Indiana's Executive Council on
Cybersecurity

The State of **Cyber** Report

2017-2021

in.gov/cybersecurity

October 29, 2021

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 relaunch in July 2017, it quickly became evident that Indiana has a passionate, expert Council, who has established Indiana as one of the leading states in cybersecurity collaboration and initiatives in the nation.

In fact, the Council has completed 78 percent of its 69 identified deliverables, and 77 percent of the 120 objectives that were presented to you in September 2018. This was in spite of a worldwide pandemic. If anything, the pandemic has only validated the importance of cybersecurity not only for individuals and businesses, but especially for local governments.

In this report, you will find two parts. The first part is the history and direct success of the IECC since its relaunch of 2017. More than 350 members between 2017-2021 were directly involved with the researching, planning, implementing, and evaluating the *2018 Indiana Cybersecurity Strategic Plan*.

Altogether, the members donated hundreds of hours and millions of dollars in the way of expertise, services, and resources to Hoosier individuals, governments, and businesses.

The second part is a collection of other cybersecurity initiatives in Indiana outside of the IECC. And while this is not an all-inclusive list, it is an important sampling of the many amazing, innovative projects that continue to take Indiana to the *Next Level* in cybersecurity.

These two parts working together is the only way that Indiana has been so successful in its cybersecurity initiatives. In particular the efforts of our academic, military, private, and public partners are who truly make Indiana a leading state in cybersecurity.

What follows are the results from those who have the passion, dedication, and expertise to make a difference in our state, whether through the IECC or on their own with their organization. To learn more about the cybersecurity initiatives of Indiana, please contact the state's Cybersecurity Program Director Chetrice Mosley-Romero at RomeroCLM@iot.in.gov.

Sincerely,

Stephen Cox
Executive Director, Indiana Department of Homeland Security

Tracy Barnes
Chief Information Officer, State of Indiana

Table Of Contents

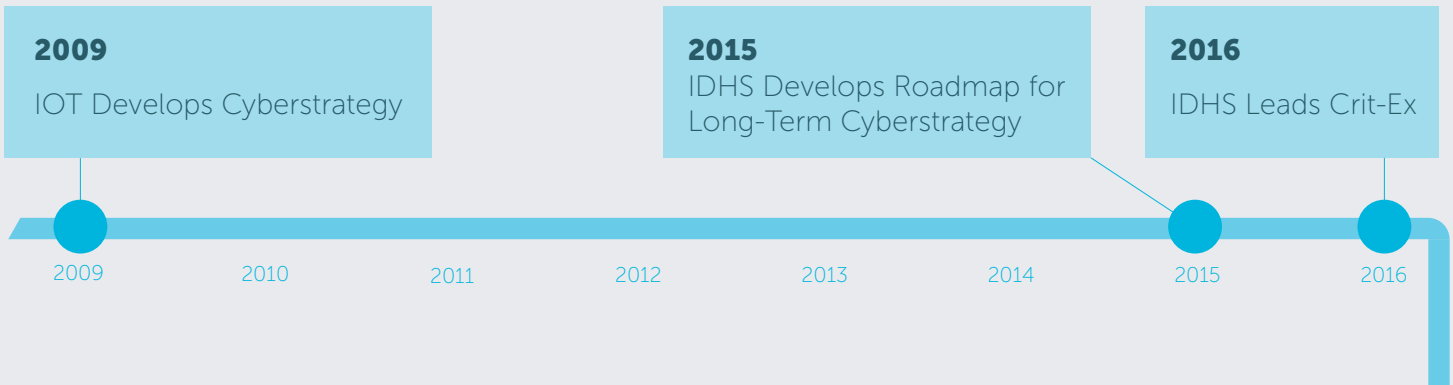
PART 1: The Indiana Executive Council on Cybersecurity

A Brief History of the IECC

When the State of Indiana became more centralized in its information technology, the Indiana Office of Technology (IOT) was ahead of many other states when it developed its state cyber strategy in 2009. This internal strategy provided state leadership with organization, governance, practices, and policies to be implemented in order to achieve an effective security approach. While inward focus and inter-agency coordination created a more efficient and effective way to work with many agencies, more needed to be done to protect the citizens and businesses of Indiana as cyber threats began to infiltrate the smallest of critical infrastructures.

In August 2015, the Indiana Department of Homeland Security (IDHS) conducted additional research and developed a roadmap of how to better collaborate and engage with public and private partners in developing a long-term cyber strategy for the state.

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. The initial phase of Crit-Ex was a full-day tabletop exercise that 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 second part of the Crit-Ex series was an operational exercise at the 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 in the nation that made clear that information sharing, training opportunities, partnerships, and response planning across the state was paramount.



2021 2020 2019 2018 2017

2021
IECC Delivers Second Strategic Plan and State of Cyber Report

2020
IECC Reorganizes into 15 Committees and Working Groups

2018
IECC Delivers First Strategic Plan

2017
Governor's Executive Order 17-11 and Councils Formed

After this inaugural cyber exercise, it was 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 a Governor's Executive Order established the Indiana Executive Council on Cybersecurity (IECC or Council), which was continued on Jan. 9, 2017, through Executive Order 17-11, when Governor Eric J. Holcomb took office.

Per Executive Order 17-11, Governor Holcomb tasked the state and its partners to:

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, as needed, 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 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 Council was first 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) from 2017-2019. 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.

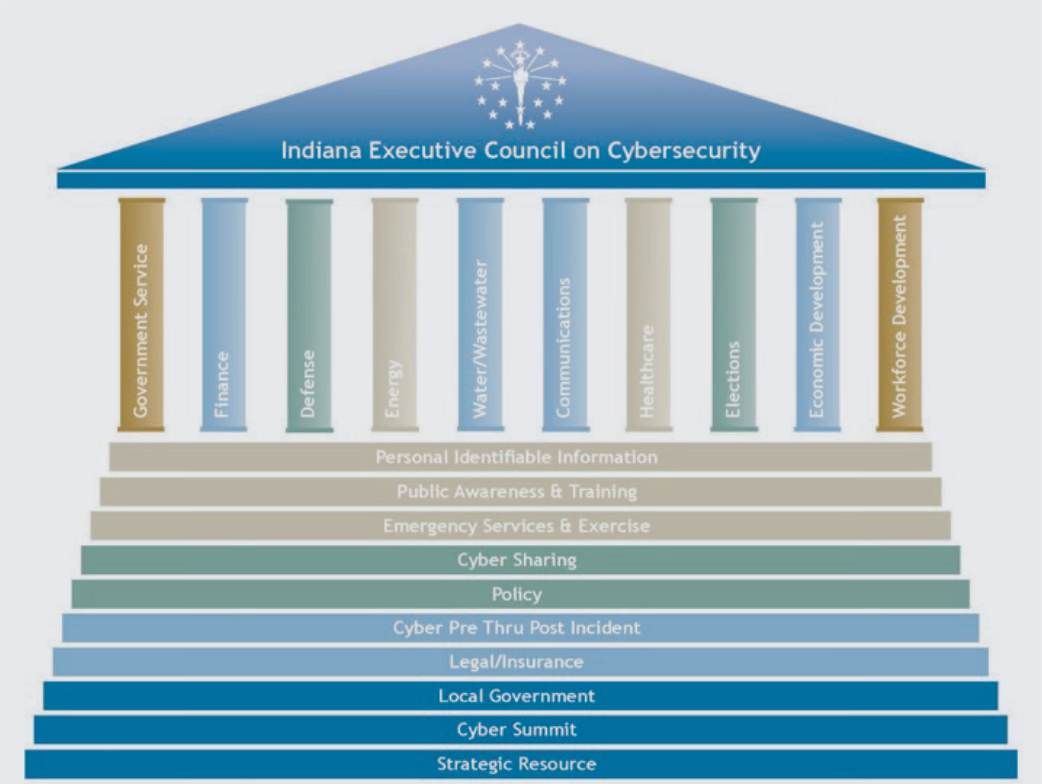


Figure 1. 2017-2019 Breakdown of IECC Committees and Working Groups

After the creation of the 20 committees and working groups, each committee and working group had to accomplish four things:

- A charter that established its purpose and goals
- A strategic plan that was the combination of the team's research, planning, implementation, and evaluation methodology
- Deliverables that the committee agreed to completing or leading with additional partners
- Provide the deliverables to the correct agencies, contacts, and associations so that the resources can be used by all when appropriate

On Sept. 21, 2018, the Indiana Executive Council on Cybersecurity delivered a comprehensive strategic plan to Governor Eric J. Holcomb per Executive Order 17-11.

The 2018 Indiana Cybersecurity Strategic Plan encompasses not only the breadth of topics but the depth as well. 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.

This is not a strategy to be completed by one entity alone. By working collaboratively with others, the State of Indiana has established long-term protection strategies that now provides Hoosier residents and businesses with the knowledge and infrastructure needed to be safer from the ever-evolving cyber threats.

Due to many deliverables that were not yet completed but cross overed other committees and working groups, the IECC was reorganized into 15 committees and working groups in January 2020 (See Figure 2).

