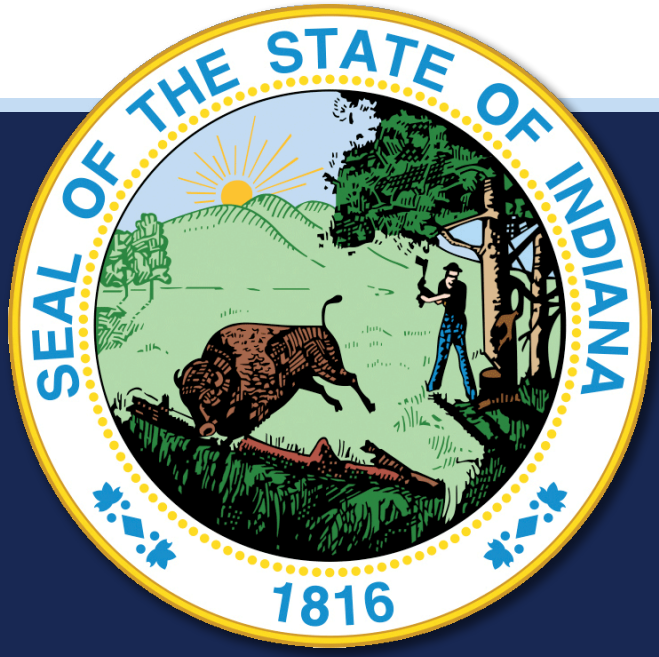
INDIANA
CYBERSECURITY STRATEGIC PLAN



September 2018

September 21, 2018

The Honorable Eric J. Holcomb
Governor, State of Indiana
State House, Room 206
Indianapolis, Indiana 46204

Dear Governor Holcomb:

As Indiana's Executive Council on Cybersecurity embarked on taking cybersecurity to the Next Level since your launch in July 2017, it quickly became evident that we had members who not only met the challenge, but exceeded all expectations. It has been an honor to lead such a passionate, expert Council, which has positioned Indiana to have a comprehensive and deep understanding of matters pertaining to cybersecurity.

The efforts of your Council and its first-of-its-kind strategic approach has fostered significant progress in Indiana's cybersecurity planning initiatives. In fact, in the first year the Council already has completed 27.5 percent of its 69 identified deliverables, and 31.6 percent of the stated objectives.

This was not completed by one entity alone. By working collaboratively, Indiana will establish long-term protection strategies that will provide Hoosier residents and businesses with the knowledge and infrastructure needed to be safer from the ever-evolving cyber threats.

As many of the deliverables are being developed and executed by the state and partners, the Council asks for your continued leadership in:

- Supporting of a statewide cybersecurity public relations and awareness campaign;
- Encouraging the highest-level technical and administrative cybersecurity best practices and standards be followed;
- Supporting policy that will boost the cybersecurity posture of Indiana;
- Providing appropriate support to the critical infrastructures as they move forward with their many deliverables;
- Encouraging all of Indiana's workforce ecosystem to follow national standards and develop the cybersecurity pipeline;
- Developing local law enforcement and emergency management in their knowledge to best respond and recover from a cyberattack; and
- Supporting the Council as it moves forward, including ensuring its membership matches the needs of the state.

The following *Indiana Cybersecurity Strategic Plan* encompasses not only the breadth of topics, but also the depth. While the plan in its entirety is large and comprehensive, it is organized so that specific information regarding specific topics can easily be accessed as needed. Each section can stand alone and readers, based on their interests, can select one or a combination of parts of the plan as they aim to learn and further develop solutions addressing cybersecurity in the state.

We appreciate the opportunity to serve Hoosiers and further posture Indiana's cybersecurity strategy, and we look forward to continuing our efforts to supporting the mission of taking cybersecurity to the Next Level.

Sincerely,

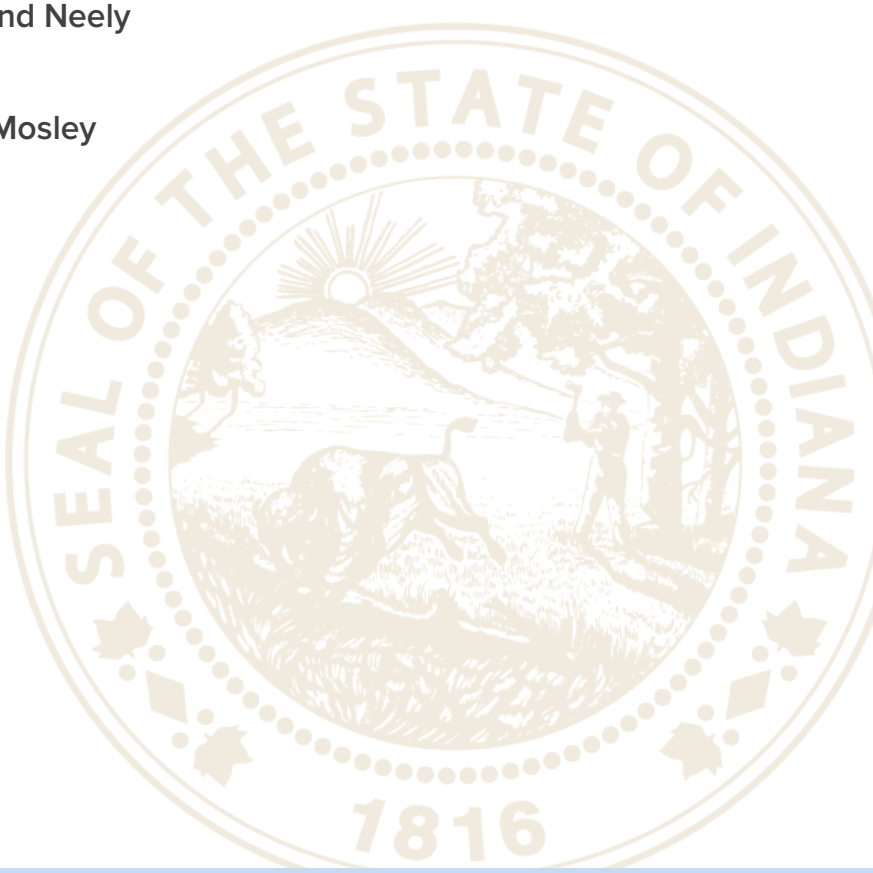
Executive Director Bryan Langley
Indiana Department of Homeland Security

Superintendent Doug Carter
Indiana State Police

Adjutant Major General Courtney Carr
Indiana National Guard

Chief Information Officer and Director Dewand Neely
Indiana Office of Technology

Cybersecurity Program Director Chetrice L. Mosley
State of Indiana



INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY

2018 Voting Members

Senior Operations Director Samuel Hyer, Office of Governor Eric J. Holcomb

Chief of Staff Tracy Barnes, Office of Lt. Governor Suzanne Crouch

Executive Director Bryan Langley, Indiana Department of Homeland Security

Chief Information Officer and Director Dewand Neely, Indiana Office of Technology

Superintendent Douglas Carter, Indiana State Police

Adjutant General MG Courtney Carr, Indiana National Guard

Cybersecurity Program Director Chetrice L. Mosley, State of Indiana

Secretary of State Connie Lawson, State of Indiana

Attorney General Curtis Hill, State of Indiana

Chair James Huston, Indiana Utility Regulatory Commission

Commissioner Teresa Lubbers, Indiana Commission for Higher Education

Commissioner Adam Krupp, Indiana Department of Revenue

Secretary of Commerce Jim Schellinger, Indiana Economic Development Corporation

Commissioner Fred Payne, Indiana Department of Workforce Development

Director Danielle Chrysler, Indiana Office of Defense Development

Information Security Officer Owen LaChat, MutualBank

Executive Director Stephen A. Key, Hoosier State Press Association

Partner Ronald W. Pelletier, Pondurance

Information Technology Vice President John Lucas, Citizens Energy Group

President Mark T. Maassel, Indiana Energy Association

Executive Director Rhonda Cook, Accelerate Indiana Municipalities (AIM)

