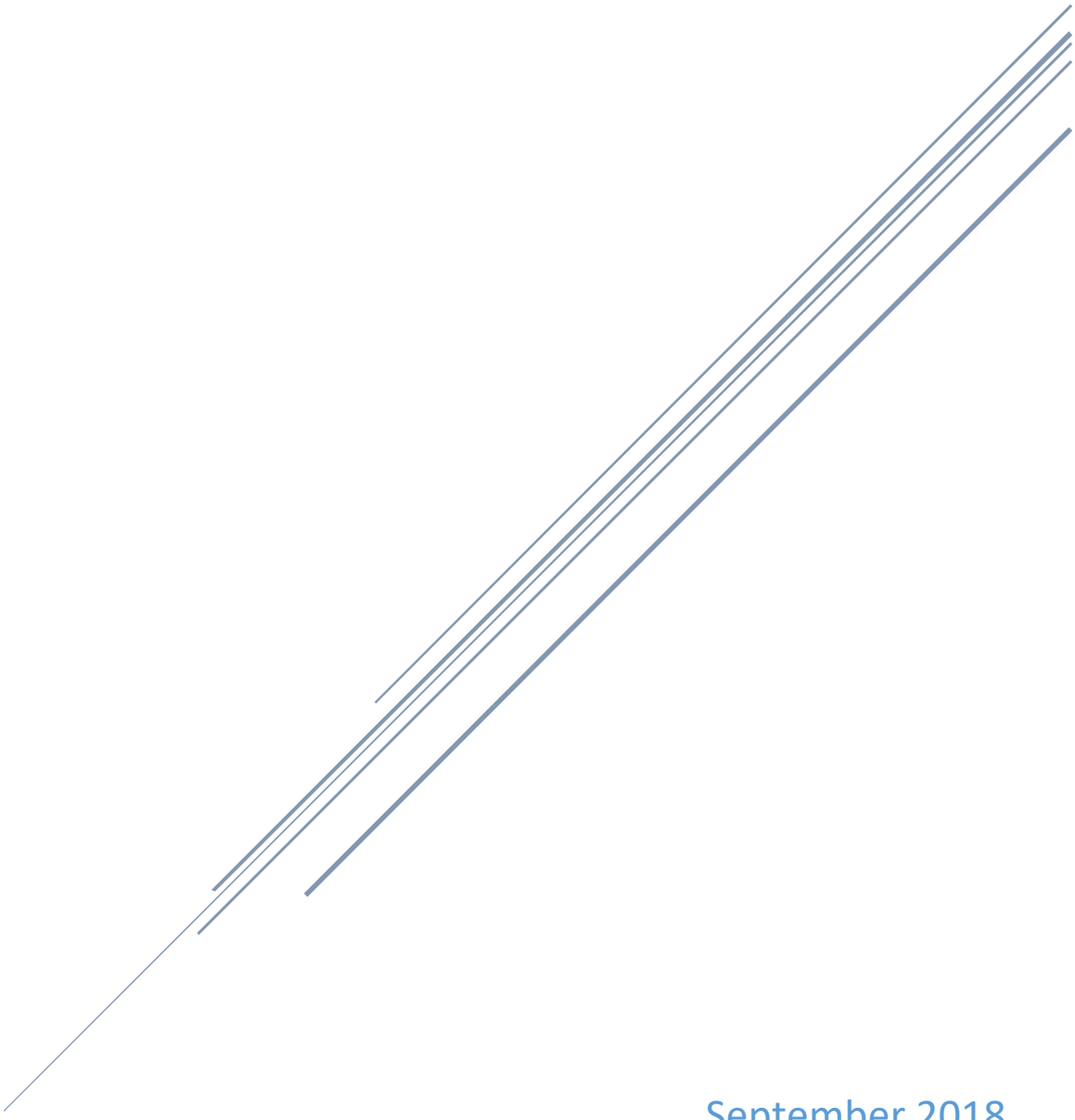
CYBER SHARING WORKING GROUP STRATEGIC PLAN

