider housing as a platform for access to opportunity and equity
- Implement community, partner, and stakeholder support

The goal is to complete the recommendations process and publicly release the Action Plans in May 2020.

MORPC Data & Mapping staff is seeking input on how data products will be organized and presented. The hope is to publish the work as a large digital resource that is well organized and comprehensive, so that other agencies or partners can either access the data directly, or review the findings and the summary outputs of what has been learned. RDAC members were asked to forward suggestions about the data presentation to Aaron Schill within the next few weeks.

Central Ohio Growth and Development

The methodology for the population projections will come out soon as part of the Metropolitan Transportation Plan.

MORPC staff has identified a need to develop a clear, overarching narrative about regional growth. The insight2050 work over the last few years has shown what growth means to the development of the region and how the Regional Housing Strategy will be created. One key talking point is that the region will have a population of 3,000,000 by 2050. Household growth is also important for its impact on housing to support and meet future demand. Particularly relevant right now is the older adult population, because for the next 10 or 15 years that group will going to be growing at a faster rate than others.

The narrative related to this growth is very important because as economic development drives business, the business owners need to where people will live. This need circles back into the Regional Housing Strategy's affordable housing component.

Working Group Reports

Regional Information & Data Group (RIDG)

The first RIDG User Group meeting was held on January 29, with 40 people attending. The users discussed the 2020 Census and participated in networking, team building, and small group activities. The goal was to determine what users want from the group, what tools they are using, and any specific topics to discuss at the Quarter 2 2020 meeting. The RIDG Working Group is in the process of compiling the information gathered at the January meeting.

Sustainability Dashboard

The data to be used in the Dashboard is being vetted. The first round of beta testing is complete, with CURA working on revising the program. The next step for the Working Group is the second-round user testing. RDAC members will be asked to participate in the second-round user testing.

Data Policy Needs Survey & Toolkit

The survey is in the editing phase, and the Working Group is refining the list of proposed respondents. The plan is to hold at least two focus groups in the near future, consisting of those proposed respondents.

Regional Municipal Fiber Strategy

Regional Intergovernmental Private Network

Members are working to create a design for the network, investigating what fiber could be used for that, where to put nodes, different access methods, and different support models. Part of this work is to explore the cost of the contribution and consumer models would be, as not all network users will have the same resources to contribute.

Fiber Mapping and Clearinghouse

The Working Group will gather information from the organizations participating in the design of the network to create standards for that clearinghouse. This will make data more accessible for the longer-term goal of having a regional view of economic development access with respect to fiber.

The Working Group will be careful about not threatening the private sector, focusing on government, governmental entities and how they can share and benefit from these projects.

Central Ohio GIS User Group (COGUG)

COGUG met on February 12, with a group discussion regarding ESRI Cloud led by City of Dublin GIS staff, networking activities, and small group discussions.

Communications Strategy for RDAC Working Group Projects

If Working Group Chairs want a different type of communication other than the current of report-outs at quarterly RDAC meetings, please contact MORPC staff.

Other Business – Upcoming events:

MORPC State of the Region – April 30
The Council for Community and Economic Research Annual Conference – June 1-5
Women in Analytics Conference – June 3-5
ICF Global Summit – June 16-18

Adjourned at 2:37 pm.

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.

REGIONAL INFORMATION & DATA GROUP

Status Update – RDAC June 2, 2020

MID-OHIO REGIONAL
MORPC
PLANNING COMMISSION

REGIONAL INFORMATION & DATA GROUP

MORPC

4/22

HELD SECOND RIDG MEETING (VIRTUAL)

2020 Census Update

Sustainability Dashboard Update / Beta Testing Invitation

COVID-19 Data Presentations from:

- Ohio Development Services Agency
- Regionomics
- Scioto Analysis
- MORPC

REGIONAL INFORMATION & DATA GROUP

32

PARTICIPANTS

Participants from **public, private, and non-profit** sectors

Signs of **cross-pollination** of data work

REGIONAL INFORMATION & DATA GROUP

MORPC

5

BREAKOUT SESSIONS

Topics about or stemming from COVID-19 were developed in response to the concerns of the moment:

- Long term impacts of COVID-19
- Remote work
- Lessons on data governance in a crisis
- Metadata woes
- Efficient data sharing

REGIONAL INFORMATION & DATA GROUP

JULY TBD

THIRD MEETING PLANNED (VIRTUAL)

Meeting will focus on the **Census differential privacy standards**, in response to conversations from members of the group

NEXT STEPS

Develop a clear **communication and engagement** plan

Develop transition plan to transfer RIDG oversight to a **participant-led steering committee** in early 2021