Executive Director Stephanie Yager, Indiana Association of County Commissioners

Chief Information Officer Mark A. Lantzy, Indiana University Health

Executive Director Joni K. Hart, Indiana Cable Telecommunications Association

Business Manager for IT Security David Ehinger, Rolls Royce

Chief Information Officer Brad Wheeler, Indiana University

Chief Information Officer Gerry McCartney, Purdue University

2018 INDIANA CYBERSECURITY STRATEGIC PLAN

Table of Contents

...continued on next page

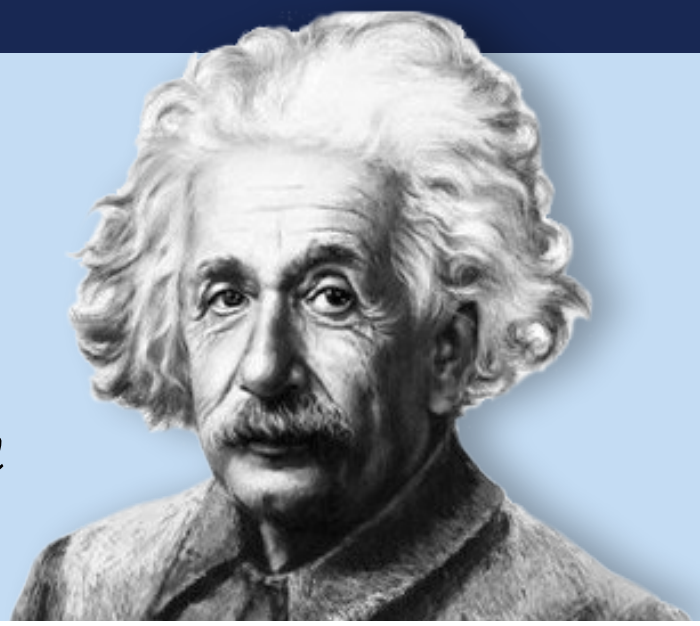
Table of Contents (continued)

APPENDICES (continued)

ABOUT THIS PLAN

"Out of clutter, find simplicity."

-Albert Einstein



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. This has been a key element in determining not only where Indiana's past and current cybersecurity efforts are, but also where the state will go next.

The *Indiana Cybersecurity Strategic Plan* outlines those directions as simply and as directly as the complexity of the effort allows.

This plan is organized into three sections: the Framework, in which the Indiana Executive Council on Cybersecurity (IECC or Council) was built; the detailed Implementation Plans developed by the members; and a Year in Review.

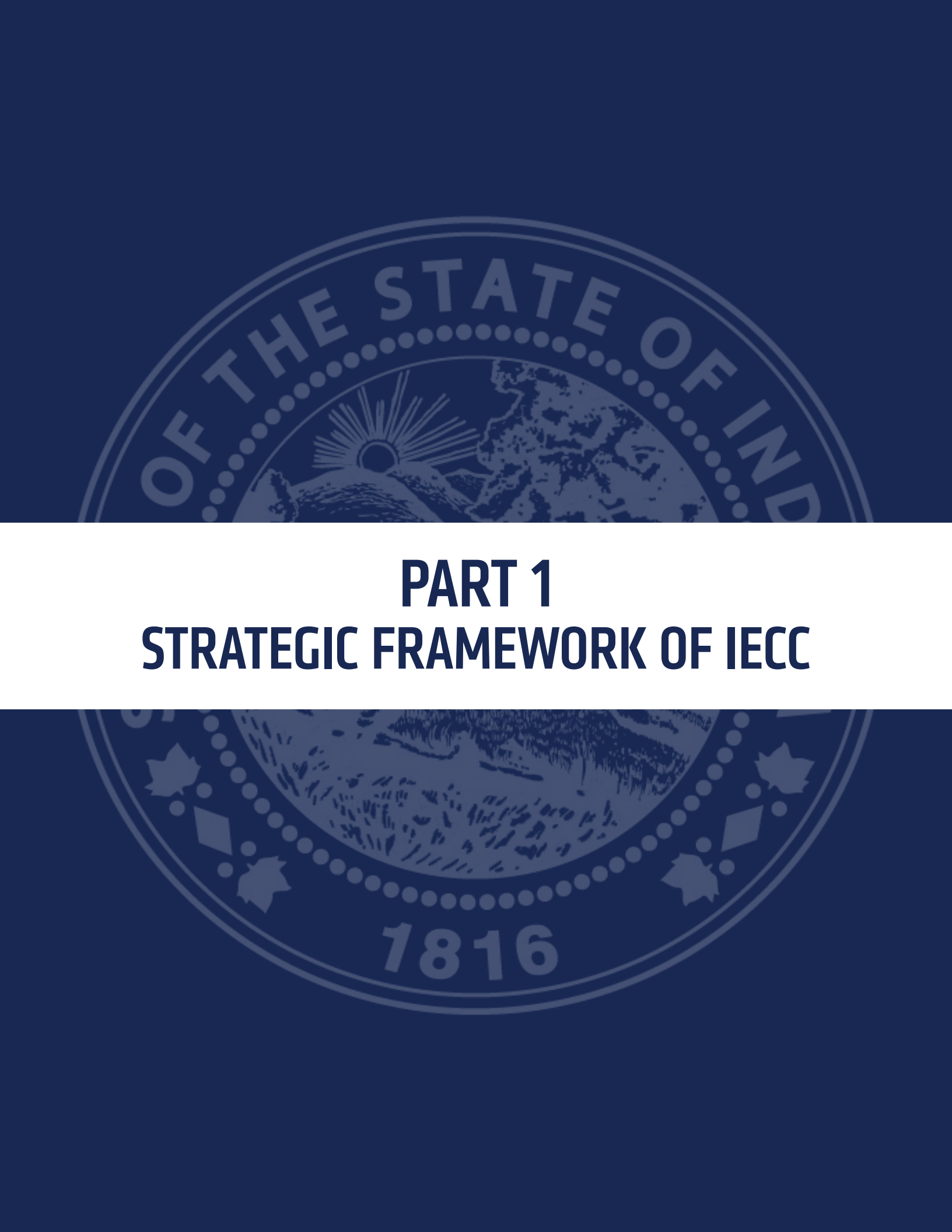
Part One is the Council's strategic framework. It provides the background of the Council, establishes high-level cybersecurity goals, presents the composition of membership, and addresses how it has met the objectives of Indiana Governor Eric J. Holcomb's Executive Order.

Part Two is an executive summary of the implementation plans created by 20 separate committees and working groups, each developed with objectives that are specific, measurable, achievable, and relevant to the overall strategic vision. Additionally, this section contains observations, considerations, and recommendations. Note that each plan is provided in its entirety in the Appendices of this strategic plan.

Part Three presents the 2017-2018 year in review. This section identifies the dedicated members and leaders of the Council who developed these plans, completed deliverables of the first-year plans, contributed to additional accomplishments in Indiana, and advised the Council on how to move forward.

In addition to the aforementioned parts of this plan, the heart of the Indiana Cybersecurity Strategic Plan is Appendix D. These are the 20 detailed implementation plans developed for the respective sectors and areas by the more than 200 members of the Council.

This plan and all the appendices also can be found on www.in.gov/cybersecurity/3842.htm.



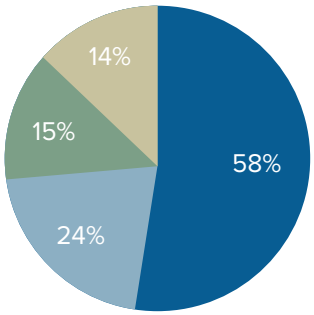
PART 1
STRATEGIC FRAMEWORK OF IECC

TODAY'S CYBER THREAT

Critical infrastructure and key resource sectors rely heavily on information technology to manage complex systems; including public utilities, healthcare, telecommunications, transportation, financial services, manufacturing, education, research, and public safety. The reality of this interconnectivity is that cyber risks grow at an exponential rate and pose a profound risk to citizens, organizations, and industries, as well as threaten the security and economy of Indiana. This is all the more relevant considering the most recent worldwide cyberattacks along with those that have occurred right here in Indiana.

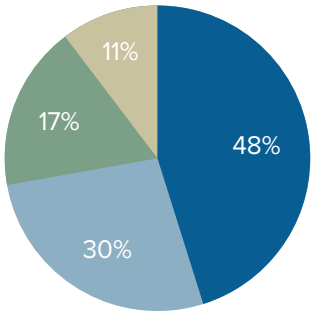
In fact, the 2018 Verizon Data Breach Investigations Report found the victims of breaches to be 58 percent small businesses, 24 percent healthcare organizations, 15 percent accommodation and food services, and 14 percent public sector entities. Of those breaches, 48 percent occurred from hacking, 30 percent included malware, 17 percent were social attacks (such as phishing), and 11 percent involved physical security. Email continues to be the most common method of delivery, accounting for 96 percent of breaches.

