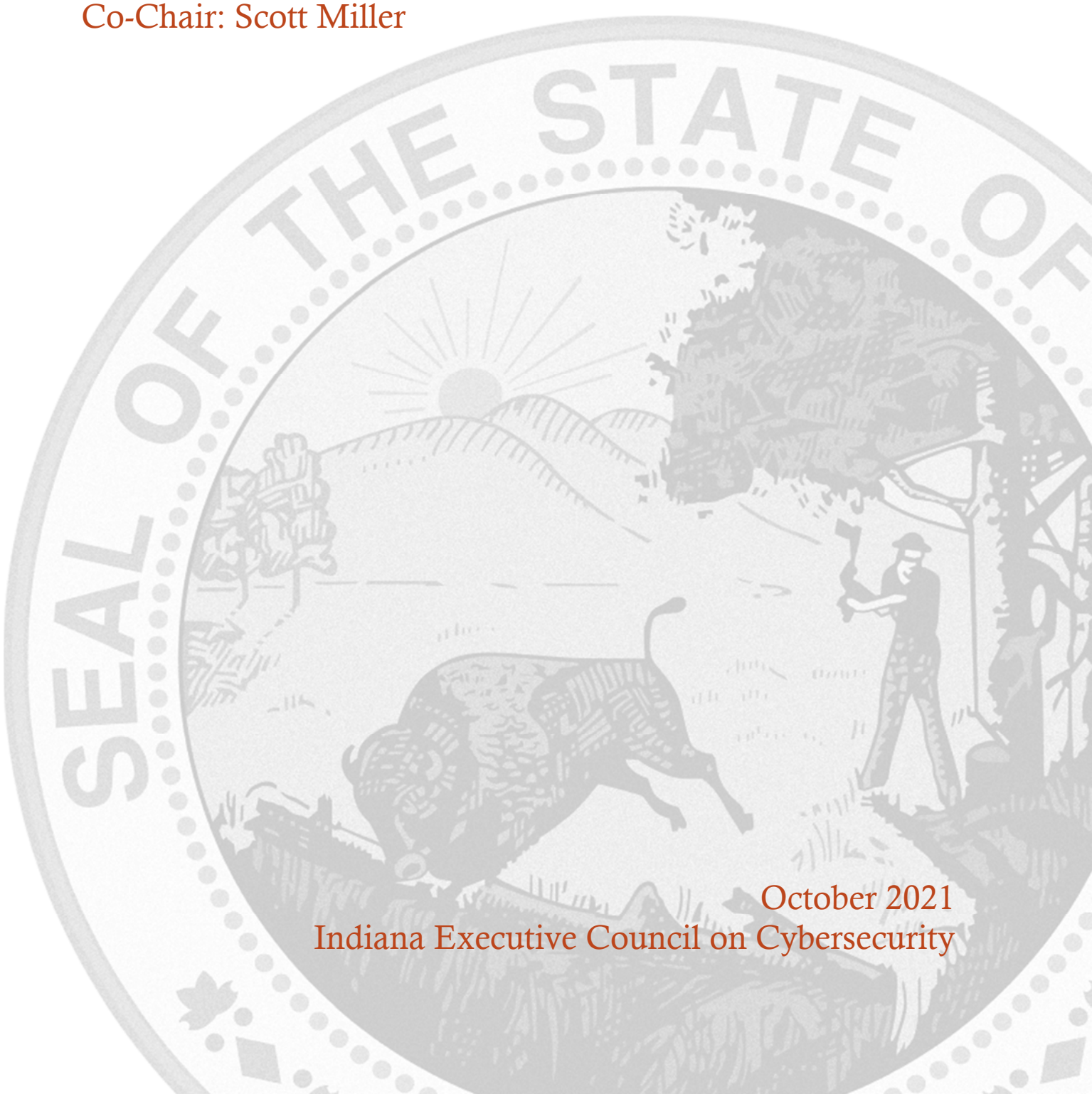
STRATEGIC RESOURCE WORKING GROUP STRATEGIC PLAN

Chair: Chetrice Mosley-Romero
Co-Chair: Scott Miller



October 2021
Indiana Executive Council on Cybersecurity

Strategic Resource Working Group Plan

Table of Contents

Committee Members

Committee Members

Last Name	First Name	Organization	Title	Member Type (Chair/Co-chair/Full-time, As needed)
Ayers	David	Indiana Office of Technology	Program Communications Manager	Chair Proxy
Banta	Rich	Lifeline Datacenters	Principal & Chief Information Security Officer	Full Time
Beard	Amy	Indiana Department of Insurance	Commissioner	As Needed
Best	Gerald	Astro Logistic Solutions	Managing Director	As Needed
Creech	Bill	Cadre Information Security	Enterprise Sales Manager	As Needed
Cudby	Joe	MXL Consulting	Chief Executive Officer/Principal	Full Time
Dietz	J. Eric	Purdue University	Professor-Computer and Information Technology	As Needed
Dittmer	Robert	Government Performance Solutions, LLC	Senior Consultant	Full Time
Goldsmith	Reid	Indianapolis International Airport	Senior Director Information Technology	Full Time
Guarente	Tom	DeepInstinct	Americas Vice President	Full Time
Huston	Jim	Indiana Utility Regulatory Commission	Commissioner	As Needed
Hyer	Sam	Indiana Governor's Office	Senior Operations Director	As Needed

LaChat	Owen	Northwest	VP,Technology Infrastructure and Security Management	As Needed
Langelier	Mike	TechPoint	President	As Needed
Lewis	Landon	Pondurance	Chief Executive Officer	As Needed
Loepker	Mark	Insure	Director	As Needed
Lowden	Rob	Indiana University	Chief Information Officer	As Needed
Mackey	William	Indiana State University	Instructor	Full Time
McGuinness	Joe	Indiana Department of Transportation	Commissioner	As Needed
Miller	Scott	Citizens Energy Group	Manager of Security and Compliance	Co-Chair
Mosley-Romero	Chetrice	State of Indiana	Program Director	Chair
Newman	Anthony	Purdue University	Chief Information Security Officer	As Needed
O'Hara	Brian	BTO Associates, LLC	President/CEO	Full Time
Owen	Dan	Sexton's Creek	Associate	As Needed
Phelps	Tasha	Phelco Technologies, Inc.	President	Full Time
Roeder	John	Lt. Governor's Office	Director of Legislative Affairs & Parliamentarian	As Needed
Rupel	Johnathan (CPT)	Raytheon	Cyber Engineer	Full Time
Xu	Dongyan	Purdue University	Director-CERIAS and Samuel Conte Professor of Computer Science	Full Time

Introduction

Introduction

The world of cybersecurity is highly complex and cluttered with information, misinformation, and disinformation. As a consequence, it is important to approach it strategically and create simplicity.

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) continues its mission to move efforts and statewide cybersecurity initiatives to the "Next Level." With the ever-growing threat of cyberattacks, protecting Indiana's critical infrastructure is the focus of the IECC. Cybersecurity cannot be solved by one entity alone. The IECC works with private, public, academic, and military partners from all over the state to develop and maintain a strategic framework that establishes goals, plans, and best practices for cybersecurity.

The IECC is comprised of fifteen committees and working groups who have worked together to implement the statewide strategy of 2018 while developing an updated comprehensive strategic plan.

The following implementation plan is one of the fifteen specific plans that encompass the complete *2021 Indiana Cybersecurity Strategic Plan*.

For more information, visit www.in.gov/cybersecurity.

Executive Summary

Executive Summary

- **Research Conducted**
  - National Governors Association (NGA)
  - National Association of State Chief Information Officers (NASCIO)
  - Purdue Homeland Security Project
  - State-to-State Comparison Research
  - Cybersecurity Prediction Reports
  - Fusions Centers
  - Information Sharing and Analysis Centers (ISAC)
  - Indiana Department of Homeland Security (IDHS)/U.S. Department of Homeland Security (USDHS)
  - Conferences
  - Webinars
  - Best Practices/Examples of other Councils and Boards
  - Feedback from Council members
  - INSuRE Program
  - Presidential Executive Order
  - National Conference of State Legislators Cybersecurity Taskforce Resources and Whitepapers

- **Research Findings**
  - It was imperative to understand all aspects of the cyber ecosystem within state government. This included understanding:
    - Fusions Centers
      - https://www.dhs.gov/annual-fusion-center-assessment-and-gap-mitigation-activities
      - https://nfcausa.org/
      - https://www.dhs.gov/national-network-fusion-centers-fact-sheet
      - 2018-to-2021-National-Strategy-for-the-NNFC7715.pdf (wpengine.com)
    - Information Sharing
      - National Strategy for Information Sharing: https://www.dni.gov/index.php/who-we-are/organizations/ise/ise-archive/ise-additional-resources/1763-2012-national-strategy-for-information-sharing-and-safeguarding-nsiss
      - ISAC state to state comparison primary research
      - See Research Executive Summary for Cyber Awareness and Sharing Working Group
    - National Guard cyber strategy and capabilities
    - IDHS cyber strategy and capabilities
    - Federal partnerships
    - In our research, we were unable to find a comprehensive, deep analysis of federal and state policy around cybersecurity from 2011-2021, which included not just legislation that passed, but legislation that failed as well.

    - The INSuRE project develops a partnership among Centers of Academic Excellence in Information Assurance Research (CAE-R), the National Security Agency (NSA), the Department of Homeland Security, and other federal agencies in order to design, develop and test the research network. INSuRE is a self-organizing, cooperative, multi-disciplinary, multi-institutional, and multi-level collaborative research project that can include both unclassified and classified research problems in cybersecurity.
    - The mission of the National Conference of State Legislators Cybersecurity Task Force is to engage members in policy discussions, educate members and extend networking opportunities to legislative leaders on cybersecurity issues through a series of well-defined programs, webinars on key definitions and critical cyber policy issues as well as supporting private-public networks. The lifespan of this task force would be two years with the option to extend for one additional year.

