Indiana Executive Council on
**Cybersecurity**

# The State of **Cyber** Report

2021-2024

in.gov/cybersecurity

February 21, 2025

Governor, State of Indiana
State House, Room 206
Indianapolis, Indiana 46204

Dear Governor Braun:

In the more than seven years since Governor Eric Holcomb extended Executive Order 17-11, a directive that continued the Indiana Executive Council on Cybersecurity (IECC), the State of Indiana is capitalizing on its commitment to protect the State's security and economy through its ability to deliver on its responsibility for supporting the prevention, protection, mitigation, response and recovery programs related to cyber threats.

In fact, the Council completed 84% of its 80 identified deliverables and 79% of the 151 objectives — a body of work that includes 11 new deliverables and 17 new objectives that were added to the 2021 Indiana Cybersecurity Strategic Plan that was presented to Gov. Holcomb in October 2021.

Because of the collective work of the Council, together with the contributions of the Indiana Department of Homeland Security (IDHS) and the Indiana Office of Technology (IOT) and the collaboration with numerous other state agencies and our federal partners, as well as those efforts involving local government, public and private sector, military, research and academic stakeholders, Indiana is recognized nationally as a top-tier state for cyber governance. The IECC is unlike any government organization of its kind and its advisory members are all volunteers. Thanks to their contributions and the expertise and knowledge they provide, it represents a savings of millions of dollars annually for all Hoosiers.

The second part of the report is a collection of other cybersecurity initiatives in Indiana outside of the IECC. And while this is not an all-inclusive list, it is, again, an important reflection of the vibrant level of cybersecurity-related activity that's occurring throughout our state. To learn more about the cybersecurity initiatives of Indiana, contact the state's interim Cybersecurity Program Director and Communications Manager David Ayers at dayers@iot.in.gov.

Sincerely,

Jennifer-Ruth Green
Secretary, Indiana Office of Public Safety
Executive Director, Indiana Department of Homeland Security

# Table of Contents

# The Indiana Executive Council on Cybersecurity

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.

## Work of the IECC Continues at High Level Amid Challenging Threat Environment

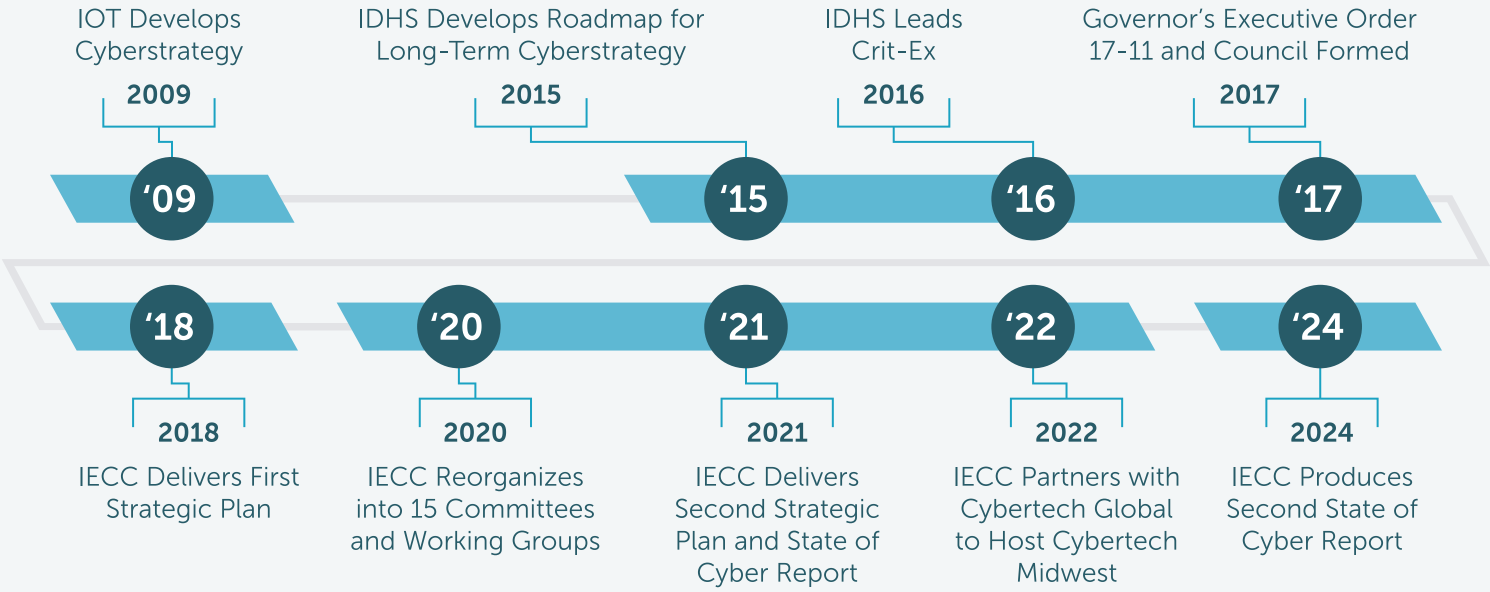
Beginning in 2009 with the development of the state's cyber strategy and continuing through 2016 with the completion of the unique critical infrastructure tabletop and operational exercises — known as Crit-Ex — Indiana continues to assert its leadership, among all states, when it comes to cyber governance.