Chair: Dewand Neely | Co-Chair: Ron Pelletier



September 2018
Indiana Executive Council on Cybersecurity

Cyber Sharing Working Group Plan

Contents

Committee Members

Committee Members

Name	Organization	Working Group Positon	IECC Membership Type
Dewand Neely	Indiana Office of Technology	Chair	Voting
Tad Stahl	Indiana Office of Technology	Chair Proxy	Advisory
Ronald W.Pelletier	Pondurance	Co-Chair	Voting
Nick Sturgeon	CLA	Co-Chair Proxy	Advisory
Paul Baltzell	IEDC	Full time	Advisory
Franco Cappa	Purdue University	As needed	Advisory
Chris Carter	Indiana State Police	As needed	Advisory
Paul Dvorak	Secret Service	As needed	Non-Voting
Greg Hedrick	Purdue University	Full time	Voting
Owen LaChat	MutualBank	As needed	Voting
Benjamin Marrero	Ivy Tech	Full time	Advisory
Kim Milford	Indiana University	Full time	Advisory
Nicole Needham	Indiana Office of Technology	Full time	Advisory
Mitchell Parker	IU Health	As needed	Advisory
Stan Partlow	American Electric Power	As needed	Advisory
Chad Pollitt	Indiana University	Full time	Advisory
Joel Rasmus	Purdue University (CERIAS)	As needed	Advisory
Bryan Sacks	Indiana Office of Technology	As needed	Advisory
Michael Servas	MutualBank	As needed	Advisory
Dave (LT)Skalon	Indiana National Guard	As needed	Advisory
Darryl Togashi	Ivy Tech	As needed	Advisory
William Tucek	Navient	As needed	Advisory
Andrew VanZee	Indiana Hospital Association	As needed	Advisory
Brian Vitale	Notre Dame Federal Credit Union	Full time	Advisory

Introduction

Introduction

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) and its mission was continued. With the ever-growing threat of cyberattacks, the IECC has been tasked with developing and maintaining a strategic framework to establish goals, plans, and best practices for cybersecurity to protect Indiana's critical infrastructure. The IECC is comprised of twenty committees and working groups who worked together to develop a comprehensive strategic plan and implementation plans. This implementation plan is one of the twenty specific plans that make up the complete 2018 Indiana Cybersecurity Strategic Plan.

Executive Summary

Executive Summary

- **Research Conducted**
  - State cybersecurity plans
  - Magazine articles on state cyber sharing articles
  - Team member familiarity with resources
  - Applied experience by team members for their own operations, experience and networks with other organizations

- **Research Findings**
  - An inventory of cyber sharing resources of various sources
  - Articles depicting the various strategies used by state governments
  - Communication types produced by the Multi-State Information Sharing and Analysis Center (MS-ISAC) (a similar model for states that Indiana might learn from for counties)

- **Working Group Deliverables**
  - Best Practices
  - Cyber Sharing Maturity Model
  - Inventory of Cyber Sharing Resources
  - MS-ISAC Member Recruitment
  - Secured Information Sharing Program

Additional Notes
  - N/A

References
  - State cybersecurity plans (multiple)
  - Pew article - http://pellcenter.org/wp-content/uploads/2017/02/State-of-the-States-Report.pdf
  - ISC2 survey on cybersecurity from a Federal Executive perspective - https://www.isc2.org/-/media/ISC2/Documents/ISC2-Federal-Cyber-Survey-Report.ashx?la=en&hash=7AFB8F6E0A67C2D417D7031E17DF9E481DB21E20

Research

Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
    a. Over the last five years and before, there has been an emerging number of excellent cyber sharing resources. The process of finding information can be initially difficult and somethings the need and/or value of information is not recognized. If the need and/or desire for cyber information exists, the vast majority of it is available by searching websites and news articles.
    b. The numerous sources of information take various approaches to distributing material to their audiences. There are corporate sources providing the information as their primary product, there are technical sources providing cyber information as a value in the form of enhanced support to their customers, Information Sharing and Analysis Centers (ISAC) serving particular business sectors against common threats, and Fusion Centers sharing information to Federal sources and local law enforcement.

2. **What (or who) are the most significant cyber vulnerabilities in your area?**
    a. Filtering valuable information from the mountain of content available. The amount of information can be overwhelming and much of it is of no value to an organization. Identifying sources that provide pertinent information to a business function in an efficient manner is more difficult.
    b. Organization of cybersecurity maturity. Many agencies have not reached a maturity level with cybersecurity, or are not staffed to needed levels, to recognize and define the cyber information needed.

3. **What is your area's greatest cybersecurity need and/or gap?**
    a. To identify common needs that can be filled through economies of scale and facilitated by the Council.
    b. An understanding of where various entities in Indiana, public and private, are underserved and why they are underserved.

