Indiana
Cybersecurity Strategic Plan

October 2021

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

October 29, 2021

Dear Governor Holcomb:

Since 2018, the Indiana Executive Council on Cybersecurity has not only been successful with its first-of-its-kind strategic approach, but it has stepped up in the last year and a half as we have all experienced not only a different world, but some of the largest cyber attacks recorded in history.

And as millions had to become remote in a matter of days, many of the leaders within the Council provided additional deliverables and resources because businesses and local governments needed it.

These cyber warriors and their efforts on your Council have made Indiana a leading state in the nation. In fact, the Council has completed 78 percent of its 69 identified deliverables, and 77 percent of the 120 objectives identified in the strategic plan we presented to you in 2018 even with the challenges of the pandemic. Moreover, these dedicated members have donated hundreds of hours and millions of dollars of services to the businesses, local governments, and citizens in Indiana - an unprecedented amount of savings from a volunteer government Council or Commission.

Due to the success of the previous plan as well as the more than 250 dedicated subject matter experts, the following *2021 Indiana Cybersecurity Strategic Plan* encompasses not only the breadth of topics, but depth as well. The following plan will provide you the background of how we have created the proven strategic framework that we continue to use today, and the plans of 68 deliverables and 134 objectives we will strive to complete in the coming years.

As we work to implement this plan, the Council asks for your continued leadership in:

- Supporting the development of local government cybersecurity resources and education;
- Encouraging the highest-level of 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;

- Supporting a statewide cybersecurity public relations and awareness campaign;
- Encouraging all of Indiana's workforce ecosystem to follow national standards and develop the cybersecurity pipeline; and
- Supporting the Council as it moves forward, including ensuring its membership matches the needs of the state.

We appreciate the opportunity to work with so many great cyber warriors on the Council. Through these partnerships the State is able to best serve Hoosiers and further move Indiana's cybersecurity efforts to the *Next Level*.

Sincerely,

Executive Director Stephen Cox
Indiana Department of Homeland Security

Chief Information Officer Tracy Barnes
Indiana Office of Technology

Adjutant General, Brigadier General Dale Lyles
Indiana National Guard

Superintendent Doug Carter
Indiana State Police

Cybersecurity Program Director Chetrice L. Mosley-Romero
State of Indiana

Indiana Executive Council on Cybersecurity

2021 Voting Members

Operations Director Samuel Hyer, Office of Governor Eric J. Holcomb
Director John Roeder, Office of Lt. Governor Suzanne Crouch
Executive Director Stephen Cox, Indiana Department of Homeland Security
Chief Information Officer and Director Tracy Barnes, Indiana Office of Technology
Superintendent Douglas Carter, Indiana State Police
Adjutant General, Brigadier General Dale Lyles, Indiana National Guard
Cybersecurity Program Director Chetrice L. Mosley-Romero, State of Indiana
Secretary of State Holli Sullivan, State of Indiana
Attorney General Todd Rokita, State of Indiana
Chair James Huston, Indiana Utility Regulatory Commission
Commissioner Teresa Lubbers, Indiana Commission for Higher Education
Commissioner Bob Grennes, Indiana Department of Revenue
Secretary of Commerce Brad Chambers, Indiana Economic Development Corporation
Commissioner Fred Payne, Indiana Department of Workforce Development
Retired Major General Clif Tooley, Indiana Economic Development Corporation Defense Development
Chief Information Security Officer, Angie Ritchey
Tim Harmon, Journalist
Partner Ronald W. Pelletier, Pondurance
Information Technology Vice President John Lucas, Citizens Energy Group
President Daniel McGrath, Indiana Energy Association
Executive Director Matthew Greller, Accelerate Indiana Municipalities (AIM)
Executive Director Stephanie Yager, Indiana Association of County Commissioners
Chief Information Security Officer Mitch Parker, Indiana University Health
Assistant Vice President of Cybersecurity Dan Solero, AT&T
Director of Cybersecurity Defense Products Brad Swearingen, Rolls Royce
Chief Information Officer Rob Lowden, Indiana University
Chief Information Officer Ian Hyatt, Purdue University

2021 Indiana Cybersecurity Strategic Plan

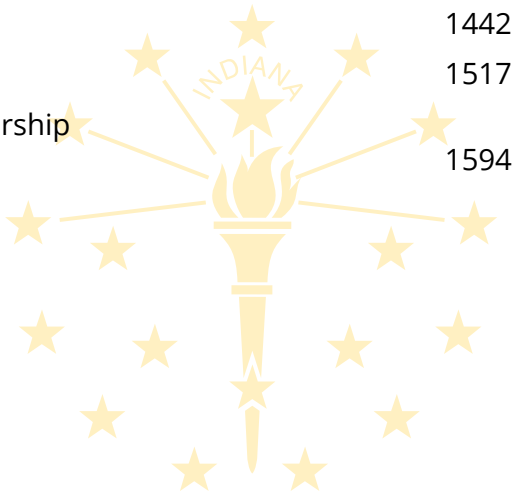
Table of Contents

... continued on next page

2021 Indiana Cybersecurity Strategic Plan

Table of Contents

Appendices (continued)



About This Plan

Our goals can only be reached through a vehicle of a plan, in which we must fervently believe, and upon which we must vigorously act. There is no other route to success.

- Pablo Picasso

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, but where the state will go next.

This Indiana cybersecurity strategic plan outlines those directions as simply and as directly as the complexity of the effort allows.

The *2021 Indiana Cybersecurity Strategic 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 summary of the work of the Council.

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 15 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 committee and working group plan is provided in its entirety in the Appendices of this strategic plan.

Part Three highlights the real people and real work since the 2018 plan. The section identifies the dedicated members and leaders of the Council who have dedicated themselves since the beginning, the success of the 2018 plans and more that will be featured in the "The State of Cyber Report", best practices of the Council, and how the Council will continue taking cybersecurity in Indiana to the *Next Level*.