- **2021 Working Group Deliverables**
  - Policy Research Report
  - IECC Scorecard 2.0
  - Indiana State of Cyber Report 2017-2021
  - IECC Strategic Plan - 2021
  - Outreach to Underrepresented Sectors

- **References**
  - NGA Meet the Threat - https://www.nga.org/cms/meet-the-threat
  - National Association of State Chief Information Officers (NASCIO) - https://www.nascio.org/
  - U.S. Computer Emergency Readiness Team (US-CERT): https://www.us-cert.gov/
  - Report: State of the States on Cybersecurity (Pell Center)
  - Memo on State Cybersecurity Governance Bodies
  - Memo on State Cybersecurity Response Plans
  - Michigan Cyber Disruption Response Plan
  - NIST Computer Security Incident Handling Guide
  - Cyber Disruption Response Planning Guide - NASCIO
  - Building a Cybersecurity Workforce Pipeline - National Governors Association
  - INSuRE Program - http://insurehub.org/
  - National Governors Association - https://www.nga.org/cms/home
  - The memo, State Cybersecurity Budgets, provides a brief review of how states budget financial resources for cybersecurity and the current levels of funding in many states.
  - National Conference of State Legislators
  - Congressional Cybersecurity Caucus
  - MS-ISAC (Multi-State Information Sharing & Analysis Center)

- **Additional Notes**
  - **State and Other Example Websites**
    - Cyber Virginia
    - Michigan Cyber Initiative
    - Missouri Office of Cybersecurity
    - Pennsylvania
    - DET Cybersecurity Strategy 2017 (wi.gov)
    - Multistate Information Sharing and Analysis Center (MS-ISAC)

Research

Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
   a. Governor established Indiana Executive Council on Cybersecurity – March 2016
   b. Crit-Ex 2016
   c. Governor continued Indiana Executive Council on Cybersecurity – January 2017
   d. Developed and implemented the 2018 State Cybersecurity Strategic Plan by the Indiana Executive Council on Cybersecurity
   e. In Indiana, as state legislation regarding cybersecurity has come up in the last several years, the appropriate state agency has provided resources as needed.

2. **What (or who) are the most significant cyber vulnerabilities in your area**?
   a. Critical infrastructure, businesses, and individuals

3. **What is your area's greatest cybersecurity need and/or gap?**
   a. A comprehensive, collaborative strategic state-wide cybersecurity approach that will address:
      - 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; and
      - Ensure a robust workforce and talent pipeline in fields involving cybersecurity.
      - An education on the topic of cybersecurity with policy makers is needed on a local, state, and federal level.

4. **What federal, state, or local cyber regulations is your area beholden to currently?**
   a. Regulations vary by industry and sector.

5. **What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?**
   a. Other State Models such as:
      - Cyber Virginia
      - Michigan Cyber Initiative
      - Missouri Office of Cybersecurity
      - Pennsylvania
      - Washington Cybersecurity Program
      - DET Cybersecurity Strategy 2017 (wi.gov)
      - Multistate Information Sharing and Analysis Center (MS-ISAC)
      - The memo, State Cybersecurity Budgets, provides a brief review of how states budget financial resources for cybersecurity and the current levels of funding in many states.
      - National Conference of State Legislators - http://www.ncsl.org/ncsl-in-dc/task-forces/task-force-on-cybersecurity.aspx

6. **What research is out there to validate your group's preliminary deliverables? This could be surveys, whitepapers, articles, books, etc. Please collect and document.**
   - National Governors Association
   - National Association of State Chief Information Officers (NASCIO)
   - Purdue Homeland Security Project – in progress
   - State-to-State Comparison Research – ongoing
   - Cybersecurity Prediction Reports
   - Fusions Centers
   - Information Sharing and Analysis Centers (ISACs)
   - Indiana Department of Homeland Security/United States Department of Homeland Security (IDHS/USDHS)
   - Policy
   - Conferences
   - Webinars
   - Best Practices/Examples of other Councils and Boards
   - National Governors Association Whitepapers
   - State-to-State Examples
   - INSuRE Program participation
   - Presidential Executive Orders
   - The National Conference of State Legislators Cybersecurity Taskforce provides policy makers a variety of resources online.

7. **What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?**
   a. See question 5 and 6.

8. **What does success look like for your area in one year, three years, and five years?**
   a. Developing a sustainability model with appropriate resources that will continue to implement and demonstrate measurable improvement in the state's cybersecurity posture will be vital to the Council's continued success. The model will ensure that the Council continues to develop, maintain, and execute the implementation plan for accomplishing strategic cybersecurity objectives that are specific, measurable, achievable, and relevant to the overall strategic vision, which will be completed within an established timeframe over the next one, three, and five years.
   b. Complete an analysis of federal policy related to cybersecurity since 2011 and any federal acts that affect cybersecurity today.
   c. Complete an analysis of state policies the last five years that have passed or been debated.
   d. Increased understanding and awareness of cybersecurity threats with state and local governments.
   e. Assist in providing guidelines and resources that encourage safer municipality, corporate, and personal practices that protect the state's infrastructure and constituents.
   f. Utilize resources allocated to the council for policy tracking and monitoring, especially through university partnerships.

9. **What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?**
    a. An overall communication plan to increase cybersecurity awareness, programs, training, and education is needed.

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. Through https://www.cyberseekin.org/ we can see the state's cybersecurity supply and demand; pathways showing common roles within cybersecurity and transition opportunities; and training opportunities.

11. **What do we need to do to attract cyber companies to Indiana?**
    a. The State's emphasis on the importance of cybersecurity will attract companies to Indiana since critical infrastructures are securing their operations and data not only physically but through technology as well.

12. **What are your communication protocols in a cyber emergency?**
    a. The State of Indiana has developed a Cyber Incident Response Plan and we offer additional resources to assess your cybersecurity preparedness, including the Indiana Cybersecurity Scorecard. In addition, in 2021 Indiana lawmakers recently passed legislation that will increase the amount of information sharing regarding cyberattacks and other threats across state agencies and local government. This new law requires public-sector entities to report incidents such as ransomware, software vulnerability exploitations, denial-of-service attacks and more.

13. **What best practices should be used across the sectors in Indiana? Please collect and document.**
    a. See sector specific questionnaires in each of the other 14 strategic plans.

Deliverable: Policy Research Report

Deliverable: Policy Research Report

General Information

1. **What is the deliverable?**
   a. An update to the State and federal updated research report on cybersecurity legislation that was completed in 2018.

2. **What is the status of this deliverable?**
   ☐ Completed ☐ In-progress 25% ☐ In-progress 50% ☐ In-progress 75% ☒ Not Started

3. **Which of the following IECC goals does this deliverable meet?**
   ☐ 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?**
   ☒ 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. Compiling the policies and legislation that have been introduced since 2018 from all 50 state legislatures and Congress so that Indiana has material and other policies to reference in reviewing policy recommendations.

6. **What metric or measurement will be used to define success?**
   a. Completion of an analysis of all 50 states and federal legislation.

7. **What year will the deliverable be completed?**
   ☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
   a. IECC's committees and members

9. **Which state or federal resources or programs overlap with this deliverable?**
   a. Perhaps the research done by the National Conference of State Legislators (https://www.ncsl.org/) may have research that overlaps with this deliverable.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. None

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. None

12. **Who should be main lead of this deliverable?**
    a. State of Indiana Cybersecurity Program Director

13. **What are the expected challenges to completing this deliverable?**
    a. Being able to complete a comprehensive analysis with limited resources.

Implementation Plan

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

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Select a resource to complete updated research report	Cybersecurity Program Director	0	January 2022	Selected INSuRE Partner
Conduct research and utilize a tool to use for future policy analysis	INSuRE Program Partner: University of Alabama	0	February – November 2022	Cybersecurity Program Director will serve as the Technical Director of the project

Final report and tool completed	INSuRE Program Partner:	0	December 2022	
Provide IECC with final report and access to tool	Cybersecurity Program Director	0	December 2022	
Update table, additional analysis, and executive summary of changes	IECC approved intern (in-state or public/private partner) or university partnership	0	Once a year	
Present IECC with updated executive summary and tool	Cybersecurity Program Director	0	Once a year	

Resources and Budget

15. Will staff be required to complete this deliverable?

☐No ☒ Yes

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
2.5 FTE	1 FTE	Research and Policy	Grant, public, or private contribution	State of Indiana	The FTEs is expected to be the students to assist with research a few months a year and the Cybersecurity Program Director providing guidance.

16. What other resources are required to complete this deliverable?

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
Airtable Tool	As the policy collection and sharing grows, there may be a need to add more records beyond the free version and use the advanced features	$10-20 per month depending on upgrade		State of Indiana		

Benefits and Risks

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

a. As the IECC continues to stay current and consider possible policy recommendations, it is imperative that we understand what policy or policies have been discussed, passed, and/or failed in all 50 states and at the federal level from 2011 - 2021. This will help assure we understand these recommendations in the proper context and communicate our recommendations, and any that do go before the legislature will likely be more successful because the state will have learned from others. There is no report or tool currently available that comprehensively looks at all cyber policy introduced in all 50 states. This will not only be of benefit to Indiana but other states as well.

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

a. As policy is being discussed, the State of Indiana does not want to pass any legislation that may have an unintended consequence that would increase the cybersecurity risks or impact the investigation of a cybercrime. It would be difficult to estimate the costs of the risk reduction.

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

a. The largest risk of not updating and completing this deliverable is creating a policy that is not well informed, and it increases the possibility of unintended consequences to occur that would increase the cybersecurity risks or impact the investigation of cybercrime.

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

a. Completion of the policy research will be one metric. Equally important is that the research and possible tool is useful for our policy efforts.

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

☐No ☒ Yes

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?

☒No ☐ Yes

a. No state has a publicly published review of all cyber legislation introduced from 2011-2021. One could assume those states have had a difficult time moving cyber policy forward, or have not been successful at doing so, and could have benefited from the lessons learned in this type of research project.

Other Implementation Factors

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

a. The scope of the project is so large that there is a likelihood that some policies have been missed.

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

☒No ☐ Yes

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

a. A resource should be devoted to updating this tool and analysis at least once a year so the information does not become stale and can continue to be useful.

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

a. The Cybersecurity Program Director will work with the INSuRE program to initiate the process of identifying a resource for completing the updated report.

27. Can this deliverable be used by other sectors?

☐No ☒ Yes

a. All sectors can benefit

Communications

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

a. IECC members, IECC leadership, Governor's Office, legislators and their staff, lobbyists, state agency policy directors, sector associations, key national associations, and other state partners.

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

☒No ☐ Yes

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

a. None as of now.

Evaluation Methodology

Objective 1: IECC and partners will update a report of state and federal cybersecurity legislation by December 31, 2022.

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: IECC Scorecard 2.0

Deliverable: IECC Scorecard 2.0

General Information

1. **What is the deliverable?**
   a. IECC Scorecard 2.0 – More specifically, providing a guide to go along with the Scorecard so that an organization can begin the process of deciding what things they can do to improve their cybersecurity posture.