4. **What federal, state, or local cyber regulations is your area beholden to currently?**
    a. A number of state entities fall under federal regulations (Internal Revenue Service (IRS), Health Insurance Portability and Accountability Act (HIPAA), Social Security Administration (SSA)). State law also directs Indiana citizens on appropriate behavior and incident response requirements.

5. **What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?**
    a. Most states find themselves in a similar position as we do. Fusion Centers seem to be the most common form of information distribution, but are limited in audience and very specific with its content. ISACs, Information Sharing & Analysis Organizations (ISAO), and state-sponsored cyber sharing organizations are growing as vehicles to share to broader audiences.

6. **What research is out there to validate your group's preliminary deliverables? This could be Surveys, whitepapers, articles, books, etc.**
    a. A number of state cybersecurity plans were reviewed. Each state seems to have a slightly different focus or approach, but also a lot of commonalities. This document from Pell discusses seven states' information sharing (among other aspects of their cybersecurity efforts). http://pellcenter.org/wp-content/uploads/2017/02/State-of-the-States-Report.pdf

7. **What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?**
    a. Most states and organizations look internally. Some states try to leverage their state, local, tribal and territorial (SLTT) relationships. ISACs and Fusion Centers work to develop economies of scales. For the most part, cybersecurity training and preparedness is left to individual organizations.

8. **What does success look like for your area in one year, three years, and five years?**
    a. Success will be identifying the information available and matching it with the information needed, adding any needed value that exists, and facilitating the exchange of information between all organizations. This could be in the form of digital information, presentations, training, etc. Digital information would be the general content, threat information, advisories, vulnerabilities, etc. that entities should be aware of.
    b. Success will be finding ways of advancing cybersecurity maturity for individual SLTT units. Often one at a time or in small groups sharing similar challenges. The difficulty is having current and useful resources/services that will be able to help with these challenges in a timely manner.

9. **What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?**
    a. This will take some investigation. There could be opportunities for general cyber information to broad audiences/communications or specific information/communications for narrower audiences. There are other opportunities to make current communications, resources, and forums known to more audiences that could benefit from the information that already exists.

10. **What is the total workforce in your area in Indiana? How much of that workforce is cybersecurity related? How much of that cybersecurity-related workforce is not met?**
    a. Unknown.

11. **What do we need to do to attract cyber companies to Indiana?**
    a. A vibrant and energetic cyber community, complete with sharing opportunities and effective communications, would be an attractive and prominent bullet point in attracting new opportunities.

12. What are your communication protocols in a cyber emergency?

a. The communication protocols vary with each communications channel. The State of Indiana communicates issues of concern with the MS-ISAC and other parties as needed. The Indiana Intelligence Fusion Center (IIFC) communicates with federal and local sources. The Indiana Information Sharing and Analysis Center (IN-ISAC) works with organizations, to include elections, state agencies, K-12, on an ad hoc basis as well as publishing a weekly security brief for the Executive Branch and a monthly newsletter for the general public.

13. What best practices should be used across the sectors in Indiana? Please collect and document.

a. The goal of the Cyber Sharing Working Group is to determine what are the best practices that should be used across the sectors of Indiana. There is a number of good information gathering organizations that effectively communicate with their constituencies. Some organizations are underserved which provides an opportunity to deliver solutions of real value.

Deliverable: Best Practices

Deliverable: Best Practices

General Information

1. **What is the deliverable?**
    a. A list of cyber sharing best practices

2. **What is the status of this deliverable?**
    a. In progress; 75% Complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
    ☒ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☐ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☒ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Provide a recommendation of best practices for information sharing in the state. This will also provide a common set of terms that will make it easier to communicate effectively.

6. **What metric or measurement will be used to define success?**
    a. The adoption of the standards and best practices throughout the State of Indiana.

7. **What year will the deliverable be completed?**
    a. 2019

8. **Who or what entities will benefit from the deliverable?**
    a. The Public and Private Sectors

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. Not applicable.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Not applicable.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Not applicable.