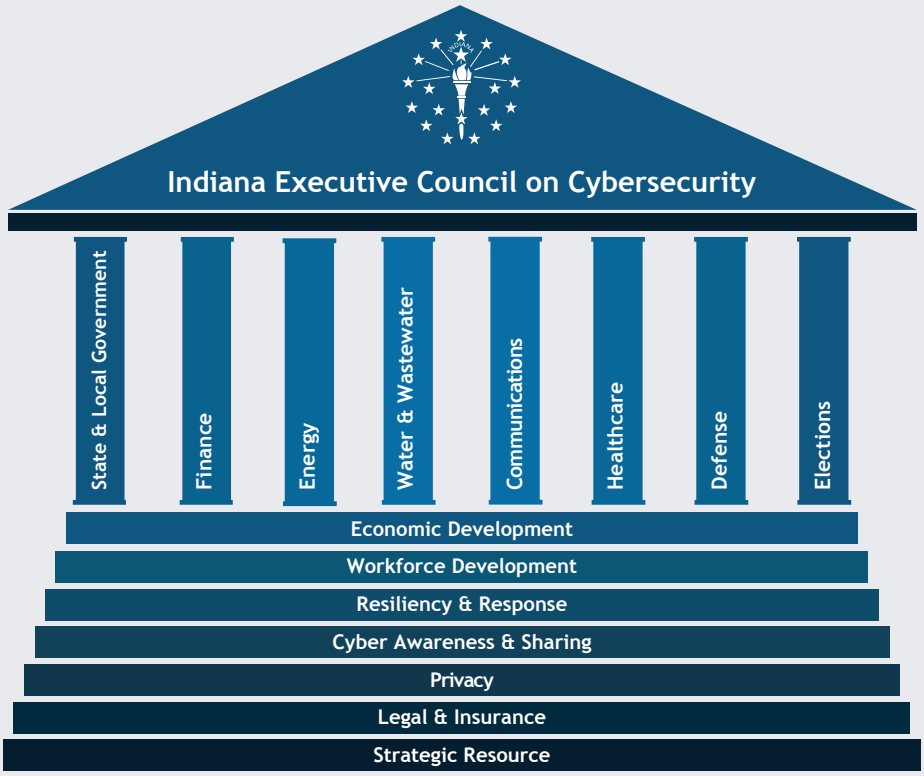


Figure 2. 2020-Present Breakdown of IECC Committees and Working Groups

It is important for any reader to understand that the creation of the IECC incorporated statewide representation. In order for this to be a true representation of the entire state, it was not enough to have representation who were conveniently located in and around the state capitol. In fact, the IECC leadership went out of their way to ensure that every committee and working group have at least 1 representative from the northern part of Indiana, southern part of Indiana, and central Indiana, a small company, a medium-sized company, a large company, an association, and more.

IECC Breakdown

Committee/Working Group Representation


Outside of Indianapolis


Northern Indiana


Central Indiana


Southern Indiana


Small Organizations


Medium Organizations


Large Organizations


Associations

Membership Breakdown

- Full Time
- Part Time
- Contributing
- Guests
- Voting
- Non-Voting (Federal partners)

More than 300 members between 2017-2021 were directly involved with the researching, planning, implementing, and evaluating the *2018 Indiana Cybersecurity Strategic Plan*. All together the members donated hundreds of hours and millions of dollars of services and resources to Hoosier individuals, governments, and businesses.

Following are the direct results of the IECC. No other state has accomplished this much from a voluntary cybersecurity Council in such a short amount of time and even through a pandemic. The results of this *State of the Cyber Report (2017-2021)* is entirely due to the passion and dedication of those who serve on the IECC and those who truly want to make a difference in our state.

69
Total Deliverables

54 Completed
2 In Progress
11 Put On Hold
2 Not Started

121
Total Objectives

93 Completed
3 In Progress
22 Put On Hold
3 Not Started

Deliverable Results of 2018 Cybersecurity Strategic Plan

COMMUNICATIONS COMMITTEE

	Complete %
Deliverable: Establish Voluntary Industry Contact List	
Objective 1: Develop a form and process to collect a central cyber industry contact list by September 2018.	✓
Objective 2: Seventy percent of all communications providers complete annual cyber contact form by December 2019.	10%*
Deliverable: Communications Sector Terminology Glossary	
Objective 1: Complete Communications Sector Terminology Glossary refresh by December 2019.	✓
Objective 2: Publish Communications Sector Terminology Glossary to IECC website by December 2019. Location: *www.in.gov/cybersecurity/government/best-practices-standards-and-resources/*	✓
Deliverable: Cyber Incident Response Engagement Guidance Engagement Guide	
Objective 1: Develop the Communications Sector Engagement Guidance by December 2019.	25%*
Objective 2: Distribute the Communications Sector Engagement Guidance to 80 percent of identified industry and key stakeholders by January 2020.	0%*
Deliverable: Communications Sector White Paper	
Objective 1: Complete the Communications Sector Whitepaper for the industry by December 2019.	✓
Objective 2: Distribute the Communications Sector Whitepaper to 80 percent of identified industry and key stakeholders by January 2020.	10%*

* = *Put on hold due to COVID-19*

DEFENSE INDUSTRIAL COMMITTEE

Deliverable: Cyber Digital Platform

	Complete %
Objective 1: Indiana Office of Defense Development (IODD) and partners will develop and implement a cybersecurity market pursuit plan and system by June 2021.	✓

Deliverable: Cyber Market System 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).	80%
Objective 2: Indiana increases to two percent (about $300M) of the Department of Defense (DOD) cybersecurity market share ($15B plus) by FY 2025.	10%

Deliverable: Cyber Statewide Testbed

Objective 1: Establish a nationally recognized cybersecurity test bed in Indiana.	50%*
Objective 2: Indiana captures five percent of international cybersecurity market share of cybersecurity test, training, and demonstration plan and capability by December 2025.	20%*

* = *Put on hold due to COVID-19*

FINANCE COMMITTEE

Deliverable: Cyber Training (Ivy Tech)

	Complete %
Objective 1: Ivy Tech will develop a cybersecurity curriculum for business executives by July 2018. Location: *https://www.ivytech.edu*	✓
Objective 2: IECC Finance Committee and Ivy Tech will launch a pilot program with participants by August 2018.	✓

Deliverable: Cyber Statewide Testbed

Objective 1: IECC Finance Committee will develop the Top Information Security Tips training material for Indiana businesses by June 2019. Location: *www.in.gov/cybersecurity/government/best-practices-standards-and-resources/*	✓

ECONOMIC DEVELOPMENT COMMITTEE

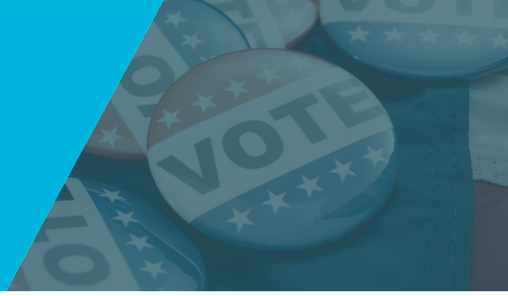
Note: Cyber Summit Working Group was consolidated under Economic Development Committee January 2020.

	Complete %
Deliverable: Incentive Program	
Objective 1: Propose a list of possible incentive programs to be considered by the State of Indiana by April 2019. Location: *www.in.gov/cybersecurity/files/Appendix-D.3-Economic-Development-Working-Group-Final.pdf*	✓
Objective 2: Using current programs, State of Indiana will establish an incentive program in Indiana by July 2020. Location: *https://www.iedc.in.gov/*	✓
Deliverable: Implementation Plan for Cybersecurity – Marketing	
Objective 1: Indiana Economic Development Corporation will develop a 2-year marketing plan focusing on economic development and Indiana's cybersecurity posture by August 2019 (dependent on funding)	25%^
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.	0%^
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.	50%*
Objective 2: Indiana captures five percent of international cybersecurity market share of cybersecurity test, training, and demonstration plan and capability by December 2023.	0%*
Deliverable: Cybertech Midwest	
Objective 1: IECC will secure a cybersecurity conference partner for three years by May 2018. Location: *https://midwest.cybertechconference.com/*	✓
Objective 2: State of Indiana will hold its first statewide cybersecurity conference by October 2018. 2018 – 700 attendees; 2019 – 2000 attendees Location: *https://midwest.cybertechconference.com/*	✓

* = *Put on hold due to COVID-19*

^ = *Put on hold due to funding*

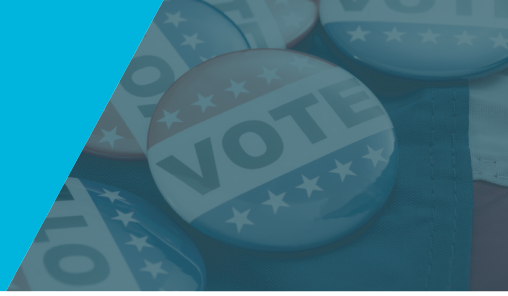
ELECTIONS COMMITTEE



Note: All the results and reports of the following deliverables can be found at www.in.gov/sos

	Complete %
Deliverable: Statewide Voter Registration System Cybersecurity Enhancements	
Objective 1: Indiana Secretary of State (SOS) Office will begin utilizing additional security protocols in 2018.	✓
Deliverable: Statewide Voter Registration System (SVRS) Network 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.	✓
Objective 2: SOS Office and Indiana Election Division will launch a Two-Factor Authentication Token Pilot by March 2018.	✓
Objective 3: SOS Office and Indiana Election Division will provide a report on Two-Factor Authentication Token Pilot by May 2018.	✓
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.	✓
Deliverable: Post-Election Risk Limiting Audit Standards and Pilot Program	
Objective 1: Indiana Voting System Technical Oversight Program (VSTOP) will develop and implement a RLA pilot in Marion County by July 2018.	✓
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.	✓
Deliverable: Cyber Threat Awareness & Training for County Election Admins	
Objective 1: SOS Office will implement and deliver a multi-year cybersecurity public awareness plan beginning in 2018.	✓
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.	✓

ELECTIONS COMMITTEE (CONTINUED)



Note: All the results and reports of the following deliverables can be found at www.in.gov/sos

	Complete %
Deliverable: Election Day Cybersecurity Tabletop Exercises	
Objective 1: SOS Office will develop and deliver a training exercise program for election officials and administrators by October 2018.	✓
Objective 2: SOS Office 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.	✓
Deliverable: Election Day Preparedness Guide	
Objective 1: SOS Office and IED provide existing Election Day emergency preparedness and response material to include cybersecurity for distribution prior to May 2018.	✓
Deliverable: Election Day Cybersecurity Monitoring and Rapid Response Technical Support	
Objective 1: SOS Office will develop and implement an Election Day cybersecurity technical support program by April 2018.	✓
Objective 2: SOS Office 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: SOS Office will develop a communications plan specific to election security by April 2018.	✓
Objective 2: SOS Office will measure the success of communications plan efforts specific to election security.	✓
Deliverable: Election Cybersecurity Incident Response and Communications	
Objective 1: SOS Office will develop and distribute an Election Day cyber security incident communications and response to all Indiana election county officials by May 2018.	✓
Deliverable: Catalog and Summaries of Best Election Cybersecurity Reports and Guides	
Objective 1: SOS Office will develop an election cybersecurity library by October 2018.	✓

ENERGY COMMITTEE

	Complete %
Deliverable: Critical Infrastructure Information	
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.	✓
Deliverable: Contacts	
Objective 1: Over 85 percent of Indiana electric and natural gas utilities provided the Indiana Utility Regulatory Commission's Emergency Support Function lead on behalf of Indiana Department of Homeland Security a cybersecurity contact by June 2018.	✓
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.	✓
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.	✓
Objective 2: IECC Energy Committee will share information with Energy ISAC regarding Indiana's new cyber sharing resources starting no later than 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 those who were surveyed was sent to the IECC.	✓
Objective 2: Eighty percent of all utilities will complete annual survey by July 2018. The actual result was one hundred percent participation with all responses received prior to June 2018.	✓
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.	✓

STATE AND LOCAL GOVERNMENT COMMITTEE

Note: State Government Services and Local Government Working Group were consolidated in January 2020.