2. **What is the status of this deliverable?**
   ☐ Completed ☐ In-progress 25% ☒ In-progress 50% ☐ In-progress 75% ☐ Not Started

3. **Which of the following IECC goals does this deliverable meet?**
   ☐ 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 goal of the scorecard is two-fold. In its current form, it serves a baseline as a measurement of the effectiveness of the IECC deliverables as well as a more detailed cybersecurity self-assessment. Secondly, it provides a starting place with some high-level direction of how to "level up."

6. **What metric or measurement will be used to define success?**
   a. In addition to completing the Scorecard Level Up Guide, there will be a sampling of local governments who will be completing the scorecard and guide to measure its effectiveness.

7. **What year will the deliverable be completed?**
   ☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
   a. Small and medium sector companies and local government.

9. **Which state or federal resources or programs overlap with this deliverable?**
   a. Federal and private assessments.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. All, as needed.

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. IECC will continue its partnership with Indiana State University and Purdue University.

12. **Who should be main lead of this deliverable?**
    a. IECC Director in coordination with Indiana State University and Purdue University.

13. **What are the expected challenges to completing this deliverable?**
    a. Ensuring the use of the Scorecard is more well-rounded and is a tool for utilizing more of the state's cybersecurity resources.

Implementation Plan

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

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Initiate next phase of the Scorecard with IECC partner to complete deliverable	Cybersecurity Program Director	100	August 2021	
Review Scorecard	Cybersecurity Program Director with Purdue University and Indiana State University	50	November 2021	
Draft Changes/Updates to the Scorecard	Cybersecurity Program Director and Program Communications Manager with Purdue University and Indiana State University	0	December 2021	
Develop implementation plan	Cybersecurity Program Director and Program Communications Manager	0	January 2022	
Identify pilot group	State and Local Government Committee	0	January 2022	
Pilot Group complete Scorecard 2.0	Pilot Group	0	June 2022	
Take survey on product	Cybersecurity Program Director	0	August 2022	
Make any additional edits based on the pilot group's feedback	Cybersecurity Program Director and Program Communications Manager with Purdue University and Indiana State University		September 2022	
Develop updated implementation plan for mass public	Cybersecurity Program Director and Program Communications Manager	0	September 2022	

Execute implementation plan for launch of Scorecard 2.0 to public	IECC partners	0	October 2022	

Resources and Budget

15. Will staff be required to complete this deliverable?

☐No ☒ Yes

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
1.5 FTE	N/A	Cybersecurity and business	State of Indiana	IECC Partner	

16. What other resources are required to complete this deliverable?

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. Measurement of the success of IECC efforts and deliverables and more importantly provide the public with an updated tool (specifically small/medium size businesses and local governments) to start to identify their current cybersecurity posture. Additionally, after making improvements, this gives immediate feedback as to whether the improvement was made.

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

a. Scorecard 2.0 is meant to assess current-state and address the problem areas most appropriate to the organization surveyed. By doing this at a business level and in a way that can be provided to executive leadership of a company, the scorecard could assist in prioritizing and providing a form of measurement to reducing cybersecurity risk or impact.

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

a. The state and IECC would have one less resource to share with emergency managers help maintain a higher level of cybersecurity preparedness; one less tool that can be used to measure Indiana's overall posture.

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

a. Completion of the Scorecard 2.0 is an output success. Having 90 percent of all sentinel sample complete the Scorecard 2.0.

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

☒No ☐ Yes

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?

☐No ☒ Yes

a. As of August 2021, according to the National Conference of State Legislators (NCSL), 28 states have created a statewide cybersecurity task force, commission or advisory council or similar group. But no other state has provided a user-friendly scorecard that can be used by the organization, as well as a measurement for the effectiveness of the tools created by the Council.

Other Implementation Factors

---

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

a. Short time frame and engaging each sector.

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

☒No ☐ Yes

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

a. It will require someone to have the ability to review and update it as necessary.

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

a. All committees and working groups will be contacted with the Scorecard 2.0

27. Can this deliverable be used by other sectors?

☐No ☒ Yes

Communications

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

a. IECC, Government, businesses, associations, sector partners

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

☐No ☒ Yes

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

a. No other like this.

Evaluation Methodology

Objective 1: IECC, along with Indiana State University and Purdue University, will develop a Scorecard 2.0 with a Level Up Guide to improve cybersecurity posture by January 2022.

Type: ☒ Output ☐ Outcome

☒ 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 pilot Indiana's Cybersecurity Scorecard 2.0 with Level Up Guide with local governments by July 2022.

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 3: IECC will relaunch Indiana's Cybersecurity Scorecard 2.0 with Level Up Guide to the public by December 2022.

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:
Indiana State of Cyber Report (2017-2021)

Deliverable: Indiana State of Cyber Report (2017-2021)

General Information

1. **What is the deliverable?**
   a. Indiana Cyber Success Report (2017-2021)

2. **What is the status of this deliverable?**
   ☒ Completed ☐ In-progress 25% ☐ In-progress 50% ☐ In-progress 75% ☐ Not Started

3. **Which of the following IECC goals does this deliverable meet?**
   ☐ 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?**
   ☒ 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 compilation of Cyber Accomplishments will illustrate and provide definition to the success achieved in Indiana with cybersecurity within the IECC and outside the IECC.

6. **What metric or measurement will be used to define success?**
   a. Presentation of successful projects and deliverables both within IECC and its members and entities outside of the Council in public and private sector.

7. **What year will the deliverable be completed?**
   ☒ 2021 ☐ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
   a. State, local government, K-12, higher education, and small/medium businesses

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

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. All the other committees will be contributing their deliverable updates and strategic plans.

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. The state agencies on the IECC will contribute as the are able and the rest of the report will be based on what outside partners (public, private, academia).

12. **Who should be main lead of this deliverable?**
    a. Indiana State Cybersecurity Program Director

13. **What are the expected challenges to completing this deliverable?**
    a. It is a volunteer council and with so many things that are priority and a lack of time and resources may also hinder the completion of this deliverable.

Implementation Plan

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

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Collect/Feature Cyber Accomplishments from IECC members/state agencies and public/private sectors	IECC	100%	September 2021	
Draft outline	Cybersecurity Program Director		September 2021	
Draft content	Cybersecurity Program Director		October 2021	
Layout with graphic designer	Cybersecurity Program Director, IN.gov		October 2021	
Edit content	IECC project support staff from IOT/IDHS		October 2021	
Get approval from IDHS/IOT	IDHS Executive Director Cox and Tracy Barnes		October 2021	
Finalize report	IECC project support staff from IOT/IDHS		October 2021	
Present report to Governor	IECC Chair Cox and Voting members		October 29, 2021	

Resources and Budget

15. Will staff be required to complete this deliverable?

☐No ☒ Yes

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
2 FTE	1 FTE	Communications	IECC Staff	N/A	

16. What other resources are required to complete this deliverable?

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?

a. This deliverable provides examples of Indiana's presence as a cybersecurity leader among states in cybersecurity governance, programming, and public awareness/education.

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

a. By continuing to educate and inform Hoosiers about cybersecurity, the knowledge gained by the general public, state and local government, education and the public/private sectors helps mitigate the potential for cyber incidents and cyberattacks, including those involving identity theft and other forms of cybercrime.
b. In the absence of a continued communications campaign – in which the public is informed and encouraged about remaining vigilant as it regards all aspects of cybersecurity and taking a personal responsibility for their part of cyberspace – not having a scorecard could create a higher likelihood that cyber incidents and cyberattacks will occur at a rate that grows, in terms of the severity of what is lost financially, as well as the protection of our own personal identifying information.

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

a. An opportunity is missed to educate and inform Hoosiers about cybersecurity.

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

a. The opportunity to inform Hoosiers regarding the continued progress being achieved in Indiana with cybersecurity.

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

☒No ☐ Yes

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?

☒No ☐ Yes

Other Implementation Factors

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

a. Not enough staff or key reviewers not making needed edits on time.

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

☒No ☐ Yes

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

a. IECC staff time to update/collect additional case studies.

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

a. IECC members

27. Can this deliverable be used by other sectors?

☒No ☐ Yes,

Communications

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

a. IECC Members, small/medium small business, state and local government, K-12 and Higher Education

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

☐No ☒ Yes

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

a. Potential to highlight selected case studies as part of the Indiana Cybersecurity Hub website, Cyber Hub Blog and "Days of Our Cyber Lives" podcast with the Treasurer of State, Indiana Bond Bank and IECC.

Evaluation Methodology

Objective 1: The Indiana Executive Council on Cybersecurity will develop a report to address the status and successes of the IECC as well as Indiana organizations by October 29, 2021.

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: IECC 2021 Strategic Plan

Deliverable: IECC 2021 Strategic Plan

General Information

1. **What is the deliverable?**
   a. IECC 2021 Strategic Plan

2. **What is the status of this deliverable?**
   ☒ Completed ☐ In-progress 25% ☐ In-progress 50% ☐ In-progress 75% ☐ Not Started

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns.**
   ☒ 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?**
   ☐ 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. Documentation of the creation, implementation, and evaluation of the IECC, including the project plan, framework, governance, tools used, and lessons learned.

6. **What metric or measurement will be used to define success?**
   a. Completion and inclusion of the IECC Program Documentation in the final plan

7. **What year will the deliverable be completed?**
   ☒ 2021 ☐ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
   a. IECC, Governor's office, federal and state partners

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. All, as needed

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. IOT, IDHS

12. **Who should be main lead of this deliverable?**
    a. State of Indiana Cybersecurity Program Director

13. **What are the expected challenges to completing this deliverable?**
    a. It is a volunteer council and with so many things that are priority and a lack of time and resources may also hinder the completion of this deliverable.

Implementation Plan

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

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Determine what the Framework Document will contain	Program Director, Program Manager	100%	April 2021	
Develop draft Table of Contents	Program Manager	100%	April 2021	
Review draft TOC	Program Director, Program Manager	100%	September 2021	
Develop list of subtopics	Program Director, Program Manager	100%	March – April 2021	
Begin documenting topics and subtopics	Program Manager	100%	April 2021	
Determine document design	Program Director, Program Manager	100%	September 2021	
Complete Draft	Program Manager	100%	September 2021	
Final Draft approval	Program Director	100%	October 2021	
Strategic Resource WG approval process	Program Manager	100%	September 2021	
Complete documentation and Final Review	Program Director	100%	October 2021	
Integrate document into final report	Program Director, Program Manager	100%	October 2021	

Resources and Budget

15. Will staff be required to complete this deliverable?

☐No ☒ Yes

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
3 FTE			State of Indiana – IOT/IDHS		

16. What other resources are required to complete this deliverable?

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
Technical Editors	Proofreading	$0	$0	State of Indiana IOT/IDHS	N/A	
Development of graphic design lay out	Design	N/A	N/A	State of Indiana IOT/IDHS		

Benefits and Risks

17. What is the greatest benefit of this deliverable?

a. Providing supporting documentation of how the Council was planned, established, and governed in addition to addressing what the Council has accomplished since it's first strategic plan in 2018. Sharing a repeatable framework for other organizations and states to leverage.