12. **Who should be main lead of this deliverable?**
    a. Cyber Sharing Working Group

13. **What are the expected challenges to completing this deliverable?**
    a. None

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Develop List	Nick Sturgeon	100%	March 2018	
Review with the Cyber Sharing Working Group	Cyber Sharing Working Group	100%	May 2018	
Present update on the deliverable	IECC	100%	April 27, 2018	
Determine the home for the list and review with the working group	Cybersecurity Program Director and Cyber Sharing Working Group	100%	August 2018	
Finalize list	Cyber Sharing Working Group	50%	January 2019	
Publish the list and move to a maintenance mode	Cyber Sharing Working Group	0%	January 2019	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
0					

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
N/A						

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. It will help businesses and citizens by creating and centralizing a list of best cybersecurity practices.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. This will help increase knowledge of cybersecurity best practices to Indiana businesses and citizens. No real cost associated with this deliverable. With the adoption of these best practices, businesses and citizens will reduce the overall cybersecurity risk profile of the entire state.

19. What is the risk or cost of not completing this deliverable?

a. No risk, will only cost time to make the updates to the Indiana Cybersecurity website.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Initial metrics will be based around unique website visits and total site visits. Additional metrics will be around capturing data to see if these best practices are being implemented.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. No

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. Yes
b. **If Yes, please list states/jurisdictions**
    i. [No Response]

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. None as of now.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. N/A

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. The only people contacted to this point are those within the Cyber Sharing Working Group.

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
    i. All

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. Sector partners, local government, state agencies, businesses and their associations, the general public

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. None as of now.

Evaluation Methodology

Objective 1: IECC Cyber Sharing Working Group will create a list of best practices by January 2019.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Cyber Sharing Maturity Model

Deliverable: Cyber Sharing Maturity Model

General Information

1. **What is the deliverable?**
    a. Cyber Sharing Maturity Model

2. **What is the status of this deliverable?**
    a. In progress; 50% complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☒ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☒ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Creation of a maturity model that businesses and governments can self-assess and use links/info provided to increase their cyber maturity.

6. **What metric or measurement will be used to define success?**
    a. Completion of product, sample feedback from a variety of stakeholders, and a number of downloads of the model from the cyber hub.

7. **What year will the deliverable be completed?**
    a. 2019

8. **Who or what entities will benefit from the deliverable?**
    a. Businesses and government

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. N/A

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Strategic Resources Working Group and the voting members of the IECC.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. N/A

12. **Who should be main lead of this deliverable?**
    a. Cyber Sharing Working Group

13. **What are the expected challenges to completing this deliverable?**
    a. Measuring of the success of the model and keeping the model simple enough for all to use.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. One-time deliverable

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Draft up model	Cybersecurity Program Director	100%	March 2018	
Review and develop model	Cyber Sharing Working Group, Strategic Resources Working Group, Indiana University Team	100%	April 2018	
Present model for feedback from Council	IECC	100%	April 27, 2018	
Make edits and design	Cybersecurity Program Director and Cyber Sharing Working Group	50%	January 2019	
Finalize Model	Cyber Sharing Working Group	0%	February 2019	
Incorporate model into IECC PR and Communications Plan	Public Awareness and Training Working Group	0%	March 2019	
Distribute to stakeholders	IECC and partners	0%	June 2019	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
N/A					

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
N/A						

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. The Cyber Sharing Maturity Model will provide all those who use it, especially local government, K-12 schools, and small businesses with a starting point to begin understanding the many resources around cyber threat sharing and education.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. By further educating those who would like to increase their cybersecurity levels, it will help reduce their cybersecurity risks and impact because they may be better prepared for a cyber event.

19. What is the risk or cost of not completing this deliverable?

a. As of now, many are confused by the many choices with cyber sharing and threat resources. Because it can be overwhelming, many do not move their cybersecurity level.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. The completion of the model will be one output measure of success. This model is to be used by local governments, businesses, and educators in Indiana and them finding value in it will be another measure of success.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. No

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. Yes
b. **If Yes, please list states/jurisdictions**
    i. While there are many states that have cyber sharing resource pages, we were not able to find a similar maturing model

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. None as of now.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. N/A

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. Indiana University who provided the idea of a cyber sharing maturity model and are partners of this deliverable.

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
    i. All

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. Sector partners, local government, state agencies, businesses and their associations, general public

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. None as of now.

Evaluation Methodology

Objective 1: IECC will develop Indiana's first cyber sharing maturity model by February 2019.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: IECC will distribute Indiana's first cyber sharing maturity model to critical infrastructures through ninety percent of Indiana associations by June 2019.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☒ Quantifiable Measurement
☐ Other

Deliverable: Inventory of Cyber Sharing Resources

Deliverable: Inventory of Cyber Sharing Resources

General Information

1. **What is the deliverable?**
    a. An inventory of resources assembled by the Cyber Sharing Working Group.