	Complete %
Deliverable: Indiana's Cybersecurity Website Hub	
Objective 1: IECC will develop and launch a statewide cyber hub website by September 2018. Location: *www.in.gov/cyber*	✓
Objective 2: Increase website traffic to www.in.gov/cyber by 50 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 November 2019. Location: *www.in.gov/cybersecurity/files/Cyber-Emergency-Resiliency-and-Response-State-Guide.pdf*	✓
Deliverable: Local Officials Cybersecurity Guidebook	
Objective 1: Develop a guidebook for local government officials to assist them with cybersecurity planning and education expected by March 2021. Location: *www.in.gov/cybersecurity/government/best-practices-standards-and-resources/*	✓
Objective 2: Promote guidebook on cybersecurity planning and education to local government officials Fall and Winter 2019.	✓

Top 5 most visited web pages:

1. Indiana Cyber Hub - Main Page
2. Indiana Cyber Blog
3. Indiana ISAC
4. Report A Cyber Incident
5. Cyber Incident Reporting Law

Top 3 most downloaded documents:

1. Indiana Scorecard
2. Emergency Manager Cybersecurity Toolkit
3. 2018 Indiana Cybersecurity Strategic Plan (with no Appendices)

HEALTHCARE COMMITTEE

	Complete %
Deliverable: Vendor Management	
Objective 1: Create vendor management resources for healthcare providers by November 2019. Location: *https://iuhealth.org/about-our-system/vendor-relations*	✓
Objective 2: Distribute vendor management resources to eighty percent of healthcare providers by December 2019.	✓
Deliverable: Long-Term Education	
Objective 1: IECC Healthcare Committee will create Indiana-focused versions of security education by October 2019. Location: *https://www.in.gov/cybersecurity/trainingevents/*	✓
Objective 2: Provide Indiana-focused versions of security education to eighty percent of Indiana healthcare providers by December 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 June 2020.	0%*
Objective 2: Evaluate pilot program and recommend a sustainability framework model for the state of Indiana to maintain by June 2020.	0%^

* = *Put on hold due to COVID-19*

^ = *Put on hold pending completion of the pilot program*

WATER AND WASTEWATER COMMITTEE

	Complete %
Deliverable: Cyber Risk Model (Plan)	
Objective 1: The IECC Water and Wastewater Committee will develop a Cyber Plan Template for Indiana water/wastewater companies by September 2018. Location: www.in.gov/cybersecurity/government/best-practices-standards-and-resources/	✓
Objective 2: Distribute Cyber Plan Template to twenty-five percent of Indiana water/wastewater companies by May 2021.	10%*
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.	✓
Objective 2: Indiana Department of Environmental Management maintains a cybersecurity contact information for 95 percent of Indiana water organizations serving a population greater than 3,301 by August 2019.	✓
Deliverable: Risk Tool	
Objective 1: Water/Wastewater Committee develops Cyber Assessment Risk Tool by March 2019 (once funding was secured).	✓
Objective 2: Eighty percent of Indiana water and wastewater companies will have used cyber assessment risk tool within 24 months of deployment and secured funding by May 2021.	1%*
Deliverable: Training Plan	
Objective 1: Water/Wastewater Committee develop training plan by March 2019 or within 3 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 training plan and securing funding.	1%*
Deliverable: Cyber Plan Template	
Objective 1: IECC Water & Wastewater Committee develop a Cyber Plan Template for Indiana water/wastewater companies by April 2019. Location: www.in.gov/cybersecurity/government/best-practices-standards-and-resources/	✓
Objective 2: IECC Water & Wastewater Committee and partners will distribute Cyber Plan Template to 50 percent of Indiana water/wastewater companies by July 1, 2019.	✓

* = *Put on hold due to COVID-19*

WORKFORCE DEVELOPMENT COMMITTEE

	Complete %
Deliverable: Generate Interest Plan	
Objective 1: Establish and fund a statewide cybersecurity program centered for K-12 stakeholders by July 2019. Location: *www.indianactocouncil.org/indianactocouncil* & *www.in.gov/doe*	✓
Objective 2: Support the launch of a statewide cybersecurity program centered for K-12 stakeholders by June 2021. Location: *www.indianactocouncil.org/indianactocouncil* & *www.in.gov/doe*	✓
Deliverable: Job Demand Tool	
Objective 1: State of Indiana adopts Cyberseek as a source for cybersecurity-related job demand and career pathways for the state by June 2019. Location: *www.cyberseekin.org*	✓
Objective 2: State of Indiana will develop integration plans for consumption of the Cyberseek data across various job seeker, employer, and education platforms by December 2019. Location: *www.cyberseekin.org*	✓
Deliverable: K-12 Offering Cyber Security Content	
Objective 1: Indiana Department of Education will develop a menu of cybersecurity content and initiatives that includes K-12 computer science offerings by December 2021.	25%*
Objective 2: Eighty percent of Indiana Schools will adopt one or more cyber initiatives by August 2021.	25%*
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: With the planning assistance of the National Governors Association, support the implementation of statewide programs that will provide educators and businesses resources for meeting best practices and standards, such as the NICE Framework, by December 2019.	✓
Objective 3: With the planning assistance of the National Governors Association, support the implementation of 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.	50%*

* = *Put on hold due to COVID-19*

WORKFORCE DEVELOPMENT COMMITTEE (CONTINUED)

Deliverable: Incentivized Cybersecurity Certifications

	Complete %
Objective 1: Support the creation and launch of a statewide cybersecurity certification training program that meets best practices and NICE standards by December 2021.	50%*

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 June 2019. Location of final: Survey with CHE	✓
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.	✓

* = *Put on hold due to COVID-19*

RESILIENCY AND RESPONSE WORKING GROUP

Note: Emergency Services Working Group was combined with Pre-thru Post-Response Working Group January 2020.

	Complete %
Deliverable: Annex	
Objective 1: IDHS will develop and distribute the IDHS CEMP Cyber Annex to appropriate parties by December 2019.	✓
Objective 2: IDHS will exercise or operationalize the IDHS CEMP Cyber Annex by December 2020.	✓
Deliverable: IDHS Exercise Management	
Objective 1: IDHS will develop and communicate a Cyber Exercise Engagement process by November 2020.	✓
Deliverable: EOC	
Objective 1: IDHS will develop a Cyber Liaison position within Emergency Operations Center by December 2019.	✓
Objective 2: IDHS will exercise or operationalize the Cyber Liaison position within the EOC by December 2020.	✓
Deliverable: Toolkit	
Objective 1: IECC Emergency Services and Exercise Working Group will develop a Cyber Response Toolkit Version 1.0 by March 2019. Location: *www.in.gov/cybersecurity/government/emergency-response-and-recovery/*	✓
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 October 2019. Location: *www.in.gov/cybersecurity/government/emergency-response-and-recovery/*	✓
Objective 4: IDHS will develop and launch four workshops throughout Indiana using the Cyber Response Toolkit 2.0 by March 2020.	25%*

* = *Put on hold due to COVID-19*

RESILIENCY AND RESPONSE WORKING GROUP (CONTINUED)

Note: Emergency Services Working Group was combined with Pre-thru Post-Response Working Group January 2020.

	Complete %
Deliverable: Exercise	
Objective 1: State of Indiana will develop and execute a Cross-Sector Critical Infrastructure Cyber Exercise by December 2020.	✓
Deliverable: Cyber Emergency Response Team (IN-CERT)	
Objective 1: 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.	25%^
Deliverable: Gap Analysis	
Objective 1: Cyber Pre thru Post Incident Working Group will complete a comprehensive gap analysis of identified high risk critical infrastructure sectors by August 2018. Location: *www.in.gov/cybersecurity/files/Appendix-D.11-Pre-Post-Incident-Working-Group-Final.pdf*	✓
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. Location: *www.in.gov/cybersecurity/files/Appendix-D.11-Pre-Post-Incident-Working-Group-Final.pdf*	✓
Deliverable: Cyber Assessments	
Objective 1: Indiana National Guard will develop a Local/State Government Cyber Assessment Program by June 2020.	✓
Objective 2: Indiana National Guard will conduct Cyber Assessment for State critical infrastructure entities by September 2020.	25%*

^ = *Put on hold due to funding*

* = *Put on hold due to COVID-19*

CYBER AWARENESS AND SHARING WORKING GROUP

Note: Cyber Awareness & Training Working Group was combined with Cyber Sharing Working Group in January 2020.