2018 BREACH VICTIMS



small businesses
healthcare organizations
accommodation and food services
public sector

2018 BREACH SOURCES



hacking
malware
social attacks (phishing)
physical security

THE SOLUTION

INDIANA'S COMMITMENT TO CYBERSECURITY

As the State of Indiana became more centralized in its information technology, the Indiana Office of Technology began developing its state cyber strategy in two documents: The Cyber Security Framework Strategy (2009) and the Information Security Framework (2013). These documents describe the organization, governance, practices, and policies to be implemented in order to achieve an effective security approach for the state.

Inward focus and inter-agency coordination were intended to protect the state, but more needed to be done to protect the citizens and businesses of Indiana. In August 2015, the Indiana Department of Homeland Security (IDHS) was tasked to conduct additional research and develop a roadmap of how to most effectively collaborate and engage with public and private partners in developing a long-term cyber strategy. This included IDHS leading a first-of-its-kind critical infrastructure tabletop and operational exercise series called Crit-Ex in 2016. This exercise was the first of these cross-sector initiatives (public and private) designed to improve the understanding of Indiana's cyber ecosystem and identify capability gaps. Crit-Ex was planned as a series of exercises that explored the intersection of cybersecurity and critical infrastructure, using scenarios in which a cyberattack on a critical asset leads to physical-world consequences.

The initial phase of Crit-Ex was a six-hour tabletop exercise. The exercise facilitated discussion surrounding the response to a cyberattack resulting in a broad energy disruption, and a myriad of other issues related to the mitigation of such a wide-scale power outage. The tabletop session emphasized the role of local, state, and federal agencies, water/wastewater utilities, and power utilities in response to a coordinated cyber incident that affected the entire State of Indiana.

The second event of the Crit-Ex series was an operational exercise at Indiana National Guard's Muscatatuck Urban Training Center, in which simulated cyberattacks disrupted real-world operational supervisory control and data acquisition (SCADA) systems at a water utility, allowing participants to exercise their cybersecurity response processes. As such, Crit-Ex 2016 was the first-of-its-kind exercise that catalyzed information sharing, training opportunities, partnerships, and response planning across the state.

After this inaugural cyber exercise, it became more evident that securing Indiana's information technology infrastructure and industrial control systems is beyond the reach of any single entity, especially as the nature of the cyber threat came into focus. That is why in March 2016 former-Governor Mike Pence signed an Executive Order establishing the Indiana Executive Council on Cybersecurity (IECC or Council).

The Council was continued on January 9, 2017, through Executive Order 17-11 (See Appendix A), when Governor Eric J. Holcomb took office, with renewed focus on how to build and best utilize the cross-sector body of subject-matter experts to effectively understand Indiana's cyber risk profile, identify priorities, establish a strategic framework of Indiana's cybersecurity initiatives, and leverage the convened talent from all sectors to stay on the forefront of the cyber risk environment.

Per Executive Order 17-11, the Council will:

- Develop, maintain, and execute an implementation plan for accomplishing strategic cybersecurity objectives that are specific, measurable, achievable, and relevant to the overall strategic vision, which shall be completed within an established timeframe.
- Establish and maintain a strategic framework document that defines high-level cybersecurity goals for the State of Indiana. This framework document shall establish a strategic vision for Indiana's cybersecurity initiatives and detail how the state will:
  - 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.
- Receive guidance from the Counter-Terrorism and Security Council, which is led by Indiana's Lt. Governor Suzanne Crouch, and report to the Homeland Security Advisor within the Office of the Governor.

Given the challenges and complexities surrounding the directives of the Executive Order, it became imperative to create a strategic framework that would address both statewide and sector-specific topics within the cybersecurity ecosystem. As a result, the State of Indiana hired its first fully dedicated cybersecurity program director in March 2017 to facilitate the Council in fulfilling its purpose. That purpose is to (1) produce an informed overview of Indiana's cyber risks and opportunities; (2) prioritize those items by criticality; and (3) suggest and/or facilitate the implementation of programs/projects designed to achieve associated objectives.

In July 2017, Governor Holcomb launched Version 2.0 of the Council with a new direction in taking cybersecurity to the Next Level in Indiana.

The Council also provides consultative direction on projects, initiatives, and programs, ensuring whole-of-state needs are met and assets are best leveraged. It confirms that these programs align with the unique needs and risk profiles of critical sectors throughout the state and accelerates cyber initiatives and ensure Indiana's cyber stakeholders have the resources and support they need to reach the objectives in cybersecurity.

COUNCIL STATS

YEAR 1

200+ MEMBERS

19 OF 69 DELIVERABLES COMPLETED

38 OF 120 OBJECTIVES COMPLETED

DEVELOPING THE COUNCIL AND THE STRATEGY

COMPOSITION OF THE COUNCIL

To move forward effectively and efficiently, especially given the broad areas and in-depth expertise on the Council, the members were provided with as much information as possible regarding the expectations, processes, roles, and responsibilities of being selected to be a member of the Council. In September 2017, the Voting Members of the Council passed the official Indiana Executive Council on Cybersecurity Charter. This Charter, found in Appendix B, includes the purpose, roles of members and expectations, appointment terms, membership requirements, meeting guidelines, council duties, the strategic breakout of the IECC, and additional provisions.

DEVELOPMENT OF COMMITTEES

The Council was organized into 20 committees and working groups composed of the more than 200 respective members who are experts in their relative fields (See Figure 1). Developing this cybersecurity ecosystem was the only way to achieve maximum results in a relatively short amount of time, but with the depth of knowledge needed to make informed operational decisions.

The IECC Charter was then used to guide the creation of individual committee and working group charters. Each charter clearly defined its goals, members (full time and as needed), and expectations. Moreover, each committee and working group was comprised of members who represented north, central, and southern Indiana as well as small, medium, and large entities, to ensure that diverse input was provided in developing strategic plans. Every committee and working group was chaired by a Voting Member of the Council to ensure that all plans were aligned with the goals of the entire Council.