2. **What is the status of this deliverable?**
    a. 100% Complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☐ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☒ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☒ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. The inventory serves as a resource for those needing trusted and vetted cyber information.

6. **What metric or measurement will be used to define success?**
    a. We envision this being static content on an IECC web page. One metric is the number of hits, though this will not likely drive huge web traffic. It could be of exceptional value to those needing information, especially those just ramping up their security programs.

7. **What year will the deliverable be completed?**
    a. 2018

8. **Who or what entities will benefit from the deliverable?**
    a. Business, government and possibly citizens.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. There is likely some overlap, but the accumulation of the inventory was straightforward. Keeping the list current will require little maintenance and any overlap would be inconsequential.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. This work is complete.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Not applicable.

12. **Who should be main lead of this deliverable?**
    a. Cyber Sharing Working Group

13. **What are the expected challenges to completing this deliverable?**
    a. Reaching the potential audiences effectively. Having the ability to share the value of the products.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
List developed	Cybersecurity Program Director	100%	November 2017	Ongoing only in that additional resources can be added
Review and develop model	Cyber Sharing Working Group	100%	November 2017	
Present model for feedback from Council	IECC	100%	December 2017	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
N/A					

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
N/A						

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. It is part of a library of resources that could be used by those needing cybersecurity guidance.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. Provides information resources that will assist those needing cyber information.

19. What is the risk or cost of not completing this deliverable?

a. No risk, but a resource that could be very valuable.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. The list could be very valuable to those that visit the library of resources. It will be hard to measure the value of coming to a trusted source and viewing the information. You could measure web hits on the document, but the value from any visit will be hard to measure.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. No

b. **If Yes, please list states/jurisdictions**

i. A number of states have lists of resources. Michigan is one example, but there are other examples as well. The types of resources in their libraries vary.

22. **Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?**
    a. Yes
    b. **If Yes, please list states/jurisdictions**
        i. There are many states that do not have a list of resources such as this. Cybersecurity and outreach from states to citizens, businesses, etc. are widely varied in both content and delivery mechanisms.

Other Implementation Factors

---

23. **List factors that may negatively impact the resources, timeline, or budget of this deliverable**?
    a. None.

24. **Does this deliverable require a change from a regulatory/policy standpoint?**
    a. No

25. **What will it take to support this deliverable if it requires ongoing sustainability?**
    a. N/A

26. **Who has the committee/working group contacted regarding implementing this deliverable?**
    a. IN-ISAC, Indiana Office of Technology (IOT)

27. **Can this deliverable be used by other sectors?**
    a. Yes
    b. **If Yes, please list sectors**
        i. All

28. **Once completed, which stakeholders need to be informed about the deliverable?**
    a. Sector partners, local government, state agencies, businesses, and their associations, as well as the general public

29. **Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?**
    a. Yes

30. **What are other public relations and/or marketing considerations to be noted?**
    a. None as of now.

Evaluation Methodology

Objective 1: IECC Cyber Sharing Working Group will complete an inventory of cyber sharing resources by August 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☒ Quantifiable Measurement
☐ Other

Deliverable: MS-ISAC Member Recruitment

Deliverable: MS-ISAC Member Recruitment

General Information

1. **What is the deliverable?**
    a. MS-ISAC is a resource delivering a broad range of information to the State of Indiana. This includes vulnerability notifications, threat notifications, and other information including a monthly conference call. The Cyber Sharing group, through the efforts of the IN-ISAC, plans to push enrollment in the MS-ISAC. Education and Local government working groups may be able to assist with this deliverable.

2. **What is the status of this deliverable?**
    a. In-progress; 50% complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☐ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☒ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☒ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Better cybersecurity information to a broad range of schools and local governments that are underserved.

6. **What metric or measurement will be used to define success**?
    a. Number of Indiana SLTT and K-12 schools signed up for the MS-ISAC.

7. **What year will the deliverable be completed?**
    a. 2019

8. **Who or what entities will benefit from the deliverable?**
    a. SLTT and K-12 organizations signing up for the information.

9. **Which state or federal resources or programs overlap with this deliverable**?
    a. MS-ISAC produces quality information in a variety of formats. This information is valuable and vetted.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Getting the word out to SLTT and K-12 would be very helpful.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Those that can help with the drive to get SLTT and K-12 organizations to join MS-ISAC.