	Complete %
Deliverable: Statewide Cybersecurity Public Relations Plan	
Objective 1: The IECC Public Awareness and Training Working Group will complete a statewide public relations cybersecurity campaign plan by June 2018. Location: www.in.gov/cybersecurity/files/Appendix-D.19-Public-Awareness-and-Training-Working-Group-Final-.pdf	✓
Objective 2: IECC leadership will approve a IECC public relations micro-plan on year one efforts by June 2019.	✓
Deliverable: Best practices	
Objective 1: Publish a list of resources that give Indiana local government and K-12 access to information depicting best practices in cyber security by September 2018. Location: www.in.gov/cybersecurity/government/cyber-threat-sharing/	✓
Deliverable: Cyber Sharing Maturity Model	
Objective 1: IECC will develop Indiana's cyber sharing maturity model by August 2019.	✓
Objective 2: IECC will distribute Indiana's first cyber sharing maturity model to critical infrastructures through ninety percent of Indiana associations by December 2020.	0%*
Deliverable: Inventory of Cyber Sharing Resources	
Objective 1: IECC Cyber Sharing Working Group will create a list of cyber sharing resources by August 2018. Location of final: www.in.gov/cybersecurity/government/cyber-threat-sharing/	✓
Deliverable: MS-ISAC Member Recruitment	
Objective 1: IECC Cyber Sharing Working Group will market the valuable services of the MS-ISAC to Indiana local government and K-12 organizations. Goal is to Increase Indiana MS-ISAC membership by twenty-five percent by June 2019. Location: www.in.gov/cybersecurity/in-isac/	✓
Deliverable: Secured Information Sharing Program	
Objective 1: IECC Cyber Sharing Working Group will develop a Secured Information Sharing Program by September 2019.	50%*
Objective 2: IECC Cyber Sharing Working Group will launch a Security Information Sharing Program in 2020.	0%*

* = *Put on hold due to COVID-19*

STRATEGIC RESOURCE WORKING GROUP

Note: Cyber Awareness & Training Working Group was combined with Cyber Sharing Working Group in January 2020.

	Complete %
Deliverable: Sustainability Recommendation	
Objective 1: IECC will develop a sustainability recommendation for the Council by September 2018.	✓
Deliverable: IECC Program Documentation	
Objective 1: IECC will develop program/framework documentation by September 2018. Location: *www.in.gov/cybersecurity/files/Cybersecurity-Report-FINAL-no-Appendices1.pdf*	✓
Objective 2: IECC will update program/framework documentation by January 2020. Complete: 100% Location: *https://www.in.gov/cybersecurity/executive-council/*	✓
Deliverable: IECC Scorecard	
Objective 1: IECC, along with Purdue University, will develop Indiana's first Cybersecurity Scorecard by August 2018. Location: *www.in.gov/cybersecurity/government/assess-yourself/indiana-cybersecurity-scorecard/*	✓
Objective 2: IECC, along with Purdue University, will launch Indiana's Cybersecurity Scorecard Pilot Program with 90 percent of selected organizations by September 2018. Location: IECC and Purdue maintain the records	✓
Objective 3: IECC will launch Indiana's Cybersecurity Scorecard to public and will have more than 500 downloads by March 2020.	✓
Deliverable: Policy Research Report	
Objective 1: IECC and partners will develop a report of state and federal cybersecurity legislation by August 2018. Location: *https://airtable.com/shrCcYzKJGH1jyvrx*	✓

LEGAL AND INSURANCE WORKING GROUP

Deliverable: Insurance Guide

Complete %

Objective 1: Develop a Cyber Insurance Guide version 2 to be provided to government and businesses by October 2019.
Location: *www.in.gov/cybersecurity/education/cyber-law-and-insurance/*

Deliverable: Policy Review

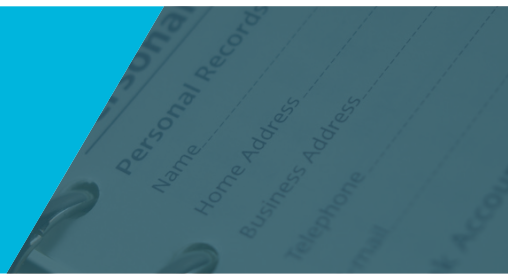
Objective 1: Update the list of cyber laws applicable to Indiana businesses and residents under current landscape by September 2019.
Location: *www.in.gov/cybersecurity/education/cyber-law-and-insurance/*

Deliverable: Cyber Insurance Survey Cyber Insurance Survey

Objective 1: Conduct a survey of businesses for insurance coverage and cybersecurity insurance coverage by December 2019.

Objective 2: Provide a report of the findings of the cyber insurance survey to the IECC by January 2020.
Location: *www.ibrc.indiana.edu/studies/State-of-Hoosier-Cybersecurity-2020.pdf*

PRIVACY WORKING GROUP



Note: PII Working Group was renamed Privacy Working Group in January 2020.

Deliverable: Indiana PII Guidebook

Complete %

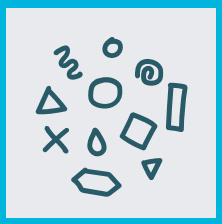
Objective: IECC PII Working Group will develop an Indiana PII Guidebook for the Indiana business community, the public sector, and the general public by 2021.
Location: *https://www.in.gov/cybersecurity/files/20210120-PII-Guidebook-FINAL.pdf*

Best Practices of the IECC

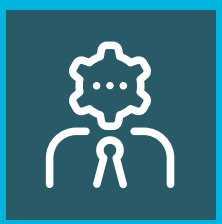
The Council has accomplished an unprecedented amount of work for the citizens and businesses of Indiana in the last four years due to the commitment of the public, private, military, and academic partnerships. Cybersecurity is not an issue that merely affects information technology professionals but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

Outreach of the IECC

As the Council efforts have grown, so has the need to communicate those efforts to the public. It is also important to provide the public, whether a business or individual, awareness and education of how cybersecurity is in their every day lives and what small steps they can take to make the biggest impact on their safety. For people to see cybersecurity differently, the state has to commit to communicating about cybersecurity differently. The purpose of the Indiana Cyber Hub, the cyber blog, and social media outreach is simple: to help every Hoosier build on their understanding about cybersecurity, how to protect themselves from cyberattacks, and to know the latest tips and trends.

Digital Outreach Stats

Cyber Hub Website - *Launched September 2018*

18K 2019 Visits / **16K** 2020 Visits / **30K** 2021 Visits

Cyber Twitter - *Launched September 2020*

25K 2020 Impressions / **92K** 2021 Impressions

Cyber Blog - *Launched December 2020*

25 2020 Subscribers / **495** 2021 Subscribers

Cyber Podcast - *Launched October 2020*

15 Episodes / **1.2K** Listeners

More than **200** Presentations Given by Cybersecurity Program Director

PART 2: Join Us In The Arena

In his speech "Citizenship in a Republic," President Theodore Roosevelt describes the courage it takes for one to take action in spite of critics in the arena:

> *"It is not the critic who counts; not the man who points out how the strong man stumbles, or where the doer of deeds could have done them better. The credit belongs to the man who is actually in the arena, whose face is marred by dust and sweat and blood; who strives valiantly; who errs, who comes short again and again, because there is no effort without error and shortcoming; but who does actually strive to do the deeds; who knows great enthusiasms, the great devotions; who spends himself in a worthy cause; who at the best knows in the end the triumph of high achievement, and who at the worst, if he fails, at least fails while daring greatly, so that his place shall never be with those cold and timid souls who neither know victory nor defeat."*

The courage it takes to step into the arena is as true today as it was in 1910. As the evolution of technology over the last century has improved our everyday lives, no one could have imagined the countless ways our lives are endangered with just a click. Attacking key critical infrastructure such as energy, water, healthcare, communications, and others would be devastating to the safety and wellbeing of our citizens as well as our financial markets.

When the IECC's strategic framework was developed by the Cybersecurity Program Director, it was her leadership who stepped into the arena with her as she invited others from private, public, academic, and military to join them in an approach that no other state has had. IECC members were invited to be innovative, be open minded, and be constructive in discussing not only the problems that increase the dangers in technology, but to come up with real, tangible solutions.

And while the IECC has most certainly thought outside the box in cybersecurity initiatives, many other organizations have joined the IECC in the cyber arena with equally important contributions to the state.

The following sections are those cyber initiatives and projects lead by organization who recognize the pivotal time our state and nation are in when it comes to the growth of technology and the respective threats. The IECC called for submissions of those organizations and efforts that are taking cybersecurity to the "Next Level." It is equally important for the state to recognize these herculean efforts of those who are making a difference in our own backyard.

The accomplishments that follow are just a key sampling of what Indiana has to offer it citizens, the nation, and the world as we all become even more connected every day.

State Agencies

State of Indiana – Multiple Agencies

Cybertech Midwest – 2018 and 2019:
The State of Indiana was pleased to host Cybertech Midwest in 2018 and 2019. Cybertech is described as the cyber industry's foremost B2B networking platform conducting industry-related events around the globe. Its international conferences serve as the go-to place to learn all about the latest technological innovations, threats, and solutions to combating cyber threats. In 2018, more than 700 professionals and executives attended its inaugural conference. In 2019, attendees almost tripled with about 2,000 people from all over the world.

Website: *https://midwest.cybertechconference.com/*

Indiana Office of Technology (IOT)

The Indiana Office of Technology (IOT) provides enterprise cybersecurity support for all executive branch agencies, protecting more than 30,000 computers, 8,000 mobile devices and 2,000 servers, ensuring the State provides services to the nearly 7 million Hoosiers.

Over the past year, IOT has implemented several changes to improve security and information sharing. Below are a couple of the more visible projects.

HEA 1169:
Cybersecurity threats are not limited to the physical locations of state government buildings. The State of Indiana works with many local government or external partners, each of which represents a possible attack vector. A new state law requires local government bodies to share specific cybersecurity threats they are facing. IOT collects this information and, if warranted, shares threat information with local government contacts. The threat information allows IOT security to better understand the types of attacks our partners see and help prepare for future cybersecurity needs.

Local Government Websites:
In every corner of the state, local government representatives are providing necessary services for Hoosiers. There has been increased demand for digital government services, and not all local government bodies have the resources or expertise to deliver high-quality services. The State of Indiana has award-winning digital government experience through IOT's IN.gov Program. In early 2020, IOT began offering inexpensive website hosting for local governments. Not only are citizens getting a top-notch digital experience, local government is receiving the same cybersecurity protections behind state government websites. So far, more than three dozen sites are in process or deployed.