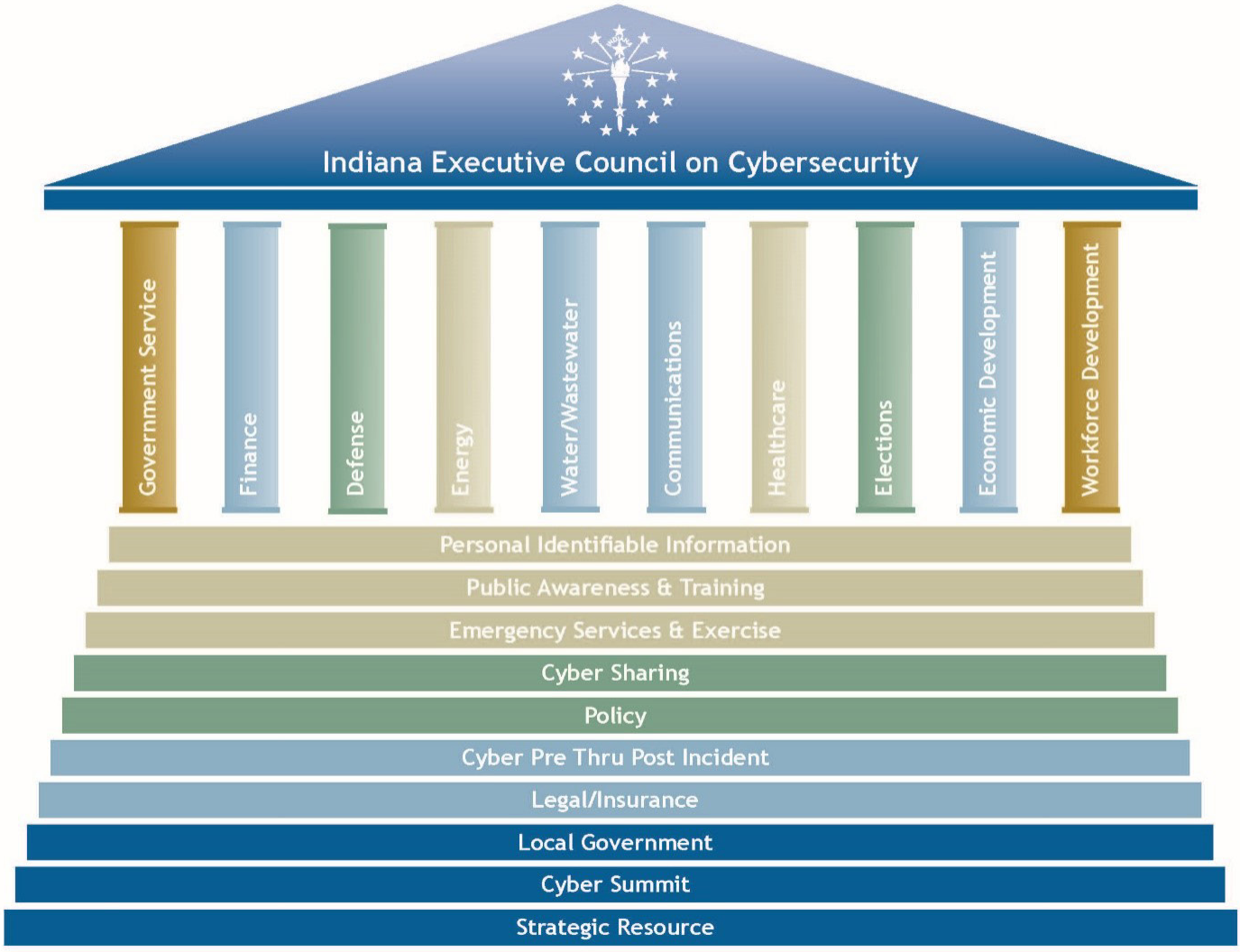


Figure 1 : IECC Strategic Breakdown

THE COUNCIL STRATEGIC PHASES

To guide the work of the 20 committees and working groups in developing a strategic plan, phases were established for each group to follow and complete concurrently. The four key phases were:

Phase 1	Research
Phase 2	Planning
Phase 3	Implementation
Phase 4	Evaluation

PHASE 1 - RESEARCH

Complete questionnaire, primary and/or secondary research

Develop preliminary deliverables and research findings

PHASE 2 - PLANNING

Select and finalize deliverables

Ensure all deliverables tied back to a specific goal of the Executive Order

Develop objectives to drive metrics

PHASE 3 - IMPLEMENTATION

Indicate further details of each deliverable including budget, tactics, resources, timeline, pilot/example products, etc.

PHASE 4 - EVALUATION

Determine the objectives of each deliverable, and methods of evaluating

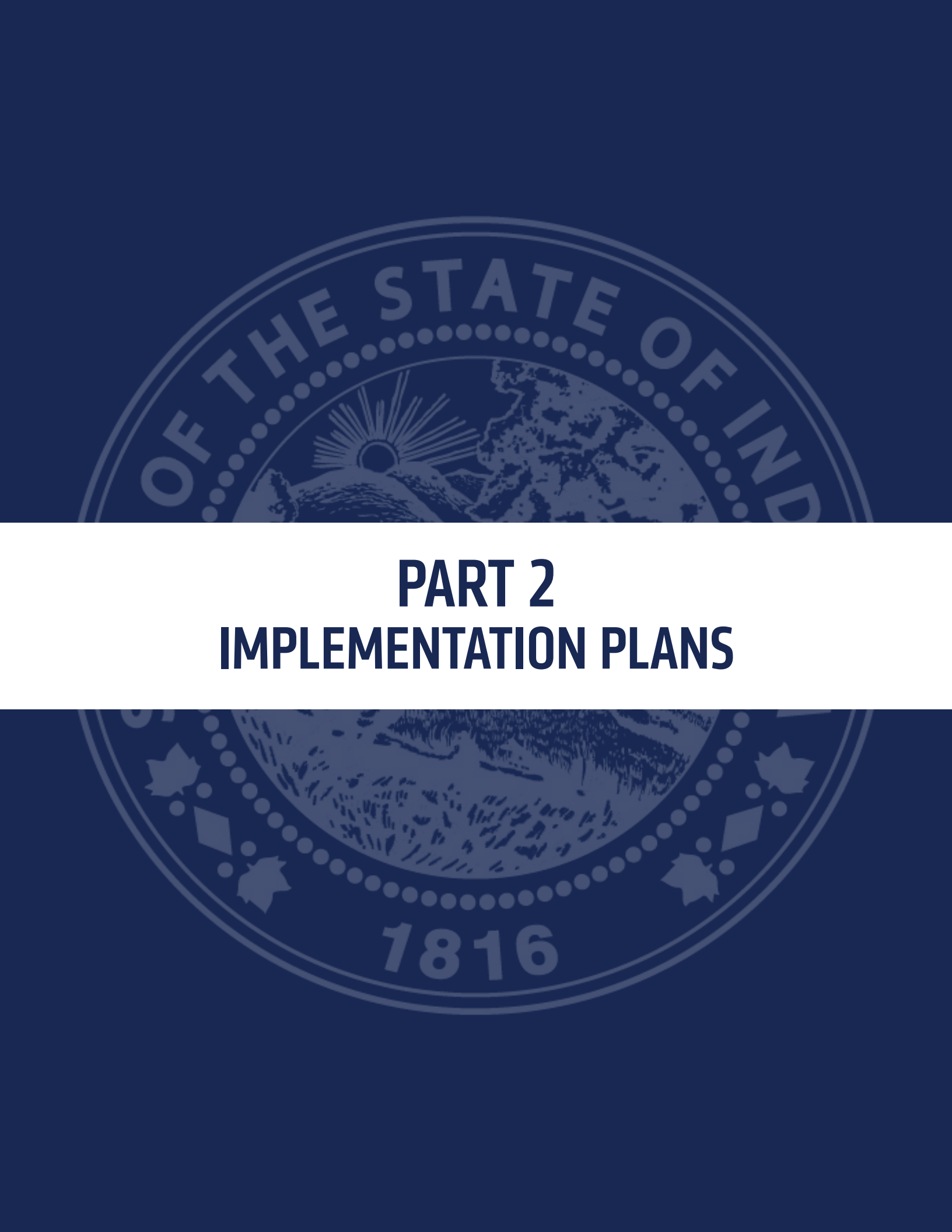
In addition, meetings, facilitated discussions, director oversight, shared online platforms, and tools, were implemented to avoid duplication of developments and deliverables, and to allow for a fully transparent process. This included a consolidated Q&A forum document that was used within and across the 20 committees and working groups to best and most effectively facilitate communications. For the templates used to assist with each Phase of the committees and working groups, see Appendix C.

EXECUTIVE ORDER COMPLETION

Executive Order (EO) 17-11 provided clear direction for the Council's focus in the coming years. Table 1 (following page) indicates the specific deliverables established within the Governor's Executive Order, the primary owners responsible for completing the requirements, as well as the month in which the performance measure was satisfied.

Table 1 : Governor's Executive Order Deliverables

EXECUTIVE ORDER REQUIREMENT	PRIMARY OWNER(S)	PERFORMANCE MEASURE
Continuance of Council and membership composition met. (EO Sections 1-5)	Indiana Department of Homeland Security, Indiana State Police, Indiana Office of Technology, Indiana National Guard, and Indiana Cybersecurity Program Director	July 2017 – Governor Holcomb and leadership launch Version 2.0 of Council with required membership.
Establish and maintain a strategic framework document that defines high-level cybersecurity goals for the state. This framework document shall establish a strategic vision for state cybersecurity initiatives and detail how the state will meet seven specific goals. (Section 6)	Indiana Cybersecurity Program Director and Voting Members of Council	September 2017 – Passed IECC Charter September 2018 – Submitted final strategic plan that addresses how each deliverable meets at least one of the specific goals in the Executive Order.
Deliver, maintain, and execute an implementation plan for accomplishing strategic cybersecurity objectives that are specific, measurable, achievable, and relevant to the overall strategic vision, which shall be completed within an established timeframe. (Section 7)	Council committees and working groups	September 2018 – Committees and working groups each submitted strategic plans that provide objectives that are specific, measurable, achievable, and relevant to the overall strategic vision, which shall be completed within an established timeframe.
Receive Guidance from the Counter-Terrorism and Security Council (CTASC) and report to the Homeland Security Advisory with the Office of the Governor. (Section 8)	Indiana Cybersecurity Program Director	July 2017 thru September 2018 – Provided updates to CTASC members, Lt. Governor's Office, and the Homeland Security Advisor.
All state agencies, departments, commissions, bureaus, institutions, and entities shall cooperate to the fullest extent possible with the Executive Order. (Section 8)	Council Members	July 2017 thru September 2018 – All members in good standing have participated to the fullest extent possible per the Executive Order.
Council shall be staffed by the Indiana Department of Homeland Security and subject to the requirements as well as the security and confidentiality expectations under Open Door Law and the Access of Public Records Act. (Section 9 and 10)	Indiana Department of Homeland Security and Indiana Office of Technology	January 2017 thru September 2018 - Indiana Department of Homeland Security has partnered with the Indiana Office of Technology to ensure the Council is staffed, provides the necessary resources, and meets the objectives. Furthermore, the Council including all committees and working groups complied with the Open Door Law and the Access of Public Records Act.