Part 1
Strategic Framework of IECC

Today's Evolving Cyber Threat

A lot has changed since the first Indiana Cybersecurity Strategy was voted on and delivered to Governor Holcomb by the IECC September 2018. But nothing has moved the state of business, workplace culture, and technology more than the months that followed Indiana's pandemic shut down in March 2020. And the reality of how interconnected we all are became even more evident when home became our new workplace and all the cyber risks that followed.

Unfortunately, the new interconnectivity has also made the cyber risks grow exponentially and poses an increased danger to citizens, organizations, and industries, as well as threatens the security and economy of Indiana.

In fact, Cisco's first Hybrid Work Index report found that hybrid workers remain a prime attack vector and that malicious remote access attempts increased 240 percent during the pandemic.

This, of course, is compounded by the fact that the overall leading cause of cybersecurity breaches are still people. According to the Verizon 2021 Data Breach report, 85 percent of breaches were caused by a human element. The 2021 Verizon Data Breach report also found that 61 percent of attacks involved use of unauthorized credentials, and phishing rose to 36 percent (up from 25 percent). And when one phishing exercise — like a malicious email — hits its target, the whole organization is at risk of compromise.

Indiana's History in Cybersecurity

To understand how the Council came to be, it is important to understand the history of the state's cybersecurity efforts.

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 was 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.

After this inaugural cyber exercise, it became even 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. While the Indiana Executive Council on Cybersecurity (IECC or Council) was established in 2016, it did not become operational until Governor Eric J. Holcomb took office, with a renewed focus and priority through his decision to extend Executive Order 17-11 (See Appendix A).

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 Security Council, and report to the Homeland Security Advisor within the Office of the Governor.

Given the challenges and complexities surrounding the Executive Order's aims, it became imperative in 2017 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. The purpose of this unique role was for information to be shared across agencies 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.

Using a comprehensive approach to its strategy as described in the next section, the Council delivered an actionable strategic plan to Governor Holcomb on Sept. 21, 2018. The *2018 Indiana Cybersecurity Strategic Plan* encompassed not only the breadth of topics but the depth as well. While the more than 2,000-page 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 their sector within the state.

The *2018 Cybersecurity Strategic Plan* can be found at www.in.gov/cybersecurity.

Developing the Council and the Strategy

To build and best utilize the cross-sector body of subject-matter experts to effectively understand Indiana's cyber risk profile, identify priorities and develop resources that those who needed it most could access them, and leverage the convened talent from all sectors to stay on the forefront of the cyber risk environment, the Cybersecurity Program Director worked with leadership to establish a strategic framework to be successful in Indiana's cybersecurity initiatives.

Composition of the Council

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.

Since 2017, the Council has reviewed its Charter, members, and priorities during its quarterly meetings. For example, its Charter, found in Appendix B, is reviewed, and voted on every year, which 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 originally organized into 20 committees and working groups composed of the more than 250 respective members who are experts in their relative fields. As more complex, mature deliverables were crossing over into other committees and working groups it was important to leadership to remain efficient and respectful of those who served on the Council. In January 2020, the Council moved its organization into 15 committees and working groups (See Figure 1). Maintaining this cybersecurity ecosystem while remaining flexible to the work the Council was doing was the only way to achieve maximum results in a relatively short amount of time with the depth of knowledge needed to make informed operational decisions. This became even more important as the world changed in the following months.

Each committee/working group has a smaller charter that 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 were chaired by a Voting Member of the Council to ensure that all plans were aligned with the goals of the entire Council.