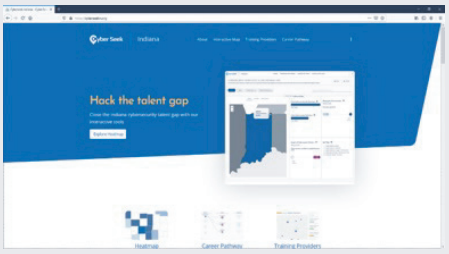
Indiana Department of Homeland Security (IDHS)

Girls Go CyberStart:
Since 2018, Indiana has participated in the Girls Go CyberStart competition hosted by the SANS Institute. Girls Go CyberStart centers on a fun and thought-provoking game to inspire young women to test their aptitude in cyber skills. Female students in grades 9–12 can participate for free, either as individuals or as part of a school-based team. As part of the CyberStart challenge, participants will take on the roles of agents in the Cyber Protection Agency, where they will develop forensic and analytical skills and deploy them to sleuth through challenges and tackle various online cybercriminal gangs.

In 2019, four teams from Indiana scored among the top 50 high schools nationally, with Noblesville High School just surpassing Walker Career Center in the national rankings.

Website: *https://girlsgocyberstart.org/*

Indiana Department of Workforce Development (DWD)



Launch of CyberSeek Indiana:
CyberSeek Indiana is a resource that can support local employers, educators, guidance and career counselors, students, current workers, policy makers, program directors, and other stakeholders as they answer important cybersecurity workforce questions. There are 20,500 openings requesting cybersecurity-related skills in the state, and employers are struggling to find workers who possess them.

Website: *https://cyberseekin.org*

Independent Cyber Vulnerability Assessment:
DWD hired Deloitte to do an assessment of our Fraud Detection capabilities as well as a full Cyber Security review. For the fraud assessment, they did an in-depth interview process to determine data systems, points of contact, inputs, and outputs, etc. The Cyber Security review went through the same type of interview process to make sure we were following the NIST Security Framework, IRS 1075, and State of Indiana security standards.

Advanced Fraud Data Analytics:
Implementing the Pondera tool uses Uplink (unemployment) data to help determine individual fraudsters as well as the larger fraud scheme which could include hundreds of people.

Identity Proofing and Verification:
DWD partnered with ID.me to help determine if a claimant is who they say they are. Before a claimant can file a claim, we require the claimant to prove who they are claiming to be. One study has this saving DWD hundreds of millions of dollars in fraud.

Advanced Web Application Firewall Protections:
DWD is now using the Shape tool to help block bot attempts. The Shape tool takes blocking the bot attempts to the next level.

Indiana Department of Revenue (DOR)

Tax Vendor Security Program:

DOR coaches companies through a process every year to ensure security is checked and rechecked as their systems undergo incremental changes, major upgrades, and modernization. DOR's assistance to tax vendors not only benefits Hoosiers. Taxpayers across the nation who use the products of these tax vendors also gain greater security over their sensitive information.

Security and Privacy Awareness Training:

DOR developed Security and Privacy Awareness (SPA) training to ensure its teammates are optimally prepared to protect sensitive Hoosier data. SPA training earned a 2020 award from the Federation of Tax Administrators that stated that all revenue departments are supposed to deliver security training, but DOR "focused attention and resources on it to do it better."

Indiana Department of Education (DOE)

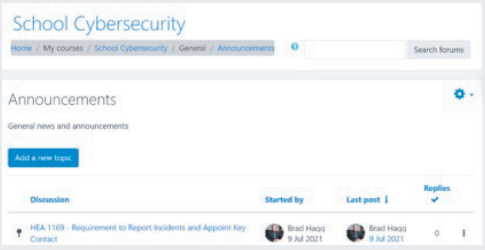
Establish Indiana Education Cybersecurity Task Force:

IOoT, Indiana ISAC, IDOE, & CoSN Indiana CTO Council established the taskforce to work together on intitiaves for K-12 schools. This initiative began with the IDOE offering the KnowBe4 platform to Indiana schools in order to provide cybersecurity training and phishing awareness. This platform is now used with over 52,000 school educators and students throughout the state. The IDOE also offered a matching managed services grant so that schools could increase their cybersecurity posture.

Website: *https://www.indianactocouncil.org/indianactocouncil and http://www.doe.in.gov*

DOE Establishes Private Moodle Course for Cybersecurity Resources and Information Sharing:

The IDOE established a private Moodle learning community where school administrators and IT leaders could receive information about cybersecurity, collaborate on best practices, and learn how to effectively use tools that are available to them. More than 170 participants are active in the community and the department now has a secure channel to communicate with these valued partners.



Website: *https://Moodle.doe.in.gov*

The Cybersecurity for Education Toolkit is Released:

A toolkit that was needed in the wake of the state and school closures due to the pandemic, where many superintendents, administrators, teachers, or staff members, found their systems even more vulnerable than before. DOE works with the IECC Program Director and Communications Manager in developing a turnkey resource. The Cybersecurity for Education Toolkit is an easy-to-understand resource complete with the latest tips and trends to help schools be cyber safe.

Website: *www.in.gov/cybersecurity/files/Indiana-Cybersecurity-for-Education-Toolkit-Final_2020.pdf*

Indiana Bond Bank, Treasurer of State's Office, IECC

Cybersecurity Podcast Series: "Days of Our Cyber Lives":
Over a series of 15 podcast episodes, Indiana Bond Bank, State Treasurer Kelly Mitchell, the IECC and a rotating panel of expert guests have highlighted timely cybersecurity issues and tips for local units of government. We believe this is the 1st and only podcast of its kind in the U.S. - generated by the public sector for the public sector on cybersecurity.

Website: *https://inbondbank.com/category/indiana-bondcast-podcast/*
or
https://podcasts.apple.com/us/podcast/indiana-bondcast/id1488634924

Indiana Small Business Development Center (IEDC)

Digital Transformation Courses:
The Indiana Small Business Development Center is providing three courses that will teach small businesses and entrepreneurs how to move their businesses online securely, safely, and successfully. The courses are self-study and self-paced.
The three courses offered are:
- Strategy, Risk and Security in Digital Transformation
- Applying Digital Tools to Your Business Operations
- Cybersecurity for Your Business

Website: *https://isbdc.org/digital-transformation-courses/*

Indiana Utility Regulatory Commission, Largest Energy Utilities (IURC)

IURC Cybersecurity Forum:
In March 2018, the Indiana Utility Regulatory Commission (Commission) organized a closed session on the topic of cybersecurity to learn more about how utilities and grid operators ensure safety and reliability for Hoosiers. The Commission met with the state's largest energy utilities – Citizens Energy Group, Duke Energy Indiana, Indiana Michigan Power Company (I&M), AES Indiana, Northern Indiana Public Service Company, LLC (NIPSCO), and CenterPoint Energy Indiana – and two regional transmission organizations (RTOs) – Midcontinent Independent System Operator (MISO) and PJM Interconnection, LLC (PJM) – to discuss their ongoing efforts regarding cybersecurity information, planning, and preparedness practices. In preparation for the meeting, each of the utilities submitted confidential responses to a Commission-issued survey on their cybersecurity capabilities. Representatives from the Indiana Department of Homeland Security and Federal Bureau of Investigation, as well as members of the Indiana Executive Council on Cybersecurity, also participated.

This experience yielded several positive outcomes for the Commission, including, but not limited to:

1. Confidential insight into the extreme threat landscape faced by our utilities;
2. Detailed explanation of the utilities' robust defense and countermeasures;
3. Successful trial use of the National Association of Regulatory Utility Commissioners' (NARUC's) cybersecurity guide and suggested questions for utilities;
4. Enhancement of personnel resources within the Commission's Cybersecurity Working Group;
5. Increased focus on cybersecurity education and training opportunities for staff; and
6. Additional involvement from staff participation in cybersecurity live tabletop exercises.

The Commission is hosting a meeting later this year to gain a better understanding of the cybersecurity practices employed by small natural gas utilities.

Website: *www.in.gov/iurc/files/IURC,-Electric-Utilities-Discuss-Ongoing-Cybersecurity-Efforts.pdf*

Academia

Purdue University

Purdue Joins Manufacturing Cybersecurity Collaboration :
Purdue University's Center for Education and Research in Information Assurance and Security (CERIAS) is joining the national Cybersecurity Manufacturing Innovation Institute (CyManII) to improve cybersecurity and energy efficiency for American manufacturing. Purdue joins 24 universities in the effort, which will develop tools, technologies, and guidance for securing manufacturing, supply chains, factory automation and information, and for manufacturing workforce development. Purdue is one of five founding university members of CyManII. The effort is being funded by the U.S. Department of Energy.

Purdue professor leads international team's research into deepfakes, manipulated media:
Deepfake videos of actor Tom Cruise on Tik Tok can create some confused fans. A deepfake video of a drug company CEO announcing COVID-19 vaccine failures, however, could cause panic. Ferreting out deepfake videos is the work of Edward Delp, the Charles William Harrison Distinguished Professor of Electrical and Computer Engineering at Purdue University, who is leading one of the teams in the Semantic Forensics program created by the Defense Advanced Research Projects Agency for the U.S. Department of Defense.

Purdue Among Select Members of New Space, Cybersecurity Organization:
Purdue University is the first university to join a select group of space community leaders as a founding member of the newly formed Space Information Sharing and Analysis Center (ISAC). The Space ISAC is unique by including academic participation in addition to predominately industry leaders on the board. The new collaboration will help fill gaps in information sharing between the ISAC partners regarding cyber and non-cyber threats.

Purdue University Global Graduate Cybersecurity Students Support Flying High Inc.:
Beginning in January 2021, some Purdue University Global students pursuing graduate degrees in information technology and cybersecurity began working with Flying HIGH Inc. to gain experience while lending their topical knowledge to the nonprofit organization in Youngstown, Ohio.