PART 2
IMPLEMENTATION PLANS

EXECUTIVE SUMMARY OF PLANS

Using the strategic framework, and operating within the four phases (research, planning, implementation, and evaluation), the 20 committees and working groups each developed a comprehensive strategic implementation plan that collectively resulted in 69 detailed deliverables and 120 objectives. The majority of the deliverables are being completed by the Council members, whose accomplishments were the result of dedicated state resources assisted by federal and military subject matter experts. Local government entities, academia, and private sector organizations also contributed a considerable amount of donated services, time, and resources.

COUNCIL STATS

YEAR 1

200+ MEMBERS

19 OF 69 DELIVERABLES COMPLETED

38 OF 120 OBJECTIVES COMPLETED

The following is a list of each committee and working group with their respective deliverables and objectives. Note all deliverables that require additional resources or funding are further detailed in the respective committee or working group plan (see Appendix D). It is also important to note that funding discussed may come from a variety of sources including but not limited to grants, federal, private, public, and academic monies. Moreover, the availability of funding and resources may change as this plan is updated and implemented.

COMMUNICATION COMMITTEE

Deliverable: Establish Voluntary Industry Contact List

- Objective 1: Develop a form and process to collect a central cyber industry contact list by October 2018.
- Objective 2: Seventy percent of all communications providers complete annual cyber contact form by December 2018.

Deliverable: Terminology Glossary

- Objective 1: Complete Communications Sector Terminology Glossary by August 2018. *Completed.*
- Objective 2: Publish Communications Sector Terminology Glossary to IECC website by September 2018. *Completed.*

Deliverable: Cyber Incident Response Engagement Guide

- Objective 1: Develop the Communications Sector Engagement Guidance by October 2018.
- Objective 2: Distribute the Communications Sector Engagement Guidance to 80 percent of identified industry and key stakeholders by November 2018.

Deliverable: Communications Sector White Paper

- Objective 1: Complete the Communications Sector Whitepaper for the industry by October 2018.
- Objective 2: Distribute the Communications Sector Whitepaper to 80 percent of identified industry and key stakeholders by November 2018.

DEFENSE INDUSTRIAL COMMITTEE

Deliverable: Cyber Digital Platform

- Objective 1: Indiana Office of Defense Development and partners will develop a pilot of the Indiana defense cybersecurity market development and capture plan and system (Digital Platform) by August 2018. *Completed.*
- Objective 2: Indiana increases to 2 percent (about $300M) of the Department of Defense (DOD) cybersecurity market share ($15B plus) by FY 2022.

Deliverable: Cyber Market System

- Objective 1: Indiana Office of Defense Development (IODD) and partners will develop and implement a cybersecurity market pursuit plan and system by January 2019.

Deliverable: Cyber Statewide Testbed

- Objective 1: Establish a nationally recognized cybersecurity test bed in Indiana by January 2020.
- Objective 2: Indiana captures 5 percent of international cybersecurity market share of cybersecurity test, training, and demonstration plan and capability by December 2023.

ECONOMIC DEVELOPMENT COMMITTEE

Deliverable: Incentive Program

- Objective 1: IECC Economic Development Committee will propose a list of possible incentive programs to be considered by the State of Indiana by April 2019.
- Objective 2: State of Indiana will establish an incentive program in Indiana by July 2020.

Deliverable: Cybersecurity SIoT Innovation District

- Objective 1: Economic Development Committee will develop business plan recommendations for first cybersecurity/Security in the Internet of Things (SIoT) innovation district by end of August 2019.
- Objective 2: State establishes first cybersecurity/Security in the Internet of Things (SIoT) innovation district, provided appropriate funding source made available, by December 2019.

Deliverable: Implementation Plan for Cybersecurity - Marketing

- Objective 1: Indiana Economic Development Corporation will develop a two-year marketing plan focusing on economic development and Indiana's cybersecurity posture by August 2019.
- Objective 2: Indiana Economic Development Corporation will execute a two-year marketing plan focusing on economic development and Indiana's cybersecurity posture beginning in 2020.

ELECTION COMMITTEE

Deliverable: Statewide Voter Registration System (SVRS) Cybersecurity Enhancements

- Objective 1: Indiana Secretary of State Office will begin utilizing additional security protocols in 2018. *Completed.*

Deliverable: Statewide Voter Registration System (SVRS) user access control enhancement.

- Objective 1: SOS Office and Indiana Election Division will implement the Statewide Voter Registration System (SVRS) user access/authentication upgrades with 100 percent of counties by January 2018. *Completed.*
- Objective 2: SOS Office and Indiana Election Division will launch a Two-Factor Authentication Token Pilot by March 2018. *Completed.*

- Objective 3: SOS Office and Indiana Election Division will provide a report on Two-Factor Authentication Token Pilot by May 2018. *Completed.*

Deliverable: Election System Physical and Logical Security Controls

- Objective 1: Indiana Voting System Technical Oversight Program will develop and distribute the Best Practices for Voting System Logical and Physical Security Manual to all Indiana counties in 2018. *Completed.*

Deliverable: Post-Election Risk Limiting Audit (RLA) Standards and Pilot Program

- Objective 1: Indiana Voting System Technical Oversight Program (VSTOP) will develop and implement an RLA pilot in Marion County by July 2018. *Completed.*
- Objective 2: Indiana Voting System Technical Oversight Program (VSTOP) will provide a report by August 2018 on the July 2018 RLA pilot in Marion County. *Completed.*

Deliverable: Cyber Threat Awareness and Training for County Election Administrators

- Objective 1: Indiana Secretary of State will implement and deliver a multi-year cybersecurity public awareness plan beginning in 2018. *Completed.*
- Objective 2: Eighty percent of Indiana election officials participate in state-offered training by November 2019.
- Objective 3: See a 30-percent decrease in click-through rates of Indiana election officials in State phishing campaign by April 2019.

Deliverable: Election Day Cybersecurity Tabletop Exercises

- Objective 1: Indiana Secretary of State will develop and deliver a training exercise program for election officials and administrators by October 2018.
- Objective 2: Secretary of State will conduct a tabletop election exercise by April 2019.

Deliverable: Indiana Best Practices Manual for the Operation of Election Equipment

- Objective 1: Indiana Voting System Technical Oversight Program (VSTOP) will develop the Indiana Best Practices Manual for the Operation of Election Equipment by July 2018. *Completed.*

Deliverable: Election Day Cybersecurity Emergency Preparedness Plans

- Objective 1: Indiana Secretary of State and Election Division will provide existing Election Day emergency preparedness and response material to include cybersecurity for distribution prior to May 2018. *Completed.*

Deliverable: Election Day Cybersecurity Monitoring and Rapid Response Technical Support

- Objective 1: Secretary of State will develop and implement an Election Day cybersecurity technical support program by April 2018. *Completed.*
- Objective 2: Secretary of State will develop an Election Day cybersecurity technical support program report and after action review with key partners by October 2018.

Deliverable: Election Cybersecurity Public Education and Awareness

- Objective 1: Secretary of State will develop a communications plan specific to election security by April 2018. *Completed.*
- Objective 2: Secretary of State will measure the success of communication plan efforts specific to election security by October 2018.

Deliverable: Election Cybersecurity Incident Response and Communications

- Objective 1: Secretary of State will develop and distribute an Election Day cybersecurity incident communications and response to all Indiana election county officials by October 2018.

Deliverable: Catalog and Summaries of Best Election Cybersecurity Reports and Guides

- Objective 1: Secretary of State will develop an election cybersecurity library by October 2018.