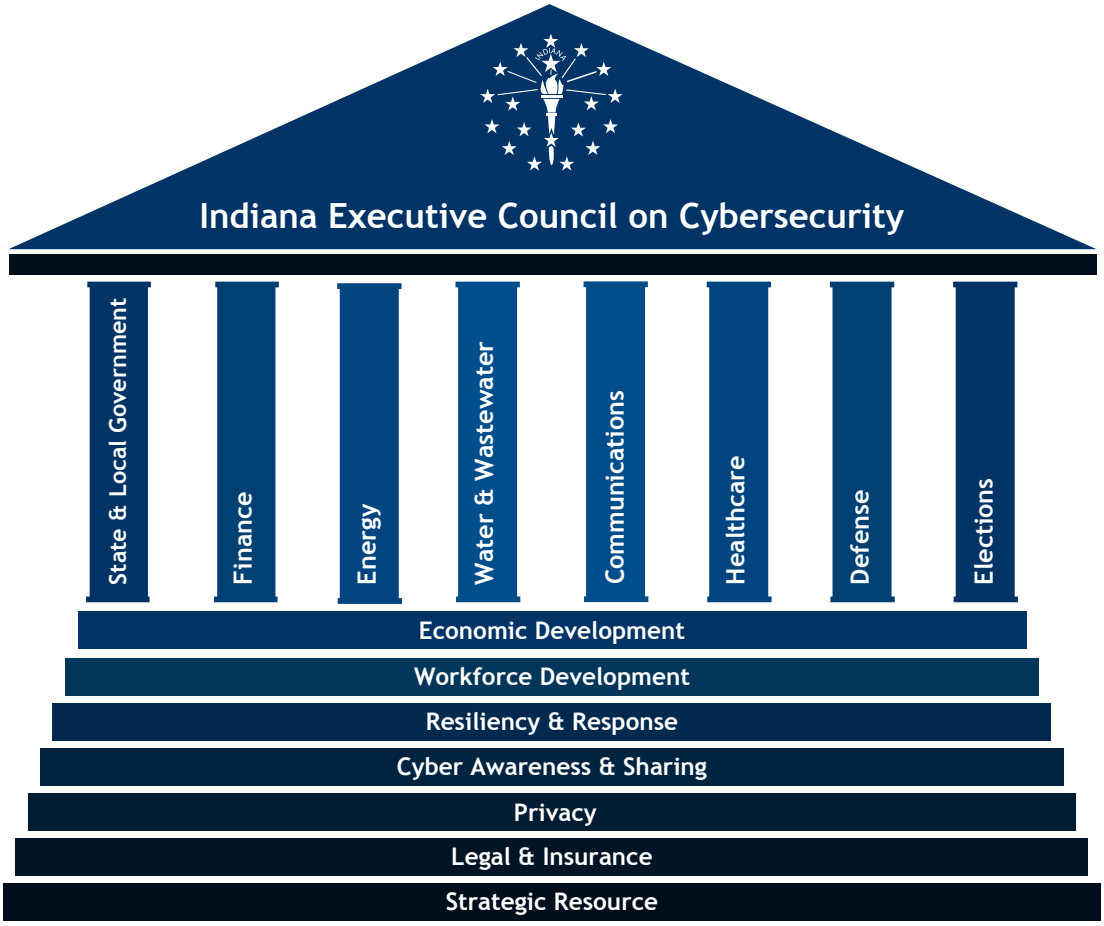
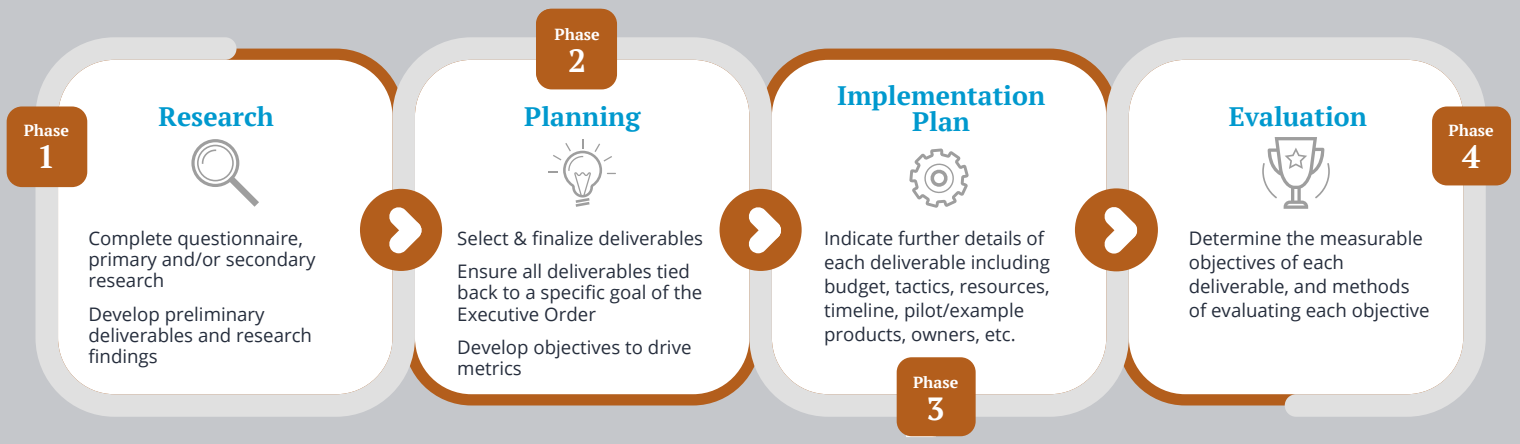


Figure1: IECC Strategic Breakdown

The Council Strategic Phases

To guide the work of the 15 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



In addition, meetings, facilitated discussions, director oversight, shared online platforms, and tools were implemented to avoid duplication of efforts, and to allow for a fully transparent process. 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 indicates the specific deliverables that were 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 the Council with required membership. 2017-2021 – Council has remained active and has met every quarter and have always met quorum
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	Passed IECC Charter annually September 2018 2018 & 2021 - Submitted final strategic plans 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 and October 2021 - 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 Counterterrorism 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 through October 2021 – 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	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	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 15 committees and working groups each developed a comprehensive strategic implementation plan that collectively resulted in 68 deliverables and 134 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 combined with a considerable number of donated services, time, and resources from local government entities, academia, and private sector organizations.

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. 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, funding and resources may change as this plan is updated and implemented.

STATE AND LOCAL GOVERNMENT COMMITTEE

Deliverable: Indiana's Cybersecurity Hub Website

Objective 1: IECC will conduct a major review and update of the Cyber Hub website by August 2022.
Objective 2: Increase website traffic to www.in.gov/cyber by 100 percent by September 2023.
Objective 3: Conduct an annual review and update the Cyber Hub website by September of every year.

Deliverable: Cyber Emergency Resiliency and Response State Guide – Update

Objective 1: The State of Indiana will update and distribute the Indiana Cyber Emergency Resiliency and Response State Guide by October 2023.

Deliverable: Local Officials Cybersecurity Guidebook 2.0

Objective 1: The State and Local Government Committee will update and distribute the Indiana Local Government Cyber Guidebook by May 2023.
Objective 2: The State and Local Government Committee will encourage the downloading of 1,000 Indiana Local Government Cyber Guidebooks by May 2024.

Deliverable: Local Government Cyber Engagement Program

Objective 1: The State and Local Government Committee, with the assistance of IECC partners and the National Governors Association, will develop the Local Government Cyber Engagement Program by January 2022.
Objective 2: The State and Local Government Committee, with the assistance of IECC partners and the National Governors Association, will pilot the Local Government Cyber Engagement Program with at least five local government entities by June 2022.

Objective 3: The State and Local Government Committee with the assistance of IECC partners will publicly launch the Local Government Cyber Engagement Program by January 2023.
Objective 4: As a result of outreach efforts, at least 30 local government entities will have begun using the Local Government Cyber Engagement Program by December 2023.

Deliverable: Identity Theft State Roundtable
Objective 1: Indiana Department of Workforce Development (DWD) and Indiana Office of Technology (IOT) will lead a round table discussion with other key state agencies about best practices with defending against identity theft and fraud.