Purdue Northwest Awarded Nearly $6 Million Grant:
The National Security Agency has awarded a nearly $6 million Cybersecurity Workforce Development grant to the College of Technology at Purdue University Northwest. The two-year grant will allow the university to collaborate with other higher education institutions to develop an artificial intelligence and cybersecurity certification-based national training program for more than 425 transitioning military, first responders, and other adult trainees. The university is a National Center of Academic Excellence in Cyber Defense Education designated jointly by the NSA and the U.S. Department of Homeland Security. PNW says the training program will be offered online and free of charge to the trainees.

Purdue University (Continued)

Medicare / Medicaid healthcare delivery orgs cybersecurity assessed:
2021 is the final year for the FSSA funded Meaningful Use Assistance to Indiana state Medicare/Medicaid providers. This work allowed cyberTAP to assess 163 organizations against the HIPAA security and privacy regulations and provide remediation plans for improvement. This is the 5th year in a row this assistance has been funded. The meaningful use program ends on December 31, 2021.

cyberTAP awarded a $2M NSA cybersecurity innovation grant to assist local governments and K12 school districts:.
Starting in late August 2021, the NSA is funding cyberTAP to conduct onsite assessment projects for Indiana's local governments and K-12 school districts.

Website: *https://cyber.tap.purdue.edu/*

Purdue University Global Earns National Center of Academic Excellence in Cyber Defense Education Designation:
Purdue University Global has been designated as a National Center of Academic Excellence in Cyber Defense Education through academic year 2025 for its Bachelor of Science degree in cybersecurity. The Department of Homeland Security and the National Security Agency jointly sponsor the National Centers of Academic Excellence program. The goal of the program is to reduce vulnerability in national information infrastructure by promoting higher education and expertise in cyber defense.

Website: *https://www.purdueglobal.edu/bachelor-cybersecurity/*

Purdue University Global Cybersecurity Bachelor's Degree Program Accredited by ABET:
The Purdue University Global Bachelor of Science degree program in cybersecurity has been accredited by the Computing Accreditation Commission of ABET, the global accreditor of college and university programs in applied and natural science, computing, engineering and engineering technology. ABET accreditation assures that programs meet standards to produce graduates ready to enter critical technical fields that are leading the way in innovation and emerging technologies and anticipating the welfare and safety needs of the public.

Website: *https://www.purdueglobal.edu/bachelor-cybersecurity/*

Indiana University

IU Center to Provide Cybersecurity Expertise to $22.5 Million NSF Initiative:
Indiana University's Center for Advanced Cybersecurity Research (CACR) will provide a team to secure a $22.5 million initiative to advance distributed high throughput computing, or dHTC, as part of the Partnership to Advance Throughput Computing (PATh).

NSF Grant Will Help Indiana University Train Next Generation of AI, Cybersecurity Professionals:
Building on its success in preparing professionals for careers in cybersecurity, Indiana University has been awarded a grant from the National Science Foundation for a new project to train the next generation of the nation's crucial cybersecurity workforce to address vulnerabilities and identify threats using artificial intelligence. The $242,863 award supplements a $2.25 million NSF grant last year that established IU as a participating institution in CyberCorps: Scholarship for Service. This national program trains information technology professionals and security managers to meet rapidly growing cybersecurity needs of federal, state, local and tribal governments.

Website: *https://cacr.iu.edu/*

Indiana Election Security:
In 2020, the Center for Applied Cybersecurity Research (CACR) collaborated with Indiana Secretary of State Lawson to better prepare Indiana's counties for cybersecurity incidents related to the 2020 election cycle. CACR provided tailored training and outreach to county election officials about the importance of preparing for incidents before they occur and empowering them to create incident response plans and playbooks for use in response to an unintended event. CACR held in-person incident response workshops in 9 locations across the state and continued those virtually during the pandemic. In addition, CACR delivered tabletop exercises, training materials, and on-the-job resources for election officials. This outreach was broadly applicable to all county election officials regardless of county size, staff experience, and technical infrastructure.

Website: *https://itnews.iu.edu/articles/2019/IU-to-help-secure-Indianas-2020-elections-.php*

IU and Crane collaborate on PACT cybersecurity assessments:
In 2019-2020, the methodology was proven by two congressionally funded, DoD-sponsored pilots, most recently at the Port of Virginia in collaboration with the United States Coast Guard.

As a testament to the impact, a Senior Vice President from the Port of Virginia stated, "Based on your recommendations we have decided to revisit our cybersecurity strategy from the top down....Thanks for all your efforts and in helping us take a different perspective."

PACT (Principles-Based Assessment for Cybersecurity Toolkit) assessments take a broad, holistic view of the organization's cybersecurity strategy and operations, among other key attributes. PACT is collaborative, non-invasive, and scalable in terms of time and effort. It is based on assessments conducted in 13 prior engagements through the NSF Cybersecurity Center of Excellence and US Navy.

Website: *https://cacr.iu.edu/pact/index.html*

Indiana University (Continued)

Research raises the bar on cybersecurity operations for NSF Major Facilities:
Science often struggles with operational cybersecurity due to limited budgets, personnel challenges, and the unusual nature of their workflows and assets. ResearchSOC brings production security operations center technology and skilled staff to science clients, empowering them to improve their cybersecurity postures and manage cybersecurity risk, without taking their focus from the science.

Funded by a $5m National Science Foundation (NSF) grant, ResearchSOC leverages the 24/7/365 monitoring and alerting capabilities of IU's OmniSOC. We add science-focused threat intelligence, support, vulnerability scanning, and managed honeypots. This focused approach has strengthened and improved some of the most mature scientific facility security programs, while bringing the least mature to a higher standard in months instead of years.

ResearchSOC is serving:
The National Radio Astronomy Observatory (NARO)
The Geodetic Facility for the Advancement of Geoscience (GAGE)
The Gemini Telescopes (NOIRlab)
The National Solar Observatory
...with more on the horizon
.
Website: *https://researchsoc.iu.edu*

State of Hoosier Cybersecurity 2020 Report:
Stakeholders statewide, including local governments and small businesses wanting to learn more about "reasonable" cybersecurity best practices. To get a more complete picture of Hoosier cyber risk planning, the Legal and Insurance Working Group of the Indiana Executive Cybersecurity Council, in collaboration with researchers at Indiana University and the University of Arizona, conducted this study to help explore how Indiana organizations perceive and manage cyber risks. We pay particular attention to the role of insurance as part of an overarching cyber risk mitigation strategy.

Website: *https://www.ibrc.indiana.edu/studies/State-of-Hoosier-Cybersecurity-2020.pdf*

Indiana University CyberCorps Program:
The CyberCorps scholarship is designed to recruit and train the next generation of cybersecurity professionals to meet the needs of Federal, State, local, and tribal government. This program provides scholarships for cybersecurity undergraduate, and graduate (MS or PhD) education funded through grants awarded by the National Science Foundation (NSF). In return for the financial support, recipients must agree to work for the U.S. Government after graduation in a cybersecurity-related position, for a period equal to the length of the scholarship.

Website: *https://graduate.iu.edu/cybercorps/*

Indiana University (Continued)

Indiana University-led Cybersecurity Center of Excellence receives $12.5M renewal grant from NSF:
The National Science Foundation has awarded Trusted CI, the NSF Cybersecurity Center of Excellence, a $12.5 million renewal grant to extend the center through 2024. The Indiana University Center for Applied Cybersecurity Research is the lead organization for the NSF Cybersecurity Center of Excellence, in collaboration with the National Center for Supercomputing Applications, the Pittsburgh Supercomputing Center, the University of Wisconsin-Madison, Internet2 and the U.S. Department of Energy's Lawrence Berkeley National Laboratory.

State, National and International Higher Education Cybersecurity Efforts by the REN-ISAC hosted by Indiana University:
Research & Education Networks, Information Sharing & Analysis Center (REN-ISAC) is an international higher education and research network cyber-threat information-sharing and cybersecurity alliance. It is hosted at Indiana University and serves the State of Indiana and upwards of 700 members nationally and internationally.

- Aligned with CISA Traffic Light Protocol (TLP)
- Led 19 incident workshops over 3 years where we facilitated cyber-threat mitigation exercises for 1,020 participants.
- Retired outdated version of REN-ISAC's proprietary automated threat intelligence services SESv3 and migration to SESv4, which allows for faster sharing of indicators of compromise and enhanced functionality.
- Completed 17 Cybersecurity Peer Assessments since 2018

Website: *https://ren-isac.net*

Indiana University Cyber Center Earns 2019 CSO50 Award:
OmniSOC at Indiana University has been named a recipient of a 2019 CSO50 Award from IDG's CSO. Each year, the publication honors a group of 50 organizations whose security projects/initiatives have created outstanding value and thought leadership.

WGU Indiana

WGU Indiana Designated as a National Center of Academic Excellence in Cyber Defense Through the Academic Year 2026:
WGU's online B.S. Cybersecurity and Information Assurance degree program was designed with input from cyber security experts and leading IT employers to meet the most recent Department of Homeland Security (DHS), and National Security Agency (NSA) guidelines.

Ivy Tech Community College

Ivy Tech Community College's Cyber Security Program Makes Top List:
A report by Intelligent.com, a trusted resource for online degree rankings and higher education planning, named Ivy Tech Community College's cyber security program in its list of Top 60 Cyber Security Degree programs for 2020.

The comprehensive research guide is based on an assessment of 105 accredited colleges and universities in the nation. Each program is evaluated based on curriculum quality, graduation rate, reputation, and post-graduate employment.

Ivy Tech was recognized as the only associate degree granting school in Indiana to make the list.