ENERGY COMMITTEE

Deliverable: Critical Infrastructure Information (CII)

- Objective 1: IECC Energy Committee will provide current definitions and review of potential policy changes to protect critical infrastructure information while maintaining public access and freedom of information by July 2018. *Completed.*

Deliverable: Contacts

- Objective 1: More than 85 percent of Indiana electric and natural gas utilities will provide the Indiana Utility Regulatory Commission's Emergency Support Function lead, on behalf of the Indiana Department of Homeland Security, a cybersecurity contact by June 2018. *Completed.*
- Objective 2: The Indiana Utility Regulatory Commission's Emergency Support Function lead will maintain the cyber contact list on behalf of the Indiana Department of Homeland Security Emergency Operations Center annually. *Completed.*

Deliverable: Coordinate with Others

- Objective 1: IECC Energy Committee will coordinate with other committees and working groups as needed to effectively complete the State Cybersecurity Strategic Plan by September 2018. *Completed.*
- Objective 2: IECC Energy Committee will share information with Energy Information Sharing and Analysis Center (ISAC) regarding Indiana's new cyber sharing resources by December 2018.

Deliverable: Metrics

- Objective 1: IECC Energy Committee will provide the utility energy industry an annual survey that will assess cybersecurity planning, preparedness, and recovery posture by June 2018. A summary of the results from all survey responses will be sent to the IECC. *Completed.*
- Objective 2: Eighty percent of all utilities will complete annual survey by July 2018. The actual result was 100 percent participation with all responses received prior to June 2018. *Completed.*

Deliverable: Training

- Objective 1: IECC Energy Committee will provide the IECC Workforce Development Committee the needs of the energy sector, as well as examples to consider, as Indiana cybersecurity training and apprenticeship programs are being developed by July 2018. *Completed.*

FINANCE COMMITTEE

Deliverable: Cyber Training (Ivy Tech)

- Objective 1: Ivy Tech will develop a cybersecurity curriculum for business executives by July 2018. *Completed.*
- Objective 2: IECC Finance Committee and Ivy Tech will launch a pilot program with seven participants by August 2018. *Completed.*

Deliverable: Top Security Tips Material

- Objective 1: IECC Finance Committee will develop the Top Information Security Tips training material for Indiana businesses by December 2018.

GOVERNMENT SERVICE COMMITTEE

Deliverable: Indiana's Cybersecurity Hub Website

- Objective 1: IECC will develop and launch a statewide cyber hub website by September 2018. *Completed.*
- Objective 2: Increase website traffic to www.in.gov/cyber by 200 percent by September 2019.

Deliverable: Indiana Cyber Disruption/Emergency Plan

- Objective 1: IECC Government Services Committee will develop the Indiana Cyber Disruption/ Emergency Plan for the public by May 2019.

HEALTHCARE COMMITTEE

Deliverable: Long-term Education

- Objective 1: IECC Healthcare Committee will create Indiana-focused versions of security education by March 2019.
- Objective 2: Provide Indiana-focused versions of security education to 80 percent of Indiana healthcare providers by May 2019.

Deliverable: Indiana Threat Intelligence Distribution System

- Objective 1: Develop a pilot program with three participants of the Indiana Health Cyber Threat Intel Committee by November 2018.
- Objective 2: Evaluate pilot program and recommend a sustainability framework model for the state of Indiana to maintain by February 2019.

Deliverable: Vendor Management

- Objective 1: Create vendor management resources for healthcare providers by February 2019.
- Objective 2: Distribute vendor management resources to 80 percent of healthcare providers by April 2019.

WATER & WASTEWATER COMMITTEE

Deliverable: Cyber Risk Model (Plan)

- Objective 1: IECC Water and Wastewater Committee and partners develops a Cyber Plan Template for Indiana water/wastewater companies by December 2018.
- Objective 2: IECC Water and Wastewater Committee and partners distributes the Cyber Plan Template to 25 percent of Indiana water/wastewater companies by March 2019.

Deliverable: Cyber Contacts

- Objective 1: Indiana Department of Environmental Management will conduct modifications to the Safe Drinking Water Information System to collect cybersecurity contact information for Indiana water and wastewater organizations by November 2017. *Completed.*
- Objective 2: Indiana Department of Environmental Management will maintain the cybersecurity contact information for 95 percent of Indiana water organizations serving a population greater than 3,301 by December 2019.

Deliverable: Risk Tool

- Objective 1: IECC Water and Wastewater Committee develops the Cyber Assessment Risk Tool within 12 months of securing funding.
- Objective 2: Eighty percent of Indiana water and wastewater companies will have used the Cyber Assessment Risk Tool within 24 months of deployment.

Deliverable: Training Plan

- Objective 1: IECC Water and Wastewater Committee will develop a training plan within three months of securing funding.
- Objective 2: Fifty percent of Indiana water and wastewater companies will incorporate the training plan as a part of their operational resources within 24 months of deployment of the training plan.

Deliverable: Cyber Plan Template

- Objective 1: IECC Water and Wastewater Committee will develop a Cyber Plan Template for Indiana water/wastewater companies by April 2019.
- Objective 2: IECC Water and Wastewater Committee and partners will distribute the Cyber Plan Template to 50 percent of Indiana water/wastewater companies by October 2019.

WORKFORCE DEVELOPMENT COMMITTEE

Deliverable: Generate Interest Plan

- Objective 1: Establish and fund a statewide cybersecurity program for K-12 stakeholders by July 2019.
- Objective 2: Launch a statewide cybersecurity program for K-12 stakeholders by August 2019.

Deliverable: Job Demand Tool

- Objective 1: State of Indiana adopts Cyberseek as the source for cybersecurity-related job demand and career pathways for the state by August 2019.
- Objective 2: State of Indiana will develop integration plans for consumption of the Cyberseek.org data across various job seeker, employer, and education platforms by December 2019.

Deliverable: K-12 Offering Cybersecurity Content

- Objective 1: Indiana Department of Education will develop a menu of cybersecurity content and initiatives that includes K-12 computer science offerings by September 2019.
- Objective 2: Eighty percent of Indiana Schools adopt one or more cyber initiatives by August 2020.

Deliverable: Best Practices and NICE Framework Standard

- Objective 1: Indiana formally establishes NICE Framework as the cybersecurity standard for the state by October 2019.
- Objective 2: Working with the National Governors Association, the IECC Workforce Development Committee will create and implement statewide program that will provide educators and businesses resources for meeting best practices and standards, such as the NICE Framework, by December 2019.
- Objective 3: Working with the National Governors Association, the IECC Workforce Development Committee will create and implement statewide outreach program for cybersecurity training that follows best practices and standards, such as the NICE Framework, to underserved communities, minorities, women, veterans, disables, and minor offenders by December 2019.

Deliverable: Incentivized Cybersecurity Certifications

- Objective 1: Indiana Department of Workforce Development and partners will create and launch a statewide cybersecurity certification training program that meets NICE standards by December 2019.

Deliverable: Program Data Tool

- Objective 1: Indiana Commission for Higher Education will develop and launch a survey for post-secondary to report on cybersecurity-related programs by March 2019.
- Objective 2: Indiana Commission for Higher Education will develop and deliver a final report to the IECC on findings of post-secondary survey by December 2019.

CYBER PRE- & POST- INCIDENT WORKING GROUP

Deliverable: Exercise

- Objective 1: State of Indiana will develop and execute a Cross-Sector Critical Infrastructure Cyber Exercise by December 2020.

Deliverable: Gap Analysis

- Objective 1: IECC Cyber Pre- thru Post-Incident Working Group will complete a comprehensive gap analysis of identified high-risk critical infrastructure sectors by August 2018. *Completed.*
- Objective 2: IECC Cyber Pre- thru Post-Incident Working Group will provide recommendations based on a comprehensive gap analysis of identified high-risk critical infrastructure sectors by December 2018.

Deliverable: Cyber Emergency Response Team (IN-CERT)

- Indiana State Police will develop and launch Indiana Cyber Emergency Response Team training program within 12 months of the Council partners securing an encumbered source of funding.

Deliverable: Cyber Assessments

- Objective 1: Indiana National Guard will develop a Local/State Government Cyber Assessment Program by December 2018.
- Objective 2: Indiana National Guard will conduct Cyber Assessment for State critical infrastructure entities by December 2019.

CYBER SHARING WORKING GROUP

Deliverable: Best Practices

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

Deliverable: Cyber Sharing Maturity Model

- Objective 1: IECC will develop Indiana's first cyber sharing maturity model by February 2019.
- Objective 2: IECC will distribute Indiana's first cyber sharing maturity model to critical infrastructures through 90 percent of Indiana associations by June 2019.