12. **Who should be main lead of this deliverable?**
    a. Tad Stahl

13. **What are the expected challenges to completing this deliverable?**
    a. Reaching the potential audiences effectively and having the ability to share the value of the products.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Develop Outreach plan	IN-ISAC Manager	100%	2018	
Implement plan and tactics	IN-ISAC Manager	25%	June 2019	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
N/A					

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
[No Response]						

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. Getting good, current and vetted cyber threat, advisory, and awareness materials to those subscribed on a regular basis.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. Through better information to those involved in the daily security operations of an organization.

19. What is the risk or cost of not completing this deliverable?

a. There are many state institutions that could benefit from the federally funded service. This service is also free to SLTT and schools. Any costs for MS-ISAC would go unrealized.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Difficult to gauge the value from participants. It can be measured in the increased numbers using MS-ISAC.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. Yes
b. **If Yes, please list states/jurisdictions**
    i. All states subscribed to the MS-ISAC newsletter.

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. None as of now.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. N/A

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. IN-ISAC

27. Can this deliverable be used by other sectors?

a. Yes

b. **If Yes, please list sectors**

i. Locals and Schools

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. SLTT and schools.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. None as of now.

Evaluation Methodology

Objective 1: Increase Indiana MS-ISAC membership by twenty-five percent by June 2019.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☒ Quantifiable Measurement
☐ Other

Deliverable: Secured Information Sharing Program

Deliverable: Secured Information Sharing Program

General Information

1. **What is the deliverable?**
    a. Secured Information Sharing Program

2. **What is the status of this deliverable?**
    a. In-progress; 75%

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
    ☐ Establish an effective governing structure and strategic direction.
    ☒ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☐ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☒ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Provide a secure and trusted statewide information sharing platform.

6. **What metric or measurement will be used to define success?**
    a. Participation in the program by the private sector.

7. **What year will the deliverable be completed?**
    a. 2019

8. **Who or what entities will benefit from the deliverable?**
    a. Public and private sector

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. U.S. Department of Homeland Security's (US-DHS) Cyber Information Security Collaboration Program (CISCP), Enhanced Security Services (ECS) and Automate Indicator Sharing (AIS), MS-ISAC, and IN-ISAC.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Strategic Resource Working Group, Pre- thru Post- Incident Working Group

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. US-DHS, Indiana Department of Homeland Security (IDHS), IIFC, IN-ISAC, and Indiana State Police (ISP).

12. **Who should be main lead of this deliverable?**
    a. Cyber Sharing Working Group.

13. **What are the expected challenges to completing this deliverable?**
    a. The vetting process through US-DHS, participation from the private sector.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Develop Draft	Nick Sturgeon	100%	March 2018	
Review with the Cyber Sharing Working Group	Cyber Sharing Working Group, Strategic Resources Working Group, Indiana University Team	100%	March 2018	
Present program for feedback from Council	IECC	100%	April 2018	
Make edits to the program	Cybersecurity Program Director and Cyber Sharing Working Group	50%	March 2019	
Meet with ISP, IIFC, IDHS and US-DHS	Public Sector Working Group.	0	May 2019	
Make final edits and conduct the final review with the Cyber Sharing Working Group	Cyber Sharing Working Group	0	July 2019	
Deliver final product	Cyber Sharing Working Group	0	August 2019	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
TBD	TBD	TBD	TBD	TBD	More conversation needs to be had on determining the work effort to manage and maintain this program

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
TBD	TBD	TBD	TDB	TBD	TBD	More conversation needs to be had on determining the work effort to manage and maintain this program. There is the potential for needing IT infrastructure for this program.

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. With the State of Indiana providing a secured cyber threat information sharing service for companies that want to share with the Federal Government. The State and the companies involved will be in a position to gain a clearer common operating picture. Another benefit for those involved is that these programs provide some limited liability protections.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. This would also provide incentive for private sector businesses to share information with both the State and Federal Governments without fear of liability repercussions.

19. What is the risk or cost of not completing this deliverable?

a. There are potential liability risks at the state level with private sector and public sector sharing information. There are risks of the Cybersecurity Information Sharing Act (CISA) if information is not shared according to the guidelines needed to meet the liability protections laid out by CISA.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Initial metrics will be based on the number of private sector entities participating in the program and the level of their participation.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. Yes
b. **If Yes, please list states/jurisdictions**
    i. This program will incorporate programs offered by the US-DHS.