Deliverable: Local Government Cybersecurity Podcast Series ("Days of Our Cyber Lives")
Objective 1: Completion of a 15-minimum episode podcast series on cybersecurity topics for a Hoosier local unit of government audience over the course of one year, available via audio-only (e.g., Apple Podcasts) or video and audio (YouTube) by October 2021.
Objective 2: Realizing greater than or equal to 900 combined views & listens for the series by October 2021.

ELECTIONS COMMITTEE

Deliverable: Collaboration with State, Federal, and Sector Communities
Objective 1: The new Secretary of State will actively engage with allied organizations indicated in the state's strategic plan by Dec. 31, 2021.
Objective 2: The Secretary of State will continue to engage in election cybersecurity collaboration with allied organizations every year as appropriate.

Deliverable: Integration of Cybersecurity Professionalism, Awareness, and Practice
Objective 1: The Secretary of State will promote integration of experienced, trained, and professionally certified cybersecurity resources into all phases of election administration by November 2024.
Objective 2: More than 80 percent of state and local election officials and administrators will be provided ongoing cybersecurity awareness, training, and/or certification opportunities by November 2024.

Deliverable: Election Infrastructure Monitoring, Hardening, Testing, and Auditing
Objective 1: The Secretary of State will promote election infrastructure monitoring, hardening, testing, and auditing improvements every year until December 2024.

Deliverable: Public Engagement and Confidence
Objective 1: The Secretary of State will maintain a high level of public engagement in the area of election security and public confidence by November 2024.

Deliverable: Continuity, Coordination, Maintenance of Effort and Oversight
Objective 1: Indiana Statewide Voter Registration System Core Team will begin formally coordinating and overseeing the deliverables of the IECC Elections Committee Strategic Plan by Dec. 31, 2021.
Objective 2: Indiana Statewide Voter Registration System Core Team will assist with all the deliverables and objectives in the IECC Elections Committee Strategic Plan and report the progress to the IECC by Dec. 31 of each year.

ENERGY COMMITTEE

Deliverable: Critical Infrastructure Information (CII)

Objective 1: IECC Energy Committee will provide a review of the July 2018 definitions by October 2021.

Objective 2: IECC Energy Committee will review potential state policy changes to protect critical infrastructure information while maintaining public access and freedom of information by December 2021.

Deliverable: Training

Objective 1: Develop a survey to determine whether there are new training needs specific to the energy industry following the Pandemic by October 2021.

Objective 2: Identify and recommend opportunities at the state, vocational, or higher education level December 2021.

Deliverable: IURC Cybersecurity Forum

Objective 1: Indiana Utility Regulatory Commission (IURC) will host a cybersecurity forum for small natural gas utilities to share industry information and best practices by December 2021.

Deliverable: Resource Guide

Objective 1: The IECC Energy Committee will define emerging technology and supply chain issues related to the grid Qtr. 3 2022.

Objective 2: The IECC Energy Committee will determine whether best practices and information are widely available Qtr. 3 2022.

Objective 3: The IECC Energy Committee will develop an industry specific resource guide Qtr. 4 2022.

Deliverable: Workplace IT

Objective 1: The IECC Energy Committee will develop a survey to identify challenges in the workplace for the energy sector in Qtr. 4 2021.

Objective 2: The IECC Energy Committee will identify issues stemming from the work-from-home environment in Qtr. 4 2021.

Objective 3: The IECC Energy Committee will share best practices and coordinate with other sectors as needed in Qtr. 1 2022.

FINANCE COMMITTEE

Deliverable: Board Leadership Education Plan

Objective 1: IECC Finance Committee will develop a curriculum and identify an instructor(s) to be used for the Board and Executive Leadership Education Plan by June 2022.

Objective 2: The Board and Executive Leadership Education will be provided to a pilot group of finance institutions by December 2022.

Deliverable: Disruption Plan and Communication Evaluation

Objective 1: IECC Finance Committee will develop a Finance Sector Disruption Plan for the State of Indiana by Qtr. 3 of 2023.

Objective 2: The IECC Finance Committee will evaluate communication opportunities and identify associated barriers by Qtr. 4 of 2023.

Deliverable: Top Security Tips Material 2.0

Objective 1: IECC Finance Committee will review and distribute the Top Information Security Tips 2.0 training material for Indiana businesses by December 2022.

WATER AND WASTEWATER COMMITTEE

Deliverable: Cyber Contact List

Objective 1: Indiana Department of Environmental Management maintains a cybersecurity contact information for 85 percent of Indiana water and wastewater organizations to be reviewed annually.

Deliverable: Cyber Risk Model (Plan) – Update

Objective 1: The Water/Wastewater Committee and partners will review and update the Cyber Plan Template for Indiana water/wastewater companies in 2022.

Objective 2: Make the updated Cyber Plan Template available online and distribute to water/wastewater utilities by in 2022.

Deliverable: Risk Tool

Objective 1: Water/Wastewater Committee develops Cyber Assessment Risk Tool within 12 months of securing funding.

Objective 2: Make tool available to 80 percent of Indiana AWWA members on AWWA.org for use by Indiana W/WW companies within 12 months of launching.

Deliverable: Training Plan

Objective 1: Water/Wastewater Committee develop an initial training plan by June 2021 and full training plan within three months of funding.

Objective 2: Seventy percent of Indiana water and wastewater companies incorporate the training plan as a part of their operational resources within 24 months of deployment of training plan.

Deliverable: Cyber Plan Template – Update

Objective 1: IECC Water and Wastewater Committee and partners will distribute the updated Cyber Plan Template to 50 percent of Indiana water and wastewater companies through a variety of methods (including virtual) by March 2022.

Deliverable: Water/Wastewater Exercise and Response Education

Objective 1: IECC Water and Wastewater Committee and partners will participate in US DHS CISA Exercise August 2021.

Objective 2: IECC Water and Wastewater Committee and partners will participate in INNG Hoosier Defender August 2021.