Working from these foundational achievements — along with the recognition that securing Indiana's information technology infrastructure and industrial control systems is beyond the reach of any single entity — the results have been defined through the completion of two, three-year, cybersecurity strategic plans. This represents tireless work spelled out in the framework of the Governor's Executive Order. That was followed by Indiana's decision to hire its first, fully dedicated cybersecurity program director in March 2017 to facilitate the Council in fulfilling its purpose.

The progress that has been made is remarkable, given the fact that much of the IECC work was accomplished amid a global pandemic and during a time of an unparalleled number of cyber threats and attacks experienced in 2021.

From its inception in 2017 through October 2024, more than 350 people have served as advisory members of the IECC. In collaboration with the Council's 35 voting members and leadership, the state's cybersecurity policies and initiatives (in addition to a wealth of free resources, best practices and tips, as featured on the Indiana Cyber Hub website) have been created to provide all Hoosiers, businesses, local government and schools the opportunity and tools to increase their cybersecurity knowledge and awareness. The state also benefits from a better understanding of the infrastructure needed for everyone to be safer from the everevolving cyber threats. Much of the work has been accomplished by its membership, as part of the Council’s 15 committees and working groups (using a strategic framework that originally was comprised of 20 committees).

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 representatives who were conveniently located in and around the state capitol. In fact, the IECC leadership continues to ensure that every committee and working group have at least one representative from the northern part of Indiana, southern part of Indiana and central Indiana, as well as a small company, a medium-sized company, a large company, an association and more — as part of its membership.



IOT Develops Cyberstrategy
**2009**

IDHS Develops Roadmap for Long-Term Cyberstrategy
**2015**

IDHS Leads Crit-Ex
**2016**

Governor’s Executive Order 17-11 and Council Formed
**2017**

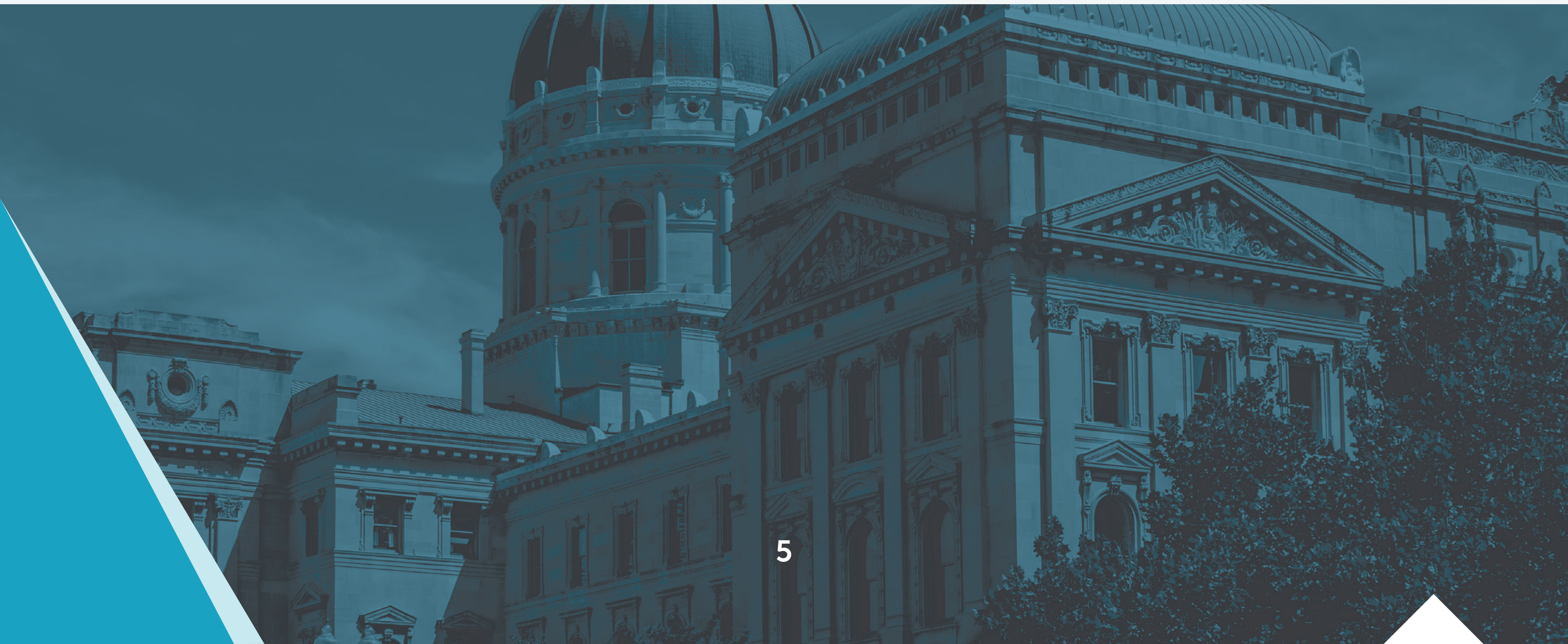
**2018**
IECC Delivers First Strategic Plan

**2020**
IECC Reorganizes into 15 Committees and Working Groups

**2021**
IECC Delivers Second Strategic Plan and State of Cyber Report

**2022**
IECC Partners with Cybertech Global to Host Cybertech Midwest

**2024**
IECC Produces Second State of Cyber Report



# Executive Order 17-11 Serves as Foundation for Hoosier State's Cybersecurity Priorities

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.

# IECC Breakdown

### Committee/Working Group Breakdown

Outside of Indianapolis

Northern Indiana