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No
b. **If Yes, please list states/jurisdictions**
    i. We are unaware of any other state jurisdiction that has this exact program. There are states that have different sharing capabilities and maturity levels.

Other Implementation Factors

---

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. The biggest factor that would negatively impact this program will be the lack of acceptance and participation by the private sector and the buy-in from ISP, IIFC, US-DHS and IDHS. There could be kick-back from programs like InfraGard

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. Yes
b. **If Yes, what is the change and what could be the fiscal impact if the change is made?**
    i. There may need to be changes to state law similar to the protections from Freedom of Information Act (FOIA) request that Michigan, House Bill 4973, signed into law in March 2018.

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. This program will require support from the ISP, IIFC, IDHS, US-DHS and private sector.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. No one at this time.

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
    i. All

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. Sector partners, local government, state agencies, businesses and their associations, general public

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. None as of now.

Evaluation Methodology

Objective 1: IECC Cyber Sharing Working Group will develop a Secured Information Sharing Program by July 2019.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: IECC Cyber Sharing Working Group will launch a Security Information Sharing Program by August 2019.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Supporting Documentation

Supporting Documentation

This section contains all of the associated documents that are referenced in this strategic plan and can be used for reference, clarification, and implementation details.

- IECC Cyber Sharing Working Group Inventory of Information Resources

IECC Cyber Sharing Working Group

Inventory of Information Resources

August 2018

GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

Inventory of Information Resources

Type of Information	Source	Interval	Audience	Notes	URL
On-line webinars	MS-ISAC	Frequent, regular	All members		https://www.cisecurity.org/ms-isac/
Monthly newsletter	MS-ISAC	Monthly	All members		https://www.cisecurity.org/ms-isac/
Advisories -UFOUO	MS-ISAC	Frequent, regular	All members	Distributes from multiple sources (DHS, FBI)	https://www.cisecurity.org/ms-isac/
SOC advisories	MS-ISAC	Frequent, regular	State of IN	We are a customer, data could be scrubbed and shared	https://www.cisecurity.org/ms-isac/
Election Communications	MS-ISAC	Frequent, regular	Sec of State	Multiple comms type, election specific	https://www.cisecurity.org/ms-isac/
News	SANS	Weekly	Subscribers	Informational	https://www.sans.org/
Advisories -UFOUO	DHS	Frequent, regular	All states		https://www.dhs.gov/
Advisories	DHS	Infrequent	All states		https://www.dhs.gov/
Advisories	FBI (IC-3)	Infrequent	All states		https://www.fbi.gov/
Advisories	McAfee	Frequent, regular	Customers	Tend to focus on McAfee products, occasional acute threats	https://www.mcafee.com/en-us/index.html
	Shadowserver.org				https://www.shadowserver.org/wiki/
	FS-ISAC				https://www.fsisac.com/
	REN-ISAC				https://www.ren-isac.net/
	Open DNS				https://www.opendns.com/
	NH-ISAC				https://nhisac.org/
Advisories	FinCEN (Financial Crimes Enforement Network)				https://www.fincen.gov/
	FBI InfraGard		Members	Similar to FS-ISAC Alerts	https://www.infragard.org/
	US-CERT		Subscribers	General - Across all sectors / industries	https://www.us-cert.gov/
	Secret Service		Subscribers	General - Across all sectors / industries	https://www.secretservice.gov/
	Consumer Financial Protection Bureau		Subscribers	Bank / Non-Bank focused	https://www.consumerfinance.gov/
	Office of Comptroller of Currency		Subscribers	Bank / Non-Bank focused	https://www.occ.treas.gov/
	Federal Reserve Bank		Subscribers	Bank focused	https://www.federalreserve.gov/
	Federal Deposit Insurance Corporation		Subscribers	Bank focused	https://www.fdic.gov/
	National Credit Union Administration		Subscribers	Credit Union focused	https://www.ncua.gov/Pages/default.aspx
	Federal Financial Institutions Examination Council		Subscribers	Bank / Credit Union focused	https://www.ffiec.gov/
	Krebs-on-Security (Blog)		Subscribers	General - Across all sectors / industries	https://krebsonsecurity.com/
	National Association of Federally-Insured Credit Unions		Subscribers	Credit Union focused	https://www.nafcu.org/
	Indiana Credit Union League		Subscribers	Credit Union focused	https://www.icul.org/Pages/default.aspx
	Credit Union National Association		Subscribers	Credit Union focused	https://www.cuna.org/