Objective 3: Working with partners, develop a water/wastewater virtual workshop launch by October 2021.

Objective 4: Promote virtual workshop that result in at least 100 registrants by October 2021.

COMMUNICATIONS COMMITTEE

Deliverable: Establish Voluntary Industry Contact List

Objective 1: IECC Communications Committee will develop a form and process to collect a central cyber industry contact list by Qtr. 2 of 2022.

Objective 2: Seventy percent of all communications providers complete annual cyber contact form by December 2022.

Deliverable: Terminology Glossary – Update

Objective 1: IECC Communications Committee will update Communications Sector Terminology Glossary by December 2021.

Objective 2: IECC Program Communications Manager will publish the Communications Sector Terminology Glossary to IECC website by January 2022.

Deliverable: Broadband and Local Government Education

Objective 1: IECC Communications Committee will complete the rural broadband education packages by January 2023.

Objective 2: IECC Program Communications Manager will publish the rural broadband education packages by February 2023.

Objective 3: Working with identified partners, provide cyber 101 tips for 1,000 individuals and organizations who are learning to operate with high-speed internet by December 2024.

Deliverable: Cyber Incident Response Engagement Guide

Objective 1: IECC Communications Committee will develop the Communications Sector Engagement Guidance by May 2022.

Objective 2: Communications sector partners will distribute the Communications Sector Engagement Guidance to eighty percent of identified industry and key stakeholders by June 2022.

HEALTHCARE COMMITTEE

Deliverable: Long-term Education

Objective 1: IECC Healthcare Committee will update Indiana-focused versions of security education in 2022.

Objective 2: IECC Healthcare Committee and partners will provide updated Indiana-focused versions of security education to 80 percent of Indiana healthcare providers in 2022.

Objective 3: IECC Healthcare Committee and partners will collect customer effectiveness, usage, and/or feedback survey for future development in 2023.

Deliverable: "Healthcare Cyber in a Box"

Objective 1: IECC Healthcare Committee will create a "Healthcare Cyber in a Box" of security education designed for small- to medium-size offices and systems in 2022.

Objective 2: Healthcare Committee and partners will distribute Healthcare Cyber in a Box of security education information to 80 percent of Indiana healthcare providers.

Objective 3: IECC Healthcare Committee and partners will measure feedback/usage of the toolkit by 2023.

Deliverable: Vendor Management - Healthcare IT Security, Risk & Compliance Handbook

Objective 1: IECC Healthcare Committee will draft the initial document including key outline of processes and procedures Indiana providers need to implement by Qtr. 1, 2022.
Objective 2: Circulate the document among the IECC Healthcare Committee for revisions and edits by Qtr. 2, 2022.
Objective 3: Implement Committee feedback and finalize document by Qtr. 2 of 2022.
Objective 4: Publish final draft on the Indiana Cybersecurity website by Qtr. 3 of 2022.

Deliverable: Exercise

Objective 1: Working with partners, participate in a statewide cyber exercise that affects healthcare industry by August 2021.
Objective 2: Working with partners, participate in an exercise with the National Guard at Muscatatuck by August 2021 that addresses a known cyber vulnerability.

Deliverable: Cyber Sharing Platform

Objective 1: IECC Healthcare Committee will beta test with the Cyber Awareness and Sharing Working Group by Qtr. 1 2022.

DEFENSE INDUSTRIAL COMMITTEE

Deliverable: Cyber Market System

Objective 1: IEDC Defense Development and partners will review the current cybersecurity market pursuit plan and system in 2021.

Deliverable: Cyber Digital Platform

Objective 1: IEDC Defense Development and partners will develop a pilot of the Indiana defense cybersecurity market development and capture plan and system (Digital Platform) by 2021.
Objective 2: Indiana increases to two percent (about $300M) of the Department of Defense (DOD) cybersecurity market share ($15B plus) by FY 2025.

Deliverable: Cyber Statewide Testbed

Objective 1: Establish a nationally recognized cybersecurity test bed in Indiana by June 2021.
Objective 2: Indiana captures five percent of international cybersecurity market share of cybersecurity test, training, and demonstration plan and capability by December 2025.

Deliverable: Cybersecurity Capability Maturity Model (CMMC) Program

Objective 1: IEDC and partners will develop a Cybersecurity Capability Maturity Model (CMMC) framework in Indiana by December 2021.
Objective 2: IEDC and partners will promote Cybersecurity Capability Maturity Model (CMMC) in Indiana to 80 percent of key stakeholders and associations by January 2022.

ECONOMIC DEVELOPMENT COMMITTEE

Deliverable: Investment

Objective 1: The Economic Development Committee with the IEDC will develop an economic development support framework for Indiana companies to thrive in the cybersecurity landscape by December 2022.

Objective 2: Companies that move, start, or grow here will have a framework for economic development support by December 2023.

Deliverable: Leadership

Objective 1: Indiana Economic Development Corporation and Committee will work to identify potential partners, activities, and initiatives of cybersecurity influencers in the State of Indiana by December 2022.

Objective 2: Measure the effectiveness of IEDC supported activities and initiatives in the cybersecurity space by December 2023.

Deliverable: Technical Assistance

Objective 1: IEDC and partners will develop a cybersecurity technical assistance plan in Indiana by January 2022.

Objective 2: Measure the effectiveness of the Cybersecurity technical assistance plan by the number of participants (40) by February 2023.

WORKFORCE DEVELOPMENT COMMITTEE

Deliverable: Enhance CyberseekIN.org Data Tool - Workforce Pillar

Objective 1: Indiana DWD add Credential Engine certifications data to CyberseekIN.org (training providers) by June 2022.

Objective 2: Indiana DWD continue Data enhancements to CyberSeekIN.org including continual updates to training providers, Apprenticeship Data/Opportunities, and Promote opportunities, training, events surrounding cybersecurity in Indiana by October 2022.