Ivy Tech Community College – Valparaiso Campus

Ivy Tech Receives the CAE Center of Academic Excellence Designation Through 2022 from the NSA and DHS in Cyber Security (June 2017):
Release:
https://news.ivytech.edu/2017/06/09/ivy-tech-named-national-center-of-academic-excellence-in-cyber-defense/

Ivy Tech Valparaiso Campus Receives IDOE Award for Excellence (Feb. 2019)

National Security Agency (NSA) Awards Ivy Tech Portion of $5.9 Cyber Grant, Provides Extension to Grant Program Through 2023:
Website:
https://www.chicagotribune.com/suburbs/post-tribune/opinion/ct-ptb-ivy-tech-column-st-1113-20201112-7mx4dvs3zzhkrcbngw5izxvzxi-story.html

Ivy Tech Hosted and Participated in Virtual US Cyber Challenge 2020:
All students in the Cybersecurity program benefited from the cyber challenge and Ivy Tech Valparaiso Student Mina Saad won 1st place; Eileen Peden and Ray Cales won 2nd place honors and USDHS CIO Keren Evens presented the awards.
Website: https://uscc.cyberquests.org

Ivy Tech Hosted a 25-State Regional for the Virtual US Cyber Challenge 2021:
All students in the program benefited from the challenge. Ivy Tech Valparaiso students Michael Hallmen and Christian Bryan won 2nd place honors and Ivy Tech will be attending in the National USCC 2021 in October.

Indiana Tech

Indiana Tech – Cybersecurity Operations Center:
Indiana Tech is creating a state-of-the-art learning environment for its cybersecurity students which will include a security operations center, a digital forensics lab and an interactive data center. This reimagined and robust center will be completed in time for the 2021-22 academic year.

Indiana Tech's Bachelor of Science in Cybersecurity prepares students for a career and leadership within the rapidly expanding cybersecurity field. Our program blends the technical aspects of cybersecurity, information security, network security, network penetration, digital forensics and defensive CyberOps with a fundamental understanding of criminal investigation.

Website: *https://academics.indianatech.edu/cyber-center/*

Indiana Tech Cyber Warriors Collegiate Cyber Competition Team:
Led by Coach Matt Hansen, since 2006, Indiana Tech Cyber Warriors have grown into an elite collegiate cyber competition team, claiming 14 state CCDC championships and ranking in the top 10 teams nationwide three times: in 2007, 2011, and 2018. In March 2021, Indiana Tech claimed its 7th consecutive state championship and advanced to the Midwest Regionals in April and earned a 2nd place finish.

Anderson University

Established Center for Security Studies and Cyber Defense:
Anderson University's Center for Security Studies and Cyber Defense was established through a $1 million dollar Lilly Endowment Grant to support both the mission of Anderson University's Security Studies Program and the surrounding community.

The CSSCD challenges our students and staff to use their expertise in ethical and constructive ways, while equipping students with the knowledge and skills that can be used to preserve and promote security in every sector of American society.

The Center supports the surrounding community by providing security services to local and regional constituents. The Center's student interns, and affiliated faculty provide those services and educate the public about cybersecurity issues.

Website: *https://www.anderson.edu/csscd*

Vincennes University

Created an Industry Recognized Credential (Cisco Beginning Level Certification):
Petitioned Indiana Department of Education to achieve approval and VU is an authorizing body.
Website: *https://www.vinu.edu/cblc*

Cloud Based Network as a Service Data Center:
Awarded Perkins Grant to implement Netlab system that removed the hardware cost barrier for High Schools and allowed students virtual access to real hardware for the completion of lab assignments remotely.

Center for Academic Excellence:
Cyber Defense Education – recognition as a validated Cyber Security degree program from the National Centers of Academic Excellence in Cybersecurity benefiting Vincennes University and High School students in Indiana.

Established a Cyber Center: Launched a website to convey Cyber Security information and news to students in the state of Indiana.
Website: *https://www.vinu.edu/web/securevu*

EC-Council ATC Circle of Excellence Award Recipient:
Jaci Lederman earned the award for making a difference in the cyber security workforce in the state of Indiana.

Certified Secure Computer User Curriculum/Certification added to a class on the Indiana Core Transfer List:
Jaci Lederman created the opportunity for hundreds of Indiana High Students to obtain a certification in Cyber Security.

Vincennes University Cyber Security degree programs:
The university continues to recruit, retain, and graduate students from the following degree programs: 5457 Cyber Security and Network Operations Certificate (Qualifies for Next Level Jobs initiative), 5440 Cyber Security A.S.

Ivy Tech, Purdue, and Finance Sector Partners

Increasing Cybersecurity Awareness in Finance Training:
The IECC Finance Committee partnered with Ivy Tech in 2018 to three courses with eight participants in the pilot program, and funded by Northwest Mutual. These courses can then allow for completion of a certificate program and degree at Ivy Tech with further transfer to four year colleges. The program went so well that the committee asked for it to be further extended into three deeper areas, and has split into two roll outs.

The pilot was expanded within Muncie to three law enforcement agencies in the Spring of 2021 in the same manner and is ongoing.

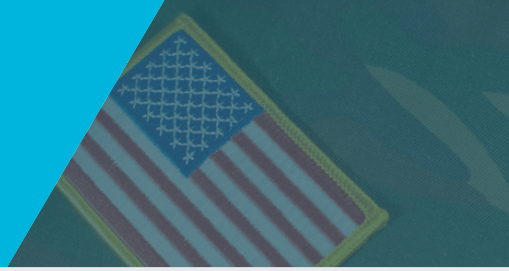
The pilot was also extended starting with development in Fall 2020 as www.cwct.us with implementation June 2021 to August 2022, through a $5.8M National Centers of Academic Excellence in Cybersecurity (NCAE-C) grant, funded by the National Security Agency National Cryptologic School. It uses CompTIA A+, Cisco CyberOps and Security+ as the required first three courses. Then the participants choose three additional courses in three more in depth areas of Cybersecurity, Forensics, Cloud System Administration, and AI and IoT Security. They can complete the program in six months taking two classes at a time, however, most will take a year to complete taking one course at a time.

An additional $2.8M dollars has been awarded to the consortium to extend the work through August 2023.

The NCAE-C grant was awarded as a national consortium to Purdue University North West, and sub awarded to Ivy Tech Community College Lake County, and Valparaiso Campuses, University of Tennessee - Chattanooga, and University of North Carolina – Charlotte. The 425-550 participants per year must be of 75% current or former military, law enforcement, fire, EMT, or other first responder status. The other 25% percent can be any US Citizen over the age of 18, but a preference is given for those of minority or a disadvantaged status. The participants obtain this training and three certification vouchers at no cost. There are currently more than 3,000 applications with a non-priority wait list until October 2022.

Website: *www.pnw.edu/cybersecurity/cwct/training-paths/cybersecurity-system-administration-certificate-program/*

Military



Indiana National Guard

INNG passes Command Cyber Readiness Inspection:
The Indiana National Guard underwent a Command Cyber Readiness Inspection from 7 to 11 June 2021. Within the inspection framework are three main areas: 1. Compliance with computer network directives. 2. Thorough scans into the network components. 3. Contributing factors like organizational culture and conduct.

The results provide situational awareness for Senior Leadership in order to enhance their cybersecurity and computer network defensive posture. It also provides mechanisms to decrease exposure to vulnerabilities within the given networks.

By passing this inspection, the Indiana National Guard demonstrated use of tactics, techniques, and procedures to respond to current and emerging threats. The validated compliance with mandatory directives aligns the Indiana National Guard with US Cyber Command's objectives, ensuring a secure operating presence. MCTC Provides Physical-Virtual Training Support to Cyber Yankee 2021.

MCTC Provides Physical-Virtual Training Support to Cyber Yankee 2021:
In collaboration with United States Cyber Command's (USCYBERCOM) Persistent Cyber Training Environment (PCTE), the Muscatatuck Cyber Training Center (MCTC) of the Indiana National Guard provided direct support to Cyber Yankee 2021.

The water treatment facility (WTF) at MCTC is a self-supporting system with industrial control equipment from three of the major vendors allowing testing and training opportunities which mimics the vast majority of water treatment plants in the United States.

By linking the PCTE virtual training environment with the MCTC physical facility, cyber defensive forces positioned in multiple states were able to rehearse defensive capabilities against aggressor forces.

Indiana National Guard Soldier Secures Cyber Success:
In a feature of a National Guard soldier, we meet James Gill, an information technician specialist with Headquarters Battery, 2nd Battalion, 150th Field Artillery Regiment in Bloomington, was pursuing an IT degree at Northern Kentucky University while serving in the National Guard and working part-time at a local superstore. After graduating from the program, Gill landed a job working for the Department of Financial Services through the network he had built at the Cyber Academy. In less than a year, Gill went from earning $11.50 per hour to making more than $60,000 per year in his dream career field.

Private/Public

Cloud Security Alliance Ohio River Valley Chapter

Establishment of regional chapter (Ohio River Valley) of the Cloud Security Alliance:
The Cloud Security Alliance (CSA) is the world's leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment.

Our chapters are made up of local security professionals who volunteer to increase cloud security awareness in their local community and provide outreach for CSA research, education, and training resources. They work to solve cloud vulnerabilities and challenges, by collaborating with other experts in the field to establish cloud security best practices.

Chapters offer participants an opportunity for leadership in regional communities, and the chance to establish thought leadership in their field.

Website: *https://orv-csa.org/*

Rofori Corporation

CyberKnights
CyberKnights is a cloud portal for cybersecurity skills assessment and workforce development built on the NICE Framework, a widely adopted standardized taxonomy, enabling assessment and development of skills by individuals, employers, government, and academia.

Employers are able to take inventory of their organization's current cybersecurity skills. CyberKnights identifies the skills gaps, displays the various training pathways for upskilling employees and developing internal talent, with the option to search external talent that can be further assessed to fill the skills gaps. Academia can keep their cybersecurity curriculum current based on the knowledge and skills needs of industry.

Website: *www.cyberknights.us*

Accelerate Indiana Municipalities

Cyber Security Training for Local Governments:
Over the past three years, Accelerate Indiana Municipalities (Aim), an association serving Indiana's cities and towns, has offered numerous cyber security training opportunities for municipal elected officials, municipal employees, and local government attorneys. The training opportunities have consisted of webinars as well as in-person and virtual workshops taught by experts in the field with the goal to provide cybersecurity awareness and to prompt government action and investment to secure systems.

Website: *www.aimindiana.org*

Pondurance

Keeping Indiana's Kids Safe Online (June 2021):
Pondurance hosted a training for the Girl Scouts of Central Indiana staff to teach them about cybersecurity and how to stay safe online. Pondurance also developed resources for the Girl Scouts participants for online safety.