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

a. This framework documentation provides support for the Council's work and will help support the organization of future Council efforts.

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

a. The organization and processes used with the Council will be lost and the future movement of the IECC support organization will have less direction and strategy. Knowledge sharing with other states and agencies will not occur.

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

a. Completion of the documentation and Strategic Resource Working Group approval in October 2021. The final to the Governor in late October.

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

☐No ☒ Yes

a. Many states now have cybersecurity strategic plans. Indiana, however, is still the leading state of the having the most comprehensive, in-depth plan.

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?

☐No ☒ Yes

a. Of the states that do not have cybersecurity efforts to the degree of Indiana, they often struggle with public/private partnerships as well as state-agency fighting. These are things we do not experience in Indiana around the cybersecurity strategy.

Other Implementation Factors

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

a. Resource constraints, competing priorities, and a short timeframe.

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

☒No ☐ Yes

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

a. Maintaining the current structure of the IECC, as it regards the responsibilities of the Cybersecurity Program Director and the collaboration by/between all members of the Council and its leadership.

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

a. State of Indiana Cybersecurity Program Director

27. Can this deliverable be used by other sectors?

☐No ☒ Yes,

a. All sectors

Communications

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

a. IECC, State and Local Government, Public and Private Sector, General Public

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

☐No ☒ Yes

a. It will be posted on the Indiana Cybersecurity Hub website in October 2021.

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

a. Further detailed information can be shared with internal management and those who request it, such as the National Governors Association (NGA), and other states.

Evaluation Methodology

Objective 1: IECC will develop a 2021 Strategic Plan for the Council by October 29, 2021.

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: Outreach to Underrepresented Sectors

Deliverable: Outreach to Underrepresented Sectors

General Information

1. **What is the deliverable?**
   a. To develop an outreach and communications strategy for industrials that are not represented on the council. The ongoing communications strategy will help ensure the council is informed of cyber concerns occurring within these industries and that these industries are aware of the activities and deliverables of the council.

2. **What is the status of this deliverable?**
   ☐ Completed ☐ In-progress 25% ☐ In-progress 50% ☐ In-progress 75% ☒ Not Started

3. **Which of the following IECC goals does this deliverable meet?**
   ☐ 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?**
   ☐ 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. Increased awareness within the council of cyber challenges or concerns within the unrepresented industries. Increase awareness within the industries of activities and deliverables of the council.

6. **What metric or measurement will be used to define success?**
   a. The establishment of primary contacts for each industry and regular meetings to facilitate knowledge sharing between industry and the council.

7. **What year will the deliverable be completed?**
   ☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
   a. The strategic resources working group and the unrepresented industries.

9. **Which state or federal resources or programs overlap with this deliverable?**
   a. None at this time.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. None

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. Industry Groups of the unrepresented industries

12. **Who should be main lead of this deliverable?**
    a. The strategic resources working group.

13. **What are the expected challenges to completing this deliverable?**
    a. Establishing the right contacts within each of the unrepresented industries

Implementation Plan

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

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Develop list of unrepresented industries	Strategic Resources Committee	0	03/2022	
Identify organizations and primary contacts for each industry	Strategic Resources Committee	0	17/2022	

Make preliminary introductions to each industry	Strategic Resources Committee	0	12/2022	
Establish regular communication cadence for each industry	Strategic Resources Committee	0	03/2023	

Resources and Budget (Please add rows as needed)

15. Will staff be required to complete this deliverable?

☒No ☐ Yes

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
None	None				

16. What other resources are required to complete this deliverable?

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
None						

Benefits and Risks

17. What is the greatest benefit of this deliverable?

a. Providing a communications conduit for unrepresented industries

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

a. By establishing processes to share resources available to Indiana industries that could benefit from the work being performed by the council.

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

a. Increased cyber risks to the unrepresented sectors due to not leveraging the state resources available to them.

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

a. Success is defined by providing the unrepresented industries with the tools and resources to better mitigate cyber risks.

21. Are there comparable jurisdictions (e.g., other states) that have similar projects that we can compare this project to using the same metrics?
☒No ☐ Yes

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?
☒No ☐ Yes

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?
☒No ☐ Yes

25. What will it take to support this deliverable if it requires ongoing sustainability?
a. Not ongoing

26. Who has the committee/working group contacted regarding implementing this deliverable?
a. None

27. Can this deliverable be used by other sectors?
☒No ☐ Yes

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?
a. All IECC members

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?
☐No ☒ Yes

30. What are other public relations and/or marketing considerations to be noted?
a. As we gather resources and deliverables that will be helpful to other industries, it would be prudent to update the website as well.

Evaluation Methodology

Objective 1: With key partners, identify cybersecurity awareness needs in additional Indiana industries (manufacturing, transportation, small business, and agriculture) by December 2022.

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: Provide industry contacts with education materials and set up a regular communication cadence for each industry by March 2023.

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 Cybersecurity Scorecard 1.0
- Policy Research Report 1.0

Indiana Scorecard 1.0

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

Welcome to the State of Indiana's Cybersecurity Scorecard in partnership with Purdue University!

This Scorecard should take you approximately 10-15 minutes to complete.

For your convenience, this Scorecard is a fillable PDF, can be saved with your answers, and will automatically calculate your score.

For your reference there is a Glossary of Terms on the last page with definitions for technical terms highlighted in blue lettering.

If you have any questions on this Scorecard, please email the Cybersecurity Program Director Chetrice Mosley at mosleyclm@iot.in.gov.

Name of Organization

_____

Your E-mail Address

_____

How many employees are there in your organization (full and part time)?

_____

How many employees have information technology related duties?

_____

How many employees have cybersecurity related duties?

_____

Does your organization outsource your information technology needs?

- ◯ Yes
- ◯ No

Does your organization outsource your cybersecurity needs?

- ◯ Yes
- ◯ No

Question 1

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
Our organization values cybersecurity.	○	○	○	○	○	○

Question 2

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
We know the type of data our organization stores (financial, health, customer, proprietary, trade secrets, etc.)	○	○	○	○	○	○

Question 3

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
We have evaluated the operational need of my data and systems to our organization's function (If we are a grocery store, we need to set pricing, scan barcodes, weigh produce, etc.)	○	○	○	○	○	○

Question 4

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
Our business/organization model influences the way we approach cybersecurity.	○	○	○	○	○	○

Question 5

	I Don’t Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
When we make a decision in our organization that involves legal, operational, technological, or physical/environmental (office space) change, we consider cybersecurity as part of that decision.	○	○	○	○	○	○

Question 6

	I Don’t Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
We are familiar with the cybersecurity threats or risks (malicious software, phishing, and/or data breaches) to our organization specifically to our operations, reputation, inventory, customers, and employees.	○	○	○	○	○	○

Question 7

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
We apply physical (doors and locks) controls in the same way we apply computer (ID and password) controls.	○	○	○	○	○	○

Question 8

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
We have **system checks** in place to make sure that our data is not compromised or changed.	○	○	○	○	○	○

Question 9

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
Our data is available to employees or clients when needed. (If our government or commerce site was unavailable to customers or employees, we would know what to do).	○	○	○	○	○	○

Question 10

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
As with the general policies in our organization, (dress code, paid time off, benefits, tardiness) we have policies that apply to cybersecurity.	○	○	○	○	○	○

Question 11

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
Our cybersecurity technology (such as **antivirus**, wireless access points, network equipment, etc.) is updated/configured to best protect our business operations and data.	○	○	○	○	○	○

Question 12

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
We have a process in place to address a **cyberthreat**.	○	○	○	○	○	○

Question 13

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
We have a cyber emergency response plan in place to address a **cyberattack** on our organization.	○	○	○	○	○	○

Question 14

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
If we were impacted by a cyber emergency (e.g. **ransomware**), we know how our organization would recover our data and/or operational systems.	○	○	○	○	○	○

Question 15

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
After a **cyberthreat** or emergency, our organization will make changes to people, process, technology, etc. to improve our security.	○	○	○	○	○	○

Question 16

	I Don't Know (0)	Never (1)	Almost Never (2)	Occasionally /Sometimes (3)	Almost Every Time (4)	Every Time (5)
Our executive leadership receives periodic status, physical, and cybersecurity updates.	○	○	○	○	○	○

Question 17

	I Don't Know (0)	Never (1)	Almost Never (2)	Occasionally /Sometimes (3)	Almost Every Time (4)	Every Time (5)
We keep an inventory of our data (customer, payroll, and/or financial data) and devices that provide access to our data.	○	○	○	○	○	○

Question 18

	I Don't Know (0)	Never (1)	Almost Never (2)	Occasionally /Sometimes (3)	Almost Every Time (4)	Every Time (5)
We provide our employees cybersecurity awareness and/or training.	○	○	○	○	○	○

Question 19

	I Don't Know (0)	Never (1)	Almost Never (2)	Occasionally /Sometimes (3)	Almost Every Time (4)	Every Time (5)
We protect our business and customer information so that only the employees that need to see it, can.	○	○	○	○	○	○

Question 20

	I Don't Know (0)	Never (1)	Almost Never (2)	Occasionally /Sometimes (3)	Almost Every Time (4)	Every Time (5)
We would know if our cybersecurity technology detected a **cyberthreat**.	○	○	○	○	○	○

Question 21

	I Don't Know (0)	Never (1)	Almost Never (2)	Occasionally /Sometimes (3)	Almost Every Time (4)	Every Time (5)
Our 'smart' devices (such as security cameras, thermostats, HVACs, alarm systems, etc.) are not connected to a publicly available internet connection.	○	○	○	○	○	○

Question 22

	I Don't Know (0)	Never (1)	Almost Never (2)	Occasionally /Sometimes (3)	Almost Every Time (4)	Every Time (5)
Our 'smart' devices (such as security cameras, thermostats, HVACs, alarm systems, etc.) are periodically monitored and scanned for security vulnerabilities and malicious software	○	○	○	○	○	○

To find your score, please add the numbers associated with the responses for questions 1 through 22. For example, selecting "Almost Every Time (4)" has a numberical value of 4.

Your score is 0_____

Refer to the chart below to determine where you fall on the scale.