Deliverable: Cybersecurity Talent Pipeline and Job Openings Dashboard - Workforce Pillar

Objective 1: Indiana Department of Workforce Develop will create cybersecurity workforce dashboard metrics – measuring Indiana's job demand, talent pipeline, apprenticeships, and training opportunities by January 2022.

Deliverable: K-12 Cybersecurity Content - K-12 Pillar

Objective 1: Governor's Workforce Cabinet with support from IDOE will develop and promote a high school CTE Program of Study in Cybersecurity by June 2022.

Objective 2: Indiana Department of Education will develop a menu of cybersecurity-related professional development and resources, including K-12 computer science offerings, by June 2022.

Objective 3: Indiana Department of Education and Cybersecurity Program Director will edit and distribute the Cybersecurity for Education Toolkit 2.0 by February 2022.

Deliverable: Promote Cybersecurity Training Across the K-12 Sector to Protect the Educational Process - K-12 Pillar

Objective 1: The joint Cybersecurity Task Force ensure more than 75,000 staff and students are delivered training and phishing support through the KnowBe4 platform by December 2024.
Objective 2: The joint Cybersecurity Task Force will raise awareness of schools to digital threats to the educational process by raising awareness through monthly newsletters, and by working with partners to provide professional development for school IT staff by December 2024.
Objective 3: DOE will work to encourage all schools to appoint one staff member to monitor information releases from the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the Indiana Information Sharing and Analysis Center (IN-ISAC) by December 2023.
Objective 4: Create a DOE Moodle Community to share school cybersecurity information with public, religious, and private schools as well as provide opportunities for secure collaboration and sharing of best practices by December 2021.

Deliverable: Update Cyber Program Data Tool (CHE) - Higher Education Pillar

Objective 1: Commission for Higher Education will re-launch survey/tools to capture and collect program course curriculum to help the IECC understand and inventory which higher ed schools are providing cybersecurity related training programs by December 2021.
Objective 2: Commission for Higher Education will update the Cyber Program Data Tool and Report by March 2022.

PRIVACY WORKING GROUP

Deliverable 1: Indiana PII Guidebook

Objective 1: IECC Privacy Working Group update the Indiana PII Guidebook for government and general public by the end of April 2022.

Deliverable 2: Indiana Privacy Toolkit

Objective 1: IECC Privacy Working Group develop an Indiana Privacy Toolkit for the Indiana business community, public sector, and local government by July 2022.
Objective 2: At least 200 users have accessed/downloaded the Indiana Privacy Toolkit for the Indiana business community, public sector, and local government by April 2023.

CYBER AWARENESS AND SHARING WORKING GROUP

Deliverable: Public Relations Campaign Plan - Update

Objective 1: The IECC Communications Program Manager will use the 2018 Statewide PR Cybersecurity Campaign Plan and develop a phased approach to the tactics as resources allow by December 2021.
Objective 2: IECC Communications Program Manager will leverage the assets of Indiana's cybersecurity program to create an increasingly larger presence on social media channels including Twitter, Facebook, and LinkedIn increasing its subscription by 30 percent each fiscal year.
Objective 3: The IECC Communications Program Manager will utilize a weekly blog as a tool for measurably increasing public awareness by further positioning Indiana as a leader in cybersecurity and increasing its subscription by 25 percent each fiscal year.

Deliverable: Inventory of Cyber Sharing Resources

Objective 1: IECC Cyber Awareness and Sharing Working Group will complete an inventory of cyber sharing resources by August 2021.

Deliverable: MS-ISAC Member Recruitment

Objective 1: Indiana-ISAC will work to increase MS-ISAC membership by 25 percent each calendar year.

Deliverable: Best Practices

Objective 1: IECC Cyber Awareness and Sharing Working Group will update a list of best practices by July 2022.

Deliverable: Cyber Sharing Maturity Model

Objective 1: IECC Cyber Awareness and Sharing Working Group will edit and post the Indiana's updated cyber sharing maturity model by July 2022.

Objective 2: ECC Cyber Awareness and Sharing Working Group will distribute Indiana's updated cyber sharing maturity model to critical infrastructures through ninety percent of Indiana associations by August 2022.

Deliverable: Cyber Sharing Community - Slack Channel

Objective 1: IECC Cyber Awareness and Sharing Working Group will create the Slack Channel by May 2021.

Objective 2: IECC Cyber Awareness and Sharing Working Group and IECC Healthcare Committee will conduct a beta test of the Slack Channel by December 2021.

Objective 3: Complete the Live Production Launch of the Slack Channel by January 2022.

CYBER RESILIENCY AND RESPONSE WORKING GROUP

Deliverable: State Cyber Exercises

Objective 1: The State of Indiana will develop and execute a Cross-Sector Critical Infrastructure Cyber Table Top Exercise by August 2021.

Objective 2: IECC will work with INNG to incorporate a cyberattack into a natural disaster exercise during the Homeland Defender Exercise by August 2021.

Objective 3: The State of Indiana will develop and execute a Cross-Sector Critical Infrastructure Cyber Operational Exercise by 2023.

Deliverable: Cyber Emergency Education to Local Law Enforcement

Objective 1: ISP and Cybersecurity Program Director work to develop the Cyber Emergency Response Education for Local Law Enforcement by May 2022.

Objective 2: ISP and IECC partners distribute the Cyber Emergency Response Education to 80 percent of Local Law Enforcement by June 2022.

Deliverable: Emergency Manager Cybersecurity Toolkit 3.0

Objective 1: IECC Emergency Services and Exercise Working Group will update the Emergency Manager Cyber Response Toolkit 3.0 by March 2022.

Objective 2: IDHS will launch a workshop using the Emergency Manager Cyber Response Toolkit 3.0 by April 2022.

Deliverable: Cyber Annex and Cyber Liaison

Objective 1: IDHS will edit and distribute the IDHS Cyber Annex to appropriate parties by Qtr. 3 of 2022.