Protecting Indiana's Water Supply (June 2019):
Pondurance hosted a free cybersecurity and Risk Management Workshop to help Indiana's water companies meet the requirements of Indiana SEA 362 and the US Cybersecurity and Infrastructure Security Agency Act of 2018.

Ignite Your Superpower:
Encouraging Girls to Go into STEM Careers (August 2019): This event aimed to teach middle school aged girls about careers in STEM. Pondurance built and brought in a "IOT Smart City" named Ponapolis to the event and explained the exciting career opportunities available in cybersecurity.

Training Teachers in Cybersecurity Careers (Fall 2019):
Pondurance hosted two Nextech Teachers Externships to help high school teachers understand cybersecurity careers as a way of better explaining to their students the opportunities within the cybersecurity field.

Nurturing the Next Generation of Indiana's STEM (September 2019):
Pondurance hosted more than 250 Indiana Teens at Nextech's Pathways to Tech event in September 2019. At this event, Pondurance highlighted the dynamic tech culture and career opportunities in STEM and encouraged students to practice networking with professionals.

Website: *www.pondurance.com*

IU Health

Medical Device Security Lab:
The IU Health Medical Device Security Lab responds to a pressing need in healthcare to protect medical devices from cyberattacks that can compromise patient care. Findings from the lab's research are expected to improve cybersecurity within the healthcare industry and prevent harm from cyberattacks that are increasing in number and severity.

The Ball Brothers Foundation

Ball Brothers Foundation Develops Cybercrime Initiative:
The Ball Brothers Foundation in Muncie has established a funding initiative to combat the threat of cyberattacks on the community. The foundation says Project Sybertooth is more than a funding effort, it's also a community network to enhance training initiatives and support cybercrime investigations. Project Sybertooth aims to strengthen the talent pipeline of people trained to address cyber threats as well as bolster the ability of local law enforcement agencies to deter and investigate cybercrime. The initiative also aims to develop new networks of communication between law enforcement, military, elected officials, local banks, local corporations, post-secondary education institutions and nonprofits.

Indiana National Guard, in partnership with Pondurance, Citizens Energy Group and IU Health

Full Scale Natural Disaster/Cybersecurity Exercise at Muscatatuck Urban Training Center:
The State of Indiana conducted a full-scale functional exercise, hosted by the Indiana National Guard for first responders and several military branches as well as search and rescue teams at the Muscatatuck Urban Training Center. The focus of the exercise was to measure how federal, state, local and private sectors respond to a devastating earthquake. As emergency and military teams responded to the effects of the earthquake, the Indiana National Guard also tested the additional response of its incident command leadership when the cyber experts from IU Health, Citizens Energy, and Pondurance made the efforts more difficult by attacking the water supply in the aftermath of the disaster.

Website:
https://www.wthr.com/article/news/local/indiana-holds-full-scale-cybersecurity-disaster-drill/531-e15c87fc-1cd1-46be-a9d3-379ed137d848

USDHS CISA, State of Indiana, and City of Fort Wayne, water and healthcare public/private partners

State of Indiana Cybersecurity Tabletop Exercise:
The Cybersecurity and Infrastructure Security Agency (CISA) recently partnered with the State of Indiana and the City of Fort Wayne to exercise how state, federal, mutual aid, and local government would work together in a long-term cyberattack that eliminated the supply of water from the city, with a special emphasis on the secondary effects for the city's hospitals.

Indiana Bankers Association

2020 and 2021 Indiana Bankers Association Cybersecurity Conferences:
The Indiana Bankers Association hosted two-day (in-person) cybersecurity conference in Indianapolis, following a two-day virtual conference in 2020.

The Cybersecurity Exchange

Creation of the Cybersecurity Exchange - A New Network for Cybersecurity Leaders, Experts, Talent and Startups in Southern Indiana:
Launched in March 2021, The Cybersecurity Exchange (CSX) provides a platform for cybersecurity leaders in business, higher ed, and defense to learn from one another, collaborate on ideas and projects, and advocate for cybersecurity to become an economic driver in the Innovation Corridor.

The CSX is powered by The Mill, a startup accelerator based in Bloomington that works with entrepreneurs across the Uplands.

Website: *https://www.cybersecurityexchange.org*

Rolls-Royce, Carnegie Mellon Network, and Purdue University

Purdue Researchers Join Rolls-Royce, Carnegie Mellon Network to Create Cyber Resilient Systems:
Proposed research at Purdue University is developing innovative solutions using artificial intelligence to enhance the security of current and future Rolls-Royce platforms powered by the company's propulsion systems. The project is one of three from Purdue accepted by Rolls-Royce as part of a newly launched Cybersecurity Technology Research Network, which the company April 22, 2021. The network, which is a partnership between Rolls-Royce, Purdue University's Center for Education and Research in Information Assurance and Security (CERIAS) and Carnegie Mellon University's CyLab, is focused on improving the cybersecurity for platforms powered by the company's propulsion systems.

Indiana Chamber of Commerce

Cybersecurity Conference:
The Indiana Chamber of Commerce annual Cybersecurity Conference began in 2018 as the need to share best practices became even more important. The Chamber's conference addresses key technology information, products, strategies, protections and so much more to help businesses in Indiana to ensure they are operating safely for future success.

Website: *https://www.indianachamber.com*

CircleCityCon

Security Conference:
CircleCityCon is a security conference held in downtown Indianapolis. CircleCityCon is about the community. A signature offering is the community led training classes offered to all participants. Events and contests are organized by members of the security community, including both CircleCityCon staffers and community partners. Three tracks, incredible entertainment, and technical villages help round out the CircleCityCon experience.

Website: *https://circlecitycon.com/*

AT&T

Hackathons:
A "hackathon" is a highly intense weekend event where developers, designers, and entrepreneurs get together to create an app based on the hackathon's general theme. AT&T hackathons typically last two days, where you have 24 hours to create and present an app. The repetitive nature of the hackathon enables participants to learn much faster through iteration and minimal distraction. AT&T and community partners provide lots of tools for participants to use while building apps, along with expertise from partners and staff, excellent speakers, and prizes.

Website: *https://midwestregion.att.com/*

National

National Conference on State Legislatures

Task Force on Cybersecurity:
The mission of the NCSL Cybersecurity Task Force is to engage members in policy discussions, educate members and extend networking opportunities to legislative leaders on cybersecurity and privacy issues through a series of well-defined programs, webinars on key definitions and critical cyber policy issues as well as supporting private-public networks. The task force began with an initial timeframe of two years focusing on cybersecurity issues and was renewed and has expanded its focus to include privacy issues.

Website: *https://www.ncsl.org*

National Governors Association

NGA Cyber Policy Academy:
The NGA Center for Best Practices hosts policy academy/workshops each year. Most of the 50 states apply for the academies and workshops that support the NGA's ongoing efforts since 2016 to help states and territories develop, refine, and share best practices in cybersecurity governance, workforce development, critical infrastructure security, and local engagement and partnership. Once a state is selected, they work with the NGA and its partners to focus on a specific project that year. After the academy/workshop, states share their best practices through conferences, workshops, webinars, and more. The State of Indiana has been selected for three projects since 2018. In 2018, Indiana was selected for its proposal for developing a workforce development strategy that was aligned with federal partners and the proposal for the development of the Emergency Manager Toolkit. In 2021, Indiana was selected to continue its work on a local government engagement program that will launch in 2022.

Website: *https://www.nga.org/statecyber/*

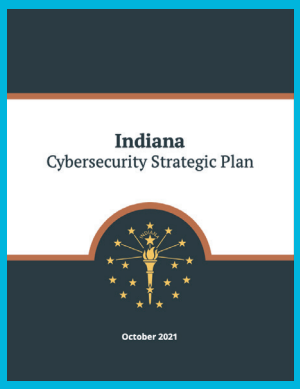
America Water Works Association

Updated Cyber Tools and Resources:
The American Water Works Association is an international, nonprofit, scientific and educational society dedicated to providing total water solutions assuring the effective management of water. Founded in 1881, the Association is the largest organization of water supply professionals in the world. Beginning in 2018, the IECC Water/Wastewater Committee began working with AWWA as they were updating their cybersecurity tools and resources. Using the IECC deliverables and extensive expertise of the IECC Water/Wastewater Committee and feedback from the industry, AWWA was able to fully test and update their resources to better serve water companies all across the nation. The significant amount of work and input from the IECC Water/Wastewater Committee has made Indiana a leader in the water/wastewater industry nationwide.

Website: *https://www.awwa.org/*

What's Next for Indiana

With the ever-growing threat of cyberattacks, it is clear from this report that protecting critical infrastructure is the focus of the State of Indiana.



Released at the same time of this report, the *2021 Indiana Cybersecurity Strategic Plan* sets the stage for a new set of 68 deliverables and 134 objectives to take cybersecurity in Indiana to the *Next Level*. Many of these deliverables would not have been possible without the foundation set by the IECC's more than 2,000-page *2018 Indiana Cybersecurity Strategic Plan* and all its successes in its implementation. But cybersecurity cannot be solved by one entity alone.

The IECC will continue to work with private, public, academic, and military partners from all over the state, nation, and world to develop and maintain a strategic framework that establishes goals, implements plans, and shares best practices with Hoosier citizens and businesses. Likewise, the State of Indiana will continue to support in any way it is able those organizations who are willing to join the IECC and state in the arena. And as President Roosevelt said, we will join those "who at the best knows in the end the triumph of high achievement, and who at the worst, if he fails, at least fails while daring greatly, so that his place shall never be with those cold and timid souls who neither know victory nor defeat."

Working to accomplish this in a way that is as intuitive as possible and does not add more clutter to the already complex topic is important to the state's overall mission in cybersecurity. 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 and its leadership throughout the State of Indiana, Hoosiers will continue to be safer, and businesses will continue to thrive.

To learn more about the cybersecurity efforts in Indiana, visit www.in.gov/cybersecurity.

Indiana's Executive Council on
Cybersecurity