Grade	Exemplary	Accomplished	Developing	Beginning	Undeveloped
Minimum with color code	88	66	44	22	0
Range	110-88	87-66	65-44	43-22	21-0
Spread	22	21	21	21	21

Glossary of Terms

System checks- procedures, equipment, and/or periodic inspection to maintain security
Antivirus- i.e. McAfee, Norton, or Windows Defender
Cyberthreat- the possibility of a malicious attempt to damage or disrupt a computer network or system. For example, social engineered trojans, unpatched software (such as Java, Adobe Reader, Flash), and/or phishing
Cyberattack- an attack initiated from one or more computers against a website, computer system or a networked enterprise of several computers that compromises the confidentiality, integrity or availability of any computer(s) or stored information
Ransomware- a type of malware that prevents users from using their computer and displays messages requiring users to pay a ransom usually through an online payment in order to regain access to his/her computer, information, and/or system.

Policy Research Report 1.0

An Analysis of Cybersecurity Legislation and Policy Creation on the State Level

Adam Alexander	Paul Graham	Eric Jackson	Bryant Johnson	Tania Williams
aha0007@uah.edu	pag0006@uah.edu	eaj0010@uah.edu	bej0003@uah.edu	tw0063@uah.edu

Cybersecurity Capstone - IS692 - Spring 2018
University of Alabama in Huntsville
301 Sparkman Drive, Huntsville
AL, United States of America 35899

***Abstract* — To best create an effective cybersecurity strategy, it is imperative to understand the policy discussions and trends on a federal and state level. Effective cybersecurity legislation is vital to maintaining our country's infrastructure and protecting our citizenry. Since cybersecurity is often decided on the state level, states need to be aware of the trends in cybersecurity legislation. The purpose of this research was to conduct an analysis of cybersecurity policy from across the United States in an effort to assist the State of Indiana in understanding its cybersecurity risk profile. This analysis included an examination of common trends in cybersecurity legislation. It involved researching cybersecurity policies from all 50 states and the federal government. After creating this baseline, the next phase of the research was to find and record relevant metadata for each policy. This data contained additional data, such as did it pass, who were the supporters, was it revised and other information that is useful to cyber security policy creators. The final goal of the research was to provide a searchable tool that could be utilized to fashion a successful cybersecurity bill and a summary of cybersecurity trends from 2011 to Spring 2018.**

***Index Terms*—cybersecurity, policy, legislation, United States, states, Federal Government**

I. Introduction

A. Problem Statement

It is critical that individual states enact policy dealing with cybersecurity. The National Governors Association, in hopes of addressing the cybersecurity deficit found in states across the nation, drafted A Compact to Improve Cybersecurity. This compact includes a commitment to build cybersecurity governance, to prepare and defend the state from cybersecurity events, and to grow the nation's cybersecurity workforce [1]. However, meeting such a commitment is difficult without an understanding of existing attempts of cybersecurity legislation from across the country.

B. Purpose Statement

In order to assist the State of Indiana in fulfilling this compact by developing their cybersecurity policy, we conducted a policy analysis using the following research questions:

- What policy has been passed successfully/unsuccessfully in other states from 2011 to present?
- Who were the supporters of the policy?
- What type of support did the proposed policy receive, and if it did not pass, why?
- How can such information be presented to Indiana stakeholders in a clear and concise manner?
- What trends are evident among the states regarding cybersecurity policy?

By providing the State of Indiana with a searchable database of successful and failed legislation from across the country, we will supply the state with information needed to create successful and effective cybersecurity legislation.

C. Motivation

As technology advances and cyber threats continue to grow, updating our country's cybersecurity policy is an important and daunting task. Our collective security infrastructure is woefully out-of-date and security policies differ from state to state. Therefore, the governor of Indiana signed executive order 17-11 in January of 2017, creating a council to "develop, maintain and execute an implementation plan for accomplishing strategic cybersecurity objectives that are specific, measurable, achievable, and relevant to the strategic vision" of the state [2]. The role of this research was to provide the state with an analysis of existing cybersecurity policy from across the United States proposed from 2011 to present. The research identified trends in policy (whether a policy was adopted or not after proposal). This research will serve as a baseline for the State of Indiana when crafting their policy and will provide valuable insight to other states who might choose to use the research.

Perhaps the greatest concrete problem regarding the research is the scope. It is challenging to do a thorough examination of all the states. We addressed the scope of our work by dividing the workload among the group members.

In order to ensure that all policy was evaluated systematically, we developed a data collection form for the team to use. Additionally, we organized the research by the 20 existing Indiana committees, streamlining the examination and evaluation of the data.

We examined similar trends analysis research and found, while research exists, the scope of the research was narrower. For example, Lowry examined the regulation of mobile payments but only dealt with federal law, making the reporting of such trends much easier [3]. Additionally, we were able to locate studies of trends resulting from one piece of legislations but did not find any previous work dealing with trends regarding state legislation.

We provided a baseline for other large scale legislative trends analysis. Additionally, our database of national cyber-related policies provides a valuable resource for other states as they seek to improve their cybersecurity posture.

II. LITERATURE REVIEW

A. Need for Cybersecurity Legislation

In 2007 the government of Estonia was hit by a cyber-attack that paralyzed the country, shutting down its largest bank, rendering credit cards useless, knocking media outlets offline, and crippling the country's telephone [4]. Could such an attack happen in the United States? Former cybersecurity czar Richard Clarke maintains that "few national governments have less control over what goes on in its cyberspace than Washington" and that "America's ability to defend its vital systems from cyber-attack ranks among the world's worst" [5]. This threat of cyber-attack is not limited the federal government. Individual states also must consider the threat of weak cybersecurity.

States, which hold databases full of health records, driving records, criminal records, professional licenses, tax information, and birth certificates, must have procedures in place to protect this personally identifiable information. The states also often have jurisdiction of cyber-related crimes and are entrusted with cybersecurity education [6]. As Glennon notes, "Every state has enacted laws directed at protecting state governments and businesses specifically from cyber-intrusions" [6]. On top of this, states also bear much of the burden of regulation; however, as Sales states, law and policy of cyber-security are undertheorized and most governments concern themselves with criminal law but are reluctant to see cybersecurity management in regulatory terms [5].

Bosch also notes issues with regulation, stating a reliability standard, such as those created through the Federal Power Act, "does not fully address Smart Grid cybersecurity from an interoperability perspective" [7]. Alternatively, he notes the difficulty of crafting the standards to begin with, citing the failed GRID Act of 2010, which the federal legislative branch could not agree on how the grid's cybersecurity concerns should be addressed [7].

As every state is unique, so must each state take a different approach to cybersecurity. Schneider, in his call for government support of cybersecurity, noted as social values differ, governments should not expect uniform sets of cybersecurity goals; instead "government interventions designed to achieve goals in some geographic region . . . must also accommodate the diversity in goals and enforcement mechanisms found in other regions" [8]. When states craft their cybersecurity legislation is it necessary to build on the experience of other states and to understand national policy trends.

B. Trend Analysis Approaches

As Godara notes, crime has seen a "revolutionary shift from the main actor, the criminal, to certain non-actors in the cyber world called 'intermediaries.' To what extent an intermediary can be held liable for the crimes committed in cyber space is a question which is mooted all over the world" [9]. Godara's research compares legislative and judicial trends in different countries. Her work was limited to rulings regarding intermediary liability in the United Kingdom, United States, and India. When examining legislation in the United States, her approach was to limit her study to federal court cases and sought to analyze fewer than ten rulings.

Bulger, Burton, O'Neill, and Staksrud also examine legislative trends in their examination of how different countries seek to protect children online [10]. In their research, they examined the United States, South Africa, and the European Union. The research targeted key crimes and then reported each country's laws regarding these crimes. Again, the authors chose to research only federal laws and did not examine legislation from individual states.

Neither Godara nor Bulger et al. considered failed legislation when examining these trends [9, 10]. While both research examples relate to trends in cybersecurity, they do not provide an approach to handling the large volume of legislation relating to cybersecurity produced by individual states from 2011 to present.

III. PROGRESS

A. Plan Overview

1) Major Tasks:

- Performed search for state and federal bills.
- Classified state and federal bills.
- Collected metadata and input into collect tool.
- Identified cybersecurity trends from collection tool.
- Created a report detailing trends.

2) Contribution of Tasks to the Overall Utility of the Work: Each task was designed to bring us closer to solving our problem (help the State of Indiana create successful cybersecurity policies). After we classified the state bills, we collected metadata for each one. This task allowed us to

create trends based upon the metadata (passed/failed, detractors/supporters, etc.). Once these trends were identified, then a report was crafted to help committees for the State of Indiana come up with cybersecurity bills that are necessary to protect Indiana's interest and have a higher chance of passing.

3) Deliverables:

- Proposal
- Bi-weekly presentation
- Midterm Presentation
- Midterm Report
- Airtable sortable table with metadata including bill location [https://airtable.com/shrCcYzKJGH1jyvrx]
- Final Presentation
- Final Report

B. Schedule

- 2/1/2018 Met with the technical director and determined goals for the project
- 2/6/2018 Discussed draft proposal with Technical Director
- 2/9/2018 Submitted final proposal
- 2/9/2018 - 3/2/2018 Searched for policies and classification
- 3/2/2018 Prepared midterm report
- 3/2/2018 - 3/23/2018 Completed metadata upload
- 3/24/2018 - 4/13/2018 Identified trends and analysis
- 4/13/2018 - 4/27/2018 Created final report
- 4/27/2018 Submitted final report

C. Detailed Plan

1) Data Collection: After meeting with our technical director, we surveyed academic journals searching for any existing research on the topic. We also reviewed sample legislation, taking note of the metadata provided in the legislation and determining how this data could best be recorded in our database.

After developing a tool for recording pertinent information from state websites, we divided the workload of data collection and started gathering our information.

2) Finding and classifying a bill: Each researcher examined digital archives to look for proposed legislation relating to cyber security. As stated before, each state usually had a digital archive of bills the researcher can look through using a keyword search. Once that location had been exhausted, secondary locations were searched. For each policy found, a certain amount of metadata was located within the policy and recorded. This included the following data:

- Researcher's name (who found the policy)
- Location it belongs to (1 of 50 states, Washington D.C., or the U.S. Congress)
- Type of policy (see classifications below)
- Bill name and/or number
- Source (where the bill can be found)

The included classifications below:

- Government Service
- Finance
- Defense
- Energy
- Water/Wastewater
- Communications
- Healthcare
- Elections
- Economic Development
- Workforce Development
- Personal Identifiable Information
- Public Awareness and Training
- Education
- Emergency Services and Exercise
- Cyber Sharing
- Cyber Organizations (Center)
- Cyber Pre-Thru Post Incident
- Legal/Insurance
- Local Government
- Other critical infrastructure

These classifications were originally the 20 groups that make up the Indiana Executive Council on Cybersecurity and provided an easy way for the end user to reference trends and policies when using the final document as reference. The groups were fine-tuned by the technical director to provide an easier form of classification and more usability.

3) Locating alternative sources for research: Data from primary online sources comprised the bulk of the information collected for the trends analysis. Most states provided some type of searchable archive. However, in cases where such databases were not available, the researchers utilized second party databases to collect policy information. These second party databases included sites such as *Find Law* and *Legiscan*.

4) Creating a collaborative database: While many tools were available for storing and managing our research, we sought one that would allow us to collaborate seamlessly and would allow us to share our data with end users without requiring specialized software or paid licensing. We also sought a product that was versatile enough to allow for linking fields together and even sharing data from one table to another. The tool also needed to have several sorting and filtering options. We found an online product called Airtable to meet our needs [11].

After deciding on a tool, we then had to finetune our database design. We listed the necessary fields and then organized them in a logical way to streamline the data entry process.

5) Importing Database Information: We formatted our information to prepare it for analysis. While reading the bills, the following information was collected in the database:

- Bill number
- State
- Type of policy
- Type of legislation
- Originator (senate, house, joint, or governor's office)
- Year introduced
- Status
- Link to online source
- Related legislation

- Description
- Political party affiliation
- Bill sponsor
- Link to vote count information

6) Trend Analysis: Our next step was to begin the preliminary analysis of our data.

a) By State: Each state had its own cybersecurity policies. The number of each classification for every state was analyzed to discover what was most important to that state. We also made an effort to determine states that were currently active in developing cybersecurity programs.

b) Vetoed Bills: Some states, while successful in passing legislation in the house and senate, failed to garner the support of the state's governor. Since the reasons for such occurrences could be valuable, we wanted to analyze these instances.

c) Failed Legislation: If a certain classification had a high number of bills written but the bills did not pass to become policies, then it can be inferred, while enough people thought the bill would be a good idea, an even greater number of people had negative thoughts about the bill to keep it from passing. This trend was explored to find out why.

d) Influence of Federal Legislation: While states are responsible for crafting their own legislation, we wished to determine if the federal government's actions played a role in determining when and what cybersecurity topics were addressed on the state level.

e) Cybersecurity Pioneers: Cybersecurity is more of a priority for some states than others. By examining the progression of cybersecurity legislation by state per year, patterns showing states who exhibited steady policy creation were evidenced. The states showing consistent policy creation over time were determined to be cybersecurity pioneers.

f) Bipartisan Policy Creation: One of our primary goals in our trends analysis was to determine factors that played a role in the successful passage of legislation. This included the success of a political party in getting a bill adopted. As data collection progressed, it became evident that bipartisan efforts garnered different results than partisan efforts.

7) Analysis of Results: After the trends were examined, then the following questions were addressed.

- Are there states that could be considered pioneers to cybersecurity legislation?
- To what degree does the federal government's actions influence state legislation?
- Are there paths that a bill takes that influences its success?

IV. RESULTS

We identified 500 pieces of legislation relevant to cybersecurity within our eight year sample size. We surveyed 454 policies from all fifty states and Washington, D.C., as well as an additional 46 policies from the federal government.

A. States Currently Active in Passing Cybersecurity Legislation

In order to determine which states are actively developing their cybersecurity program, all 50 states were examined and the number of policies by year were recorded by state, as shown in Figure 1.

Looking at the state policy by year, it was apparent that most states had between 1-10 cyber security policies. There were seven out of fifty states that had 20 or more policies.

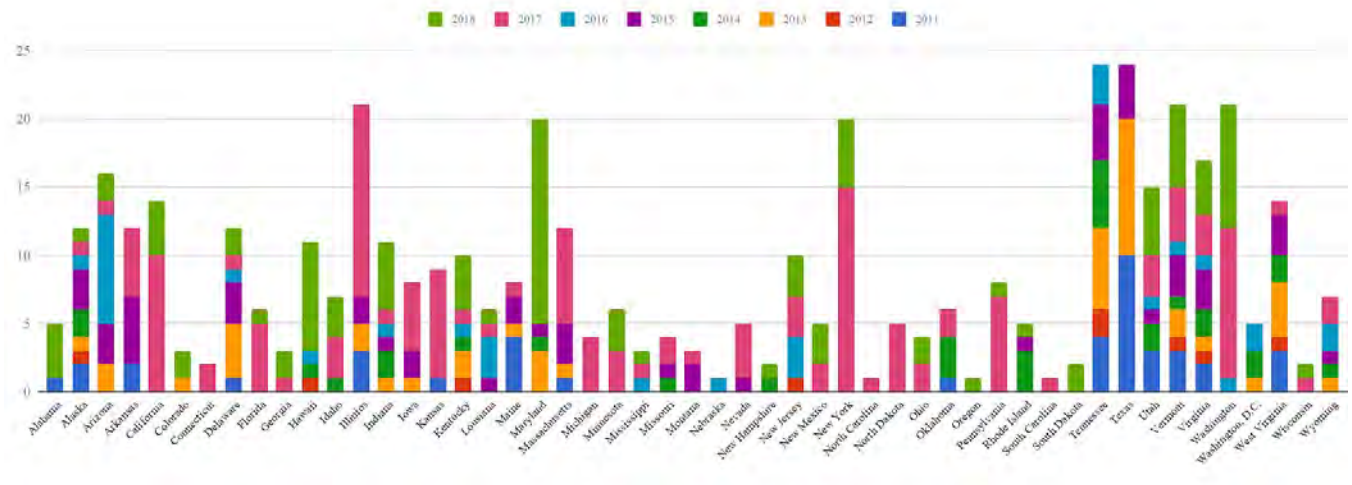


Figure 1. The quantity of policies developed by each state per year between 2011 and 2018.

The dates of the policies were also important. If most policies were proposed before 2016, then the state would not be considered as developing their cybersecurity program. Of the seven states with a large range of policies, only four states created most of their policies from 2016 until now. The four states are Illinois, Maryland, New York, and Vermont.

States with High Number of Policies 2016 - 2018				
Policy Type	**IL**	**MD**	**NY**	**VT**
Communications			5	3
Cyber Organizations	2	1	5	
Cyber Pre Through Post Incident	1	1		5
Cyber Sharing	1	1	3	
Defense		2		
Economic Development		5	5	1
Education	2	3	4	
Elections	1	2	1	
Emergency Services and Exercises			5	
Energy		1	3	3
Finance	1	2		
Government Services	3	2	3	4
Healthcare			1	
Legal/Insurance	3	3	7	5
Local Government	2		2	
Other Critical Infrastructure	1		1	
Personal Identifiable Information			3	4
Public Awareness and Training	1	1	5	
Water/Wastewater			2	
Workforce Development	2	5		
	20	29	55	25

Table 1. The quantity policies and their types that were passed between 2016 and 2018 in the states with the highest surveyed volume.

While a single policy can have multiple policy types, it is still worthwhile to look at the number for each type. Illinois, New York, and Vermont had a high number of legal/insurance policies which would support the argument that most of the new policies being created by developing states were of the type legal/insurance. Vermont also had a high number of government service policies, especially in 2018. Figure 1 shows these two states have a high number of policies spread out over the whole sampling period (2011-2018).

B. Vetoed Bills

In five instances, proposed legislation made it through both the senate and the house; however, the legislation failed to be finalized by a state's governor.

Two of the bills were vetoed by California governor Edmund G. Brown, Jr. Both were introduced in 2017 and were unanimously passed by the state's assembly and senate. Bill AB1306 detailed the scope of the California Cybersecurity Integration Center, which was established by Governor Brown's executive order in 2015 [12]. Brown, in his Governor's Veto Message, expressed concern "that placing the Center in statute as this bill proposes to do, will unduly limit the Center's flexibility as it pursues its mission to protect the state against cyberattacks" [13]. As for vetoed bill AB531, which required the department of technology's office of information security to evaluate existing security policies and develop plans to address deficiencies, Brown stated that the bill's objectives were already required by AB 670 [14].

A bill was vetoed by Governor Susana Martinez from New Mexico. It received 36 to 3 majority votes of support in the state's senate and 37 to 5 majority votes of support in the state's house. HB 364, while dealing primarily with limiting the prescription of contact lenses and glasses, did deal with cyber security by restricting a resident's access to online services. Martinez stated in her House Executive Message No. 57 that the bill limited the use of emerging technologies related to the issuance of contact lenses and glasses [15]. She cited this as the reason she chose to veto the bill.

The other two bills were vetoed by Governor Douglas Ducey of Arizona. Bill SB1434 was vetoed in 2016 after receiving unanimous votes from both the senate and the house. The governor indicated that he vetoed the bill, which dealt with consolidated purchasing and shared services of technology, stating he felt the bill added an extra layer of bureaucracy [16]. HB2566, dealing with password policy, encryption standards, and data security, was vetoed in 2015. It had passed the senate with a vote count of 17 to 11 and passed the house with a vote count of 56 to 1. Ducey stated that his administration had already addressed the concerns outlined in the bill [17].

C. Failed Legislation

Figure 2 shows the twenty classifications used to identify bills and the status count of the policies classification. Although a policy can have multiple classifications, this explores the number of times a classification has a relation to a legislation record.

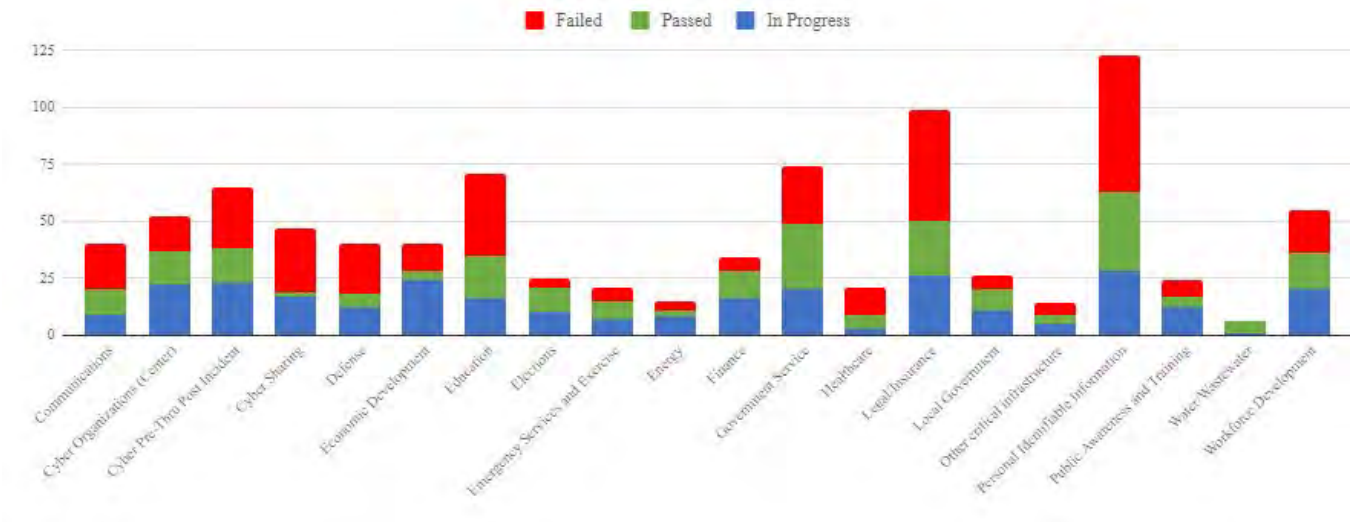


Figure 2. The quantity of each policy type surveyed that is either still in process, was passed into law, or was failed for any reason.

The label "In Progress" are for classifications that are identified to be introduced and still up for discussion, and "Failed" are bills that are inactive, died in chamber, died in committee, or vetoed.

Of the twenty classification types used to identify the bills, most classification types tended to have more failed policies than passed bills. We identified that legislation related to Cyber Sharing, Economic Development, and Education have much higher failure rates than the other classifications. The seven classifications that were an exception include: policies dealing with cyber organizations, elections, emergency services and exercise, finance, government service, local government, and water/waste-water. Furthermore, policies that were related to Elections and Water/Wastewater have greater rates of success than the other classifications. Notably, out of the six state legislations dealing with Water/Wastewater, five were passed successfully, one remains in progress, and zero failed.

D. Influence of Federal Legislation

Figure 3 separates the federal legislation from the state legislation and shows the percentage each topic was covered in bills introduced at those levels within a time frame. In this figure, our eight year sample size was divided into two seperate four year periods to show some slight changes in policy creation.

Much of the federal legislation from the U.S. Congress is focused on Defense, Cyber Pre-through-Post Incident, and

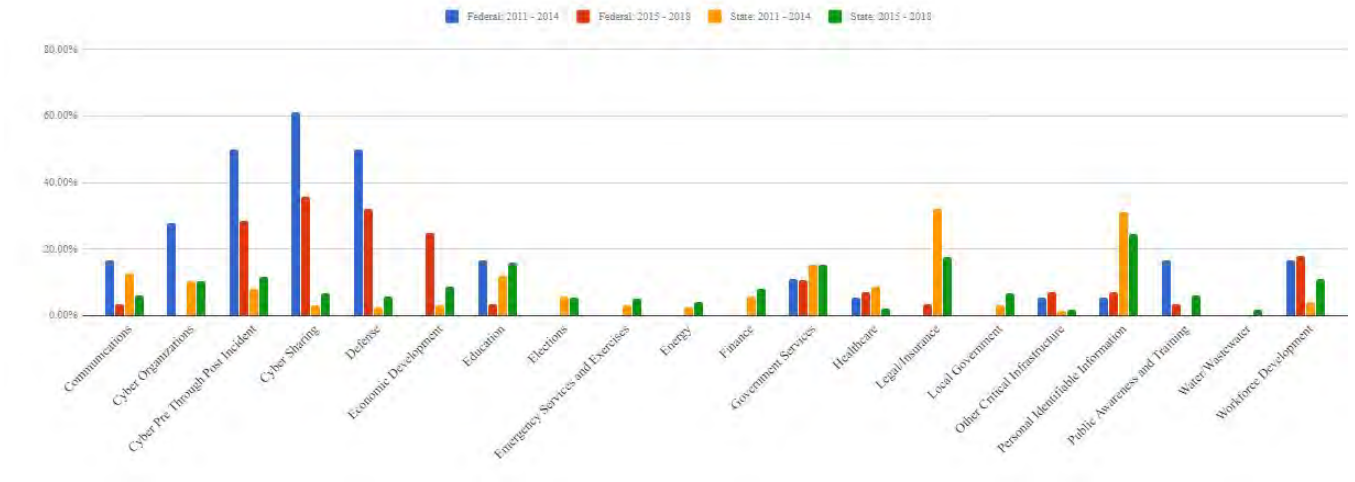


Figure 3. The percentage of state and federal policies introduced in 4 year periods (2011-2014, and 2015-18) that deal each surveyed category.

in Cyber Sharing between organizations. Federal legislation in those categories are consistently higher than all other categories surveyed since 2011. For example, from 2011 to 2014, 61.1% of the federal legislation survey dealt at least some with Cyber Sharing. While those topics were addressed by some at the state level, our data does not show them being addressed by a large amount of states until 2017. Federal legislation appears to be driving state legislation to fill in the gaps where there are security concerns not addressed by the U.S. Congress at all.

In contrast to the federal legislation, state legislation heavily focused on topics such as Education, Personally Identifiable Information, Government Services, Legal/Insurance concerns such as defining cyber security crimes. These were topics that the U.S. Congress did not have many pieces of legislation on at all.

E. Cybersecurity Pioneers

Table 1 shows the number of policies when grouped by state and year. When analyzing the states and the number of policies they have proposed, it is easy to see that most states are not creating new policies. Of the 50 states, only 16 of them have at least 10 new policies since 2011. We used 10 policies as a cut off point since 10 policies provides enough sampling to determine the regularity of policy creation. Pioneering states were Alaska(12), Arizona(16), California(14), Delaware(12), Hawaii(11), Illinois(21), Indiana(11), Maryland(20), Massachusetts(12), New York(20), Tennessee(24), Texas(24), Vermont(21), Virginia(21) Washington(21), and West Virginia(14) These states appear to be in 3 different classifications.

1) Early policy creation; however the state has not produced much legislation of late: In this category, the state created several policies earlier than 2014 and then less after 2014. These states have dropped in their proactive approach to cybersecurity and are not considered as pioneers. For example, Texas created the first bills for various types of policy. While creating several of bills early on, they have not been active in bill creation since 2015. The states of Tennessee, Texas, and West Virginia meet this criteria. Even though their number of policies are high, their concern for cybersecurity seems to have lessened.

2) Large policy creation; however, most of the policies have been created over the last 3 years: This grouping shows states that have created most of their cyber security policies over the past 3 years (2016-2018). These states, while recently producing more legislation, did not have the early policy adoption to be considered pioneers. Arizona, California, Delaware, Hawaii, Illinois, Indiana, Maryland, Massachusetts, New York, and Washington match this criteria. The higher policy producers worth nothing are Maryland (15 policies in 2018 alone), New York (20 policies in the past two years), and Washington (20 policies in the past two years also).

3) Steady policy creation: These high-producing policy creators consistently created bills over the sample years (2011-2018). As they consistently produced more cyber security policies than other states over the same sample time, it would suggest the states were pioneers in cybersecurity policy creation and not as reactive to other states through the years. As Figure 1 “Number of Policies by State per Year” shows, Alaska, Vermont and Virginia are the only states that match this criteria. Vermont has the most policies at 21 followed by Virginia at 17. Alaska did not have near as many with 12.

F. Bipartisan Success

Of the 454 examples of state level cybersecurity legislation found, 109 records were bipartisan attempts. Of those attempts, 29 pieces of joint legislation were listed as actively being considered, meaning the outcome of the legislation was yet to be determined, and 45 of the bills that were introduced passed. When excluding legislation in progress, the resulting bipartisan success rate was 56%. In addition to bipartisan efforts, there were 5 records introduced by council, with all 5 passing. This success rate is significantly higher than partisan sponsored cybersecurity legislation on the state level, where, of the bills that were no longer actively being considered, only 88 passed, indicating a success rate of 40% (see Figure 4).

Cybersecurity topics that garnered the most state level bipartisan sponsorship included those relating to personal identifiable information (22 records), government services (19 records), legal (17 records), and cyber pre through post incident (16 records). There were no examples of bipartisan sponsorship relating to general policies.

Idaho and Kansas were the two states with the most bipartisan sponsored legislation, both having 7 records with bipartisan support. Iowa, Texas, Washington, and Wyoming also were close in this category, having 6 instances each of utilizing bipartisan sponsorship for cybersecurity legislation. States with no bipartisan support of cybersecurity legislation included Arkansas, California, Georgia, Louisiana, Missouri, Montana, New Mexico, New York, North Carolina, Oklahoma, and Wisconsin. Washington, D.C., also had no records in this area.

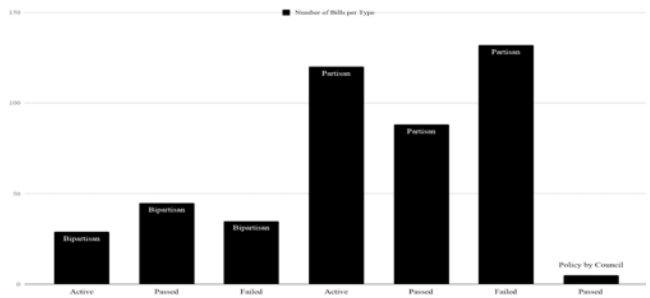


Figure 4. Success of state level bipartisan legislation attempts as opposed to partisan legislation attempts.

This data is being stored at the following link using Airtable. Please follow the link below to view the tool [11].

https://airtable.com/shrCcYzKJGH1jyvrx

V. Challenges

A. Varying Terminology

One problem with our research was how verbiage varied from state to state. For example, one state might choose to use the term *cyber security*, while other states might use terms such as *computer crime* or *online security.* To ensure that each state was researched thoroughly and consistently, the researchers agreed on a list of keywords to use in their search.

B. Determining Relevance

Also, the relevance of the proposed legislation to the targeted analysis data was also a challenge. Desired topics were often buried deep within unrelated information, resulting in researchers having to read and index bills that were, at first glance, not relevant to the desired data set.

C. Tracing a Bill's Origin

Another problem dealt with how bills are created. At times a bill originates in the house, and at other times it can be created in the senate. Bill numbers vary depending on the origin, and they can actually compete with each other. Also, a bill will stall in a committee, or the current legislature may elect not to take up a discussion on the bill. A new bill can be created the following year in order to try to create the policy. These bills must be linked in the research to provide a good picture on policy creation.