Objective 2: IDHS and IECC partners will exercise the IDHS Cyber Annex with the cyber liaisons by December 2023.

Deliverable: INNG Cyber State Capabilities

Objective 1: The Indiana National Guard will inform state leadership of their cyber response capabilities to a statewide cyber emergency when directed by a federal disaster declaration or ordered to State Active Duty by the Governor by December 2024.

LEGAL AND INSURANCE WORKING GROUP

Deliverable: Cyber Insurance Toolkit

Objective 1: IECC Legal and Insurance Working Group will develop a Cyber Insurance Toolkit to be provided to government and businesses by April 2022.

Objective 2: With an effective communications plan, point more than 1,000 users access the Cyber Insurance Toolkit by December 2023.

Deliverable: Policy Review

Objective 1: Legal and Insurance Working Group will review and distribute a list of cyber laws applicable to Indiana businesses and residents under the current landscape every year in December.

Deliverable: Funds Transfer Fraud Fact Sheet

Objective 1: IECC Legal and Insurance Working group will develop a Funds Transfer Fraud Fact Sheet to be provided to government and businesses by January 2022.

Deliverable: Cyber Insurance Survey - Post-Covid

Objective 1: Legal and Insurance Working Group with Indiana University will conduct a post-COVID survey of businesses for insurance coverage and cybersecurity insurance coverage by June 2022.

Objective 2: IECC Legal and Insurance Working Group with Indiana University will provide a report of the findings of the cyber insurance survey to the IECC by September 2022.

STRATEGIC RESOURCE COMMITTEE

Deliverable: Policy Research Report

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

Deliverable: IECC Scorecard 2.0

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.

Objective 2: IECC will pilot Indiana's Cybersecurity Scorecard 2.0 with Level Up Guide with local governments by July 2022.

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

Deliverable: Indiana Cyber Success Report (2017-2021)

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.

Deliverable: IECC 2021 Strategic Plan

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

Deliverable: Outreach to Underrepresented Sectors

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

Objective 2: Provide industry contacts with education materials and set up a regular communication cadence for each industry by March 2023.

Observations and Considerations of the IECC

Defining cybersecurity—and efforts to protect against cybersecurity threats—must be illustrated in a way that is simple yet effective, complete yet attainable. Although cybersecurity has a lot of ins, a lot of outs, a lot of what-have-yous with a lot of strands to keep in our heads, it must be demystified. 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 towards a multi-disciplinary solution to deal with such an extensive threat. It must encompass not only government at all levels, but Indiana businesses at all levels and sized, and, indeed, all Hoosiers, if it is to be effective. 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. The cyber threat is a dynamic environment. Instead, effective cybersecurity is best understood through a lens of evidence-based risk reduction.

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 ubiquitous threat it poses to all Hoosiers, which is why the Governor and state lawmakers continue to champion its importance. As with many important issues, the success of a cybersecurity strategy depends on the resources and funding available to support its implementation. It is also important to note that while these implementation plans have estimated time frames, budgets, and resources, they are agile in nature and will be updated as progress and corrections are driven by the expertise of the members on those committees and working groups.

It is imperative that the Council remains agile, 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. As many of these deliverables are being implemented, their nature and scope may change commensurate with the participants who are advising on them and the ever-evolving cyber landscape. The Council will continue to 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.

2021 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 where 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 the development of local government cybersecurity resources and education;
- Providing necessary support to the critical infrastructures as they move forward with their many deliverables This includes planning, training, and exercising in preparation of a cyberattack (e.g. working with small operators in safe environments such as Muscatatuck).
- 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 supporting the necessary cybersecurity experts, tools, and service providers as the cyber threat continues to evolve.

Part 3
Real People, Real Work

2018-2021 Membership and Leadership

Since its first strategic plan in 2018, the Council has been supported by more than 200 members consistently each year. Of those, Voting and Advisory Members were selected to lead the 15 committees and working groups. For a full list of the members and committee and working group leadership from 2018 - 2021, see Appendix E. It is important to note that while members have come and gone due to job changes, life changes, etc., every member has been a significant reason why the Council has been so successful.

Council Stats

2018

214 Members

22 of 69 Deliverables Completed

42 of **120** Objectives Completed

2019

256 Members

17 of 69 Deliverables Completed

36 of **120** Objectives Completed

2020

246 Members

8 of 69 Deliverables Completed

9 of **120** Objectives Completed

2021

238 Members

7 of 69 Deliverables Completed

93 of **120** Objectives Completed

Total

350+ Members

54 of 69 Deliverables Completed

93 of **120** Objectives Completed

Best Practices of the IECC

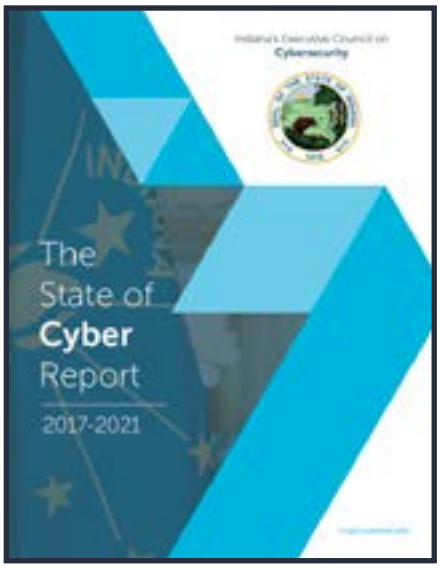
The Council has accomplished an unprecedented amount of work for the citizens and businesses of Indiana in the last four years due to the commitment of the public, private, military, and academic partnerships. Cybersecurity is not an issue that merely affects information technology professionals but one that affects all Hoosiers and businesses. Taking cybersecurity to the *Next Level* cannot be done by one entity alone. It is achieved by working 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.