Deliverable: Inventory of Cyber Sharing Resources

- Objective 1: IECC Cyber Sharing Working Group will complete an inventory of cyber sharing resources by July 2018. *Completed.*

Deliverable: MS-ISAC Member Recruitment

- Objective 1: Increase Indiana MS-ISAC membership by 25 percent by June 2019.

Deliverable: Secured Information Sharing Program

- Objective 1: IECC Cyber Sharing Working Group will develop a Secured Information Sharing Program by July 2019.
- Objective 2: IECC Cyber Sharing Working Group will launch a Security Information Sharing Program by August 2019.

CYBER SUMMIT WORKING GROUP

Deliverable: Cybertech Midwest

- Objective 1: IECC will secure a cybersecurity conference partner for three years by May 2018. *Completed.*
- Objective 2: State of Indiana will hold its first statewide cybersecurity conference by October 2018.

EMERGENCY SERVICES & EXERCISE WORKING GROUP

Deliverable: Annex

- Objective 1: Indiana Department of Homeland Security (IDHS) will develop and distribute the state's Comprehensive Emergency Management Plan (CEMP) Cyber Annex to appropriate parties by December 2018.
- Objective 2: IDHS will exercise the CEMP Cyber Annex by December 2019.

Deliverable: IDHS Cyber Exercise Engagement

- Objective 1: IDHS will develop and launch Cyber Exercise Engagement Program by July 2019.

Deliverable: Toolkit

- Objective 1: IECC Emergency Services and Exercise Working Group will develop a Cyber Response Toolkit Version 1.0 by October 2018.
- Objective 2: IDHS will launch four workshops throughout Indiana using the Cyber Response Toolkit by October 2019.
- Objective 3: Partnering with the National Governors Association, the IECC Emergency Services and Exercise Working Group will develop a Cyber Response Toolkit 2.0 with a cyber risk tool for emergency personnel by August 2019.
- Objective 4: IDHS will develop and launch four workshops throughout Indiana using the Cyber Response Toolkit 2.0 by March 2020.

Deliverable: EOC

- Objective 1: IDHS will develop a Cyber Liaison position within its Emergency Operations Center by May 2019.
- Objective 2: IDHS will complete training and exercise the Cyber Liaison position within the EOC by December 2019.

LEGAL & INSURANCE WORKING GROUP

Deliverable: Insurance Guide

- Objective 1: IECC Legal and Insurance Working Group will develop a Cyber Insurance Guide to be provided to government and businesses by September 2018. *Completed.*

Deliverable: Policy Review

- Objective 1: Legal and Insurance Working Group will develop a list of cyber laws applicable to Indiana businesses and residents under the current landscape by August 2018. *Completed.*

Deliverable: Cyber Insurance Survey

- Objective 1: Legal and Insurance Working Group will conduct a survey of businesses for insurance coverage and cybersecurity insurance coverage by August 2019.
- Objective 2: Legal and Insurance Working Group will provide a report of the findings of the cyber insurance survey to the IECC by December 2019.

LOCAL GOVERNMENT WORKING GROUP

Deliverable: Local Officials Cybersecurity Guidebook

- Objective 1: Develop a guidebook for local government officials to assist them with cybersecurity planning and education expected by fall of 2018.
- Objective 2: Promote guidebook on cybersecurity planning and education to local government officials throughout 2019.

PERSONAL IDENTIFIABLE INFORMATION WORKING GROUP

Deliverable: Indiana PII Guidebook

- Objective 1: IECC PII Working Group will develop an Indiana PII Guidebook for government and the general public by the end of Q1, 2019.

POLICY WORKING GROUP

Deliverable: Policy Research Report

- Objective 1: IECC and partners will develop a report of state and federal cybersecurity legislation by August 2018. *Completed.*

PUBLIC AWARENESS & TRAINING WORKING GROUP

Deliverable: Public Relations Campaign Plan

- Objective 1: The IECC Public Awareness and Training Working Group will complete a statewide public relations cybersecurity campaign plan by June 2018. *Completed.*
- Objective 2: IECC will implement an IECC public relations micro-plan on year-one efforts by September 2018. *Completed.*

STRATEGIC RESOURCE WORKING GROUP

Deliverable: IECC Program Documentation

- Objective 1: IECC will develop program/framework documentation by September 2018. *Completed.*

Deliverable: IECC Scorecard

- Objective 1: IECC, along with Purdue University, will develop Indiana's first Cybersecurity Scorecard by May 2018. *Completed.*
- Objective 2: IECC, along with Purdue University, will launch Indiana's Cybersecurity Scorecard Pilot Program with 90 percent of selected organizations by September 2018. *Completed.*
- Objective 3: IECC, along with Purdue University, will develop a final report of Indiana's Cybersecurity Scorecard Pilot Program by May 2019.

Deliverable: IECC Sustainability Recommendation

- Objective 1: IECC will develop a sustainability recommendation by September 2018. *Completed.*

OBSERVATIONS & CONSIDERATIONS OF IECC

The cybersecurity threat environment is dynamic and complex. Launching a successful statewide cybersecurity strategy is dependent upon a clear and consistent message from leadership at all levels of government. Cybersecurity is a priority for Indiana because of the pervasive threats, which is why the Governor and state lawmakers continue to champion its importance. Defining cybersecurity—and efforts to protect against cybersecurity threats—must be illustrated in a way that is simple yet effective, complete yet attainable. In short, cybersecurity needs to be characterized in a way that eliminates the mystery of what to do next. Effective cybersecurity goes beyond password protections and tip sheets; it requires a shift in the cultural dialogue—moving away from a purely technological view and toward a multi-disciplinary solution to the growing threat. If it is to be effective, these solutions must encompass not only government and businesses at all levels and sizes, but also all Hoosiers across the state. Further, it requires ongoing training programs, continuing public education, toolkits, and updates to address the pervasiveness of cyber threats in today's society. Cybersecurity is an exercise in continuous risk management and will never be a "one-and-done" initiative, nor will it ever offer perfect prevention. Instead, effective cybersecurity is best understood through a lens of evidence-based risk reduction.

As with many important issues, the success of a cybersecurity strategy depends on the resources and funding available to support its implementation. It also is important to note that while these implementation plans have estimated time frames, budgets, and resources, they are agile in nature. The expertise of the members on those committees and working groups will inform updates and necessary corrections to each implementation plan.

It is important that the Council remain aware and prepared to shift focus of deliverables and priorities based on emerging technology and threats. Adapting to a changing threat environment as periodically illustrated by experts and federal partners will be critical to the significant efforts of the Council. The Council will remain flexible to these adaptations but will continue to strive to complete the deliverables laid out in this state plan through the facilitation and assistance of Council leadership.

2018 RECOMMENDATIONS

As many of the deliverables are being implemented, the Council asks that the Governor and his administration continue to support the IECC implementation plans, per the experts of the Council, by:

- Supporting a statewide cybersecurity public relations and awareness campaign designed to nurture fundamental change in culture that will make not only citizens of Indiana safer in their personal endeavors, but also the places they work as good cyber hygiene is presented, understood, and employed over time.
- Encouraging the highest-level technical and administrative cybersecurity best practices and standards as well as support cybersecurity research with a focus on evidence-based policies and practices toward changing behavior and risk reduction.
- Supporting policy that will boost the cybersecurity posture of Indiana. This includes updating 2018 Senate Enrolled Act 362. The current law requires a water or wastewater utility's cybersecurity plan be a public document. An amendment to this law removing the requirement of making the cybersecurity plan a public document, while preserving this requirement for the asset management plan to be public, would ensure the safety of Indiana's critical infrastructure from bad actors.
- Providing necessary support to the critical infrastructures as they move forward with their many deliverables. In particular, utilities such as the water and wastewater where an important tool is being developed to assist operators in evaluating and improving their cybersecurity posture. This also includes efforts such as planning, training, and exercising in preparation of a cyberattack (e.g. working with small critical infrastructure operators in safe environments such as Muscatatuck).
- Encouraging all of Indiana's workforce ecosystem (K-12, post-secondary programs, underemployed, educators, employers, and partners) to follow cybersecurity best practices and national standards such as the National Institute of Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE) Workforce Development Framework; as well as assist in providing resources to educators and businesses in Indiana so that they can best develop and contribute to the cybersecurity talent pipeline.
- Developing the cyber knowledge of law enforcement and emergency management. In particular, law enforcement forensic knowledge so that they are poised to be a part of the Indiana Cybersecurity Emergency Response Team in an event of a cyber emergency.
- Supporting the Council as it moves forward, including ensuring that the Voting and Advisory Members match the needs of the state. This would mean updating the Executive Order to include additional Voting Members representing industries such as transportation, agriculture, advanced manufacturing, and the business community as well as cybersecurity experts, tools, and service providers as the cyber threat continues to evolve.