Oftentimes a generic bill will pass and become policy. After passing the first bill, a second bill will revise the original policy to provide clarification or additional direction. The original bill and the following bills must be linked in the research also.

VI. Conclusion

Excluding federal legislation and active legislation, we found 305 examples of state level legislation relating to cyber security. Of those, 138 records passed and 167 failed or were determined to be inactive, demonstrating a success rate of 45%.

Policies concerning elections and water/wastewater had higher success rates than other classifications. Policy topics that exhibited higher than average failure rates were related to cyber sharing, economic development, and education.

During the time period sampled, there seemed to be little correlation between federal cybersecurity policy efforts and those of the states. If fact, the two entities tended to complement each other, with federal policy having a much different focus than the states. For example, federal policies dealt more with defense, while state policies dealt more with education.

States showing consistent push in cybersecurity legislation were Vermont and Virginia. These states created policy steadily over the time period and met the criteria to be considered pioneers in cybersecurity legislation.

We determined that one factor that seemed to increase a piece of legislation's chance of success was the willingness of legislators to cross party lines in initiating new legislation. Bipartisan bills had a success rate of 56%, while bills introduced along party lines only had a success rate of 40%. Popular bipartisan topics included personal identifiable information, government services, legal, and cyber pre through post incident. When compared to the overall success rate of 45%. It is evident that bipartisan support is a favorable predictor of a bill's chance of passage.

VII. Future Work

In order for the research to continue to be useful, it is critical that the database be maintained. As new cybersecurity related legislation is proposed and considered, it should be catalogued in the base. By keeping the database current, the picture of national cybersecurity trends will become more granular, and the increased data will allow for better trend analysis.

Additionally, it would be beneficial for future researchers to expand the research by correlating the passage of legislation to related major cyber events. For example, researchers could determine if the Equifax breach resulted in an increase of proposed legislation related to personally identifiable information. If a correlation is evident, this could serve as a predictor of future proposed legislation.

Researchers could also attempt to measure the impact of key successful legislation. An example of this future work could be in the area of workforce development. Researchers could ascertain if states that adopted workforce development legislation have seen an increase in available professionals.

Furthermore, a thorough examination of failed legislation would aid legislators when crafting legislation. By surveying bill sponsors, researchers could identify key barriers to cybersecurity legislation, allowing policy makers the ability to better craft and propose bills. Also, researchers could compare failed legislation from one state to similar successful legislation in another state to determine why similar legislation failed in one state but found success in another.

References

[1] National Governors Association, *Meet the threat: A compact to improve State Cybersecurity*, 2017. [Online]. Available:

https://www.in.gov/cybersecurity/files/NGA%20Cyber%20Compact.pdf
[2] Holcomb, Eric J., "Exec. Order No. 17-11. Continuing the Indiana Executive Council on cybersecurity." *State of Indiana Executive Department*. Jan. 9, 2017. [Online]. Available: http://www.in.gov/gov/files/EO_17-11.pdf
[3] Lowry, C., "What's in your mobile wallet? An analysis of trends in mobile payments and regulation," *Federal Communications Law Journal*, vol. 68, no. 2, pp. 353-384, 2016. [Online]. Available: http://bi.galegroup.com.elib.uah.edu/essentials/article/GALE%7CA493323880/d7c701a94f8c8d9685b93203add71fee?u=avl_uah
[4] Sales, N. A., "Regulating cyber-security," *Northwestern University Law Review*, vol. 107, no. 4, pp. 1503-1568, 2013.
[5] Clarke, R., "War From Cyberspace," *The National Interest*, vol. 104, pp. 31-36. 2009. [Online]. Available: http://www.jstor.org.elib.uah.edu/stable/42897693
[6] Glennon, M. J. "State-level cybersecurity," *Policy Review,* vol. 171, pp. 85-102, 2012.
[7] Bosch, C., "Securing the smart grid: Protecting national security and privacy through mandatory, enforceable interoperability standards," *Fordham Urban Law Journal*, vol. 41, no.4, pp. 1349-1406, 2014.
[8] Schneider, F., "Impediments with policy interventions to foster cybersecurity," *Communications of the ACM,* vol. 61, no.3, pp. 36-38, March 2018.
[9] Godara, S., "Role of 'intermediaries' in the cyber world: a comparative study of the legislative policies & recent judicial trends," *VIDHIGYA: The Journal Of Legal Awareness*, vol. 8, no. 1, pp. 69-80, 2013.
[10] Bulger, M., Burton, P., O'Neill, B., and Staksrud, E., "Where policy and practice collide: Comparing United States, South African and European Union approaches to protecting children online," *New Media & Society*, vol. 19, no. 5, pp. 750-764. 2017.
[11] Brown, Edmund G. Jr., "Exec. Order No. B-34-15 (2015). Establishing the California Cybersecurity Integration Center," *CA.Gov*, 2015. [Online]. Available: https://www.gov.ca.gov/2015/08/31/news19083/
[12] "State of Cybersecurity," *Airtable* [Online]. Available: https://airtable.com/shrCcYzKJGH1jyvrx
[13] Brown, Edmund G. Jr., "Governor's Veto Message," *California Legislative Information*, Oct. 11, 2017. [Online]. Available: http://leginfo.legislature.ca.gov/faces/billStatusClient.xhtml?bill_id=201720180AB1306
[14] Brown, Edmund G. Jr., "Governor's Veto Message," *California Legislative Information*, Oct. 14, 2017. [Online]. Available: http://leginfo.legislature.ca.gov/faces/billStatusClient.xhtml?bill_id=201720180AB531
[15] Martinez, Susana, "House Executive Message No. 57," *New Mexico Secretary of State*, Apr. 7, 2017. [Online]. Available: http://sos.state.nm.us/uploads/files/HB364-2017-Vetoed.pdf
[16] Ducey, Douglas A., "Re:Senate Bill 1434," *Office of the Governor*, May 18, 2016. [Online]. Available: https://azgovernor.gov/sites/default/files/sb_1434_veto_letter.pdf
[17] Ducey, Douglas A., "RE: House Bill 2566," *Arizona State Legislature*, Apr. 9, 2015. [Online]. Available: https://www.azleg.gov/govlettr/52leg/1R/HB2566.pdf

TEAM INFORMATION

A. Biographical Sketches

Adam Alexander received his B.S degree in computer science from William Paterson University in Wayne, NJ in 2012. He holds a current Security+ certification. He is in his second year at the University of Alabama in Huntsville (UAH) pursuing a Master of Cybersecurity: Computer Science Track and is set to graduate in May of 2018. Alexander worked for one year as a systems administrator at a software company called Advent. The following three years were spent at MFX Fairfax working as computer technician and eventually being promoted to VDI technician. He has recently interned for TSMO's Army Red team and has participated in several Pen-testing operations.

Paul Graham received his B.S.B.A. degree in management from UAH in 2010. He holds current Security+ and Network+ certifications. He is pursuing a Master of Cybersecurity: Business Track and is set to graduate in May of 2018. Over the last seven years, Graham has worked as a government contractor for the D.O.D. Missile Defense Agency (MDA) in various IT positions. For the last two years, he has been a network design and implementation engineer and collaborated on solutions to improve the MDA's network security posture enterprise-wide. For three years before that, he provided account administration for multiple network domains.

Eric Jackson received his B.S. degree in Computer Science/Software Engineering from the University of Central Florida (UCF) in 2001. He holds a current Security+ certification as well as multiple certifications from Microsoft including Developer of Web Applications, Application Lifecycle Management, and SQL server. He is pursuing a Master of Cybersecurity from UAH with an emphasis on Computer Science.

Jackson worked for a government contractor in Florida for seven years developing simulators for the military. In 2008 he moved to Alabama and has worked as a contractor for NASA since. He is the development team lead, and his duties range from mentoring, server management (IIS), software development/architecture, and interacting with the

customers and government representatives. For the past several years, security has taken a more prevalent role in development. He is responsible for navigating policies, mitigating security scans, and providing a solid framework for use security in the applications.

Bryant Johnson received his B.S. degree in Computer Engineering from UAH in 2016. He also holds a current Security+ certification. He is a CyberCorps: Scholarship for Service student pursuing a Master's in Cybersecurity: Computer Engineering Track at UAH. His experience includes electronics, computer hardware, networking, software design and development.

Currently, Johnson works as a government civilian Computer Engineer for the Aviation and Missile Research, Development, and Engineering Center (AMRDEC) in Huntsville, Alabama, where he performs failure analysis on integrated circuits.

Tania Williams received her B.S. degree in English and professional writing from the University of North Alabama (UNA) in 1994, her Master of Education degree from UNA in 2000, and her Education Specialist Degree in Teacher Leader from UNA in 2015. She is currently pursuing a Master of Cybersecurity from UAH and holds a current Security+ certification.

Williams works for UAH's Center for Cybersecurity Research and Education as a research scientist assisting with the development of cybersecurity curriculum for various cybersecurity camps, including camps at the US Space and Rocket Center (US Cyber) and at UAH (GenCyber). She also is a teacher at Lauderdale County High School, where she teaches cybersecurity, robotics, and English. She is a CyberPatriot coach, a recent Teacher of the Year recipient, and a Fund for Teachers Fellow. Additionally, she has experience teaching on the college level, having served as an associate professor at Northwest Shoals Community college and Faulkner University.

B. Team Tasking

Team members assumed multiple roles to successfully achieve the goals of the project; regular communication of the project's goals was required from all member. Duties included providing expertise, completing deliverables, and documenting the process. While specific tasks varied throughout the course, each person contributed to the overall project objectives by following the outlined detailed plan on assigned datasets:

- Adam Alexander: Alabama, California, Colorado, Connecticut, Delaware, Florida, Georgia
- Paul Graham: Alaska, Arizona, Arkansas, Delaware, Hawaii, Idaho, Indiana, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, U.S. Congress
- Eric Jackson: Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico
- Bryant Johnson: New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota
- Tania Williams: Tennessee, Texas, Utah, Vermont, Virginia, Washington, West Virginia, Wisconsin, Wyoming, Washington D.C.

Notably, individuals performed tasks and filled extra roles where responsibility was not specifically dictated. Eric Jackson and Adam Alexander assumed the role of liaisons to the technical director and communicated progress/objectives to the course professor. Tania Williams led the documentation effort, performed the literature review, and established the collaborative database. Paul Graham and Bryant Johnson supported the document review, data management, and analysis.