When leadership is asked about what makes the IECC so unique and successful, the following best practices are shared:

- **Culture is everything.** Culture of the Council has always centered around empowerment of all our members and partners. No one entity owns cybersecurity. The state is a key facilitator but puts a lot of trust in the subject matter experts. No one needs to ask permission to do a cyber initiative. They are the experts. If a sector that is not the state feels that based on their research a particular initiative should happen, the state does not question their expertise. Instead, the state does its best to support their efforts as they lead and complete it.
- **Variety is the key ingredient to success.** The wide variety of the subject matter experts who drive the Council's innovative thinking and execution of initiatives come from public, private, academic, and military industries. But one representative on the council will not provide you the breadth and depth of viewpoints needed for a successful plan. It is important to have regional representatives (north, central, and southern Indiana) in all the committees and working groups as well as small, medium, and large entities in that sector to ensure that diverse input is provided in developing strategic plans.
- **A neutral program director.** The State of Indiana hired its first fully dedicated cybersecurity program director in March 2017 to develop the strategic framework and facilitate the Council in fulfilling its purpose. Having a director whose primary objective is not one agency's mission, but the Governor's Executive Order, has assisted the director to really understand and better represent the state as a whole instead of just one agency. It has also been beneficial that the director is not a project manager or a technologist, but is an executive who understands how government, private sector, military, and academia works with first-hand experience; respects and understands the politics (big and small) but is not political; and is a proven business strategist and effective communicator.
- **State agencies work together.** For the better part of a decade the Chief Information Officer (CIO) of the State and the Executive Director of the Indiana Department of Homeland Security have been working hand-in-hand on cybersecurity. There is not one agency in charge. In fact, much of what Indiana has done is seek to understand every agency's role in cybersecurity and embrace it within the process, not fight about it. When agencies are heard and respected, they are more willing to come to the table. This has been true with the state agencies on the Council. It is also important that the Governor has encouraged this collaboration because that is the only way we can be successful as a state.
- **Set expectations early and often.** Every year the Council reviews the membership and the Charter. And every year, the Council leadership ensures that the members are aware of the time expectations, the deadlines, the priorities, and the challenges to problem solve together. That is why meeting quarterly as a whole Council is important to its communication efforts and success.

- **Templates are key.** With so many committees and working groups and so many executives providing a volunteer service, providing templates to guide discussions and communicate what each team is doing is important to the organization, effectiveness, and efficiency of the Council.
- **Respect time.** From the beginning, it was made very clear that if a member felt like a meeting was a waste of time to be open about that frustration and the program director will see what can be improved. Being respectful of every member's time as well as making sure that when they attend a meeting, they feel excited to be a part of something that is helpful to others is a point of reference to be checked on a consistent basis. This is why it is believed all the meetings are still very well attended.
- **Be flexible.** Recognizing that we have a plan with set dates and objectives is important to every executive on the Council, but also recognizing that things happen (like a worldwide pandemic) and there is no failure is shifting things around and pausing initiatives because members are working 50-70 hours at their full-time jobs. Also being clear from the beginning of every plan that things will happen, people will change jobs or need to step away and objectives may need to be updated is also okay and not deemed a failure. In fact, even with all that has happened over the last couple of years, the Council still completed a majority of their deliverables. That is the true success.
- **Be transparent.** If all members have access to many of the inner workings of the planning and implementation of each plan, then there are never questions of impropriety or assumptions that are not correct, which in many cases can distract from what we are trying to accomplish. Since 2017, there has never been an issue raised because everything is there for members to see. And if they have questions, the Director will have transparent conversations of any possible concerns there may be.

No Smoke and Mirrors Here…



Each committee and working group followed the four-step strategic process (research, planning, implementation, and evaluation). This process provides Indiana a very accurate understanding of the many challenges facing the state, as well as the many current and possible solutions that can enhance cybersecurity at all levels. Through work of these committees, there is not just talk on how to protect Indiana from cyber threats, but there are actual plans followed by action.

In 2018, the Council submitted to the Governor a strategic plan that to some may have been too aggressive and, with a strategic framework that had never been used in the nation. And while there were those who were not sure how this complex ecosystem approach would work, the Council not only completed 78 percent of its total 69 deliverables, and 77 percent of the 120 objectives, but has seen some tremendous successes outside the Council as well.

So many private, public, academic, and military organizations along with individuals who just want to make a difference in cybersecurity have succeeded where others have not. It is an honor to be the state that supports these endeavors whether directly with the Council or from afar with acknowledgment. To learn more about the successes of the *2018 Indiana Cybersecurity Strategic Plan* and other accomplishments of cyber warries in our state, read the "2021 State of Cyber Report" found at www.in.gov/cybersecurity.

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. Council membership also will be reviewed and recruitment of experts in the fields will be ongoing.

The Council also will continue to provide 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.

The goal of the Council is to move cybersecurity to the *Next Level* in Indiana. However, we must do this 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. By providing resources to those organizations who need it most 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 Indiana. With the continued guidance and support of experts throughout the State of Indiana, Hoosiers will continue to be safer, and businesses will continue to thrive.

Appendices

- Appendix A Indiana Executive Council on Cybersecurity - Executive Order
- Appendix B Indiana Executive Council on Cybersecurity - Charter
- Appendix C IECC Phase Forms
- Appendix D IECC Committee and Working Group Implementation Plans
  - D. 1 Communications Committee
  - D. 2 Defense Industrial Committee
  - D. 3 Economic Development Committee
  - D. 4 Elections Committee
  - D. 5 Energy Committee
  - D. 6 Finance Committee
  - D. 7 State and Local Government Committee
  - D. 8 Healthcare Committee
  - D. 9 Water and Wastewater Committee
  - D. 10 Workforce Development Committee
  - D. 11 Resiliency and Response Working Group
  - D. 12 Cyber Awareness and Sharing Working Group
  - D. 13 Legal and Insurance Working Group
  - D. 14 Privacy Working Group
  - D. 15 Strategic Resource Working Group
- Appendix E IECC Membership and Leadership List 2018-2021