PART 3
YEAR IN REVIEW

2018 MEMBERSHIP & LEADERSHIP

In 2018, more than 200 members participated in the Council. Of those, Voting and Advisory Members were selected to lead the 20 committees and working groups. For a full list of members and committee working group leadership as of the last membership vote taken by the Council in January 2018, see Appendix E.

BEST PRACTICES OF IECC

The Council has accomplished an unprecedented amount of work for the citizens and businesses of Indiana in the last year due to the commitment of the public, private, military, and academic partnerships. Cybersecurity is not an issue that merely affects information technology professionals but one that affects all Hoosiers and businesses. Taking cybersecurity to the Next Level cannot be done by one entity alone. It is by working collaborally across sectors and areas of expertise to address the comprehensive ecosystem that the state will not only address its own technology and information environment, but also make great strides to further increase Indiana's broader cybersecurity posture.

DELIVERABLES COMPLETED

Each committee and working group was established within the last year, and each began following a four-step strategic process (research, planning, implementation, and evaluation). This process leads Indiana to a comprehensive understanding of the many challenges facing the state, as well as the many current and possible solutions that can enhance cybersecurity at all levels. The Council has identified in detail 69 deliverables to date and, given the right support, those will be implemented over the next few years. In fact, in the first year the Council has completed 27.5 percent of its total deliverables, and 31.6 percent of the 120 objectives.

Some of the deliverables completed within the first year include:

- Statewide cybersecurity general public awareness campaign plan
- Telecommunications sector terminology glossary
- Indiana Office of Defense Development cyber digital platform pilot
- Election system best practices, upgrades, pilot programs, education initiatives, and more
- Energy sector best practices and information
- Indiana's first Cybersecurity Scorecard that will not only provide key indicators to users, but also can be used to directly quantify the effectiveness of the Council
- Professional education pilot program for executives
- Indiana's cybersecurity hub website
- Mechanisms to collect critical infrastructure cybersecurity contact information for the State of Indiana
- Cybersecurity plan template for water and wastewater utilities
- Inventory of cybersecurity sharing resources
- Cybersecurity insurance guide
- Comprehensive cyber policy research including a tool of cybersecurity legislation proposed (passed or failed) in all 50 states and at the federal level since 2011

ADDITIONAL ACCOMPLISHMENTS IN INDIANA

Since the launch of Governor Holcomb's Council Version 2.0 in July 2017, there have been several additional Indiana programs and accomplishments, including:

DEVELOPING THE WORKFORCE

In January 2018, Governor Eric J. Holcomb invited aspiring female high school students to explore their interest in the computer science and technology field by joining the Girls Go *CyberStart* program. *CyberStart* features an online series of challenges that allow students to solve cybersecurity-related puzzles and explore exciting, relevant topics, such as cryptography and digital forensics. More than 100 Indiana teams and 380 young women entered the competition. In the end, 12 Indiana teams made it into the top 100 teams of the nation, and three of those Indiana teams made it into the top 20.

CYBERTECH MIDWEST

The State of Indiana has announced the launch of its first cybersecurity conference, in partnership with Cybertech, to be held on October 23, 2018. Cybertech is a worldwide conference series with events in Tel Aviv, Rome, Singapore, Panama, and other locations. Due to Indiana's collaborative approach to cybersecurity and proven record of public, private, academic, and military collaborations, Indiana secured the conference through 2020. More information at http://midwest.cybertechconference.com/.

CYBER ACADEMY

On August 22, 2018, Governor Holcomb joined officials from the Indiana National Guard and Ivy Tech Community College to cut the ribbon on the new Ivy Tech Cyber Academy. The Cyber Academy, located at the Muscatatuck Urban Training Center, will train military and civilian students in dealing with cyber threats. Students participating in this program can:

- Earn an accelerated Cyber Security/Information Assurance Associate of Applied Science Degree from Ivy Tech Community College - Columbus, an 11-month, 60-credit-hour program.
- Participate in exclusive training and testing events in Muscatatuck's multi-domain environment (land, maritime, air, human and cyberspace), which will provide students opportunities to conduct integrated and synchronized offensive and defensive cyberspace operations.
- Earn highly sought-after, industry-leading certifications useful in both military and civilian careers, including A+, C-CENT and Security+.
- Embark on a career path in government agencies or global security companies including companies right here in Indiana paying an average of more than $70,000 per year by having opportunities to interact with those potential future employers during the program.

JOINING OTHER STATES

The Council re-launch followed Governor Holcomb joining the National Governors Association's (NGA) "A Compact to Improve State Cybersecurity" in mid-July. The 38 governors who signed the compact agreed to protect personal and government data stored on state systems and develop statewide plans to combat cyberattacks waged against information technology networks. The agreement included a pledge to build a cybersecurity governance structure, prepare and defend the state from cybersecurity events, and increase the nation's cybersecurity workforce.

JOINING FEDERAL PARTNERS

In addition to working closely with U.S. Department of Homeland Security (USDHS), Federal Bureau of Investigation (FBI), and other federal partners, IDHS recently signed a Memorandum of Agreement (MOA) with Indiana's Chapter of InfraGard, formalizing the partnership with the State of Indiana. The InfraGard Indiana Members Alliance serves as a link between the public and private organization and is a cooperative undertaking between the U.S. Government (FBI) and an association of local businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to increasing the safety/security of Indiana and U.S. critical infrastructures.

JOINING OTHER COUNTRIES

Filing on behalf of the members of the Security in Technology Consortium, the Cyber Leadership Alliance, a non-profit organization that sits on the Council, has been granted membership to Global EPIC. Global EPIC is a worldwide program of cybersecurity ecosystems that includes the U.S., Israel, Canada, the Netherlands, Costa Rica, and others. Academic partners, private companies, and government, including the State of Indiana Chief Information Officer (CIO) and the Cybersecurity Program Director, have joined this consortium and will support projects and research.

NGA CYBER POLICY ACADEMY

As one of four states selected by the National Governors Association Cyber Policy Academy, Indiana will be able to work with other state leaders to share best practices and lessons learned. Knowledge gained from this academy will allow Indiana to accelerate its efforts and increase the knowledge of policies that will enhance education, awareness, response, and protection for all Hoosiers. The Academy also will help to guide a proactive strategy that will address cybersecurity as a common threat and best inform policy discussions that highlight and energize dialogue as the state implements viable, solutions to complex mission areas. Specifically, the state will focus on the Indiana cybersecurity workforce and develop tools for emergency managers for preparing, responding, and recovering from a cyberattack. Furthermore, the Academy will position Indiana to equip other states to implement their own cyber plans and safeguards by creating best practices and solutions that can be implemented across sectors and state lines.

HELPING THE NATION

Indiana is joining other states and providing expertise in addressing cybersecurity issues. By working collaboratively, states can establish long-term protection strategies that will provide other states and their residents with the knowledge and infrastructure they need to feel safer from such threats. Working with other states also will assist Indiana in its development of concrete protocols, policies, and programs of how to best engage and partner with not only the states in the Midwest, but also throughout the nation. This includes cyber threat sharing and response capabilities. Indiana recognizes that cyberattacks do not account for state lines, and state-to-state coordination of support and recovery is necessary when an attack occurs.

IECC MOVING FORWARD

As the Council moves forward with the deliverables in this plan, it is important to note that this is a living document and will be updated regularly. At a minimum, the plan will be updated annually and will include a progress report from each committee and working group to the Governor and public. Moreover, the Council will add committees and working groups in 2019 such as advanced manufacturing, agriculture, transportation, business, and emerging technologies now that the framework has been fully tested and successful. Council membership also will be reviewed and recruitment of experts in the fields will be ongoing.

The goal of the Council is to move cybersecurity to the Next Level in Indiana, but doing so in a way that is as intuitive as possible and does not add more clutter to the already complex topic. Indiana is only as strong as its weakest link. Providing resources to the weakest within the state will not only strengthen the posture of the many organizations who are connected, but also support an infrastructure that will continue to attract businesses and workforce to come to Indiana. With the continued guidance and support of experts throughout the State of Indiana, Hoosiers will be safer and businesses will continue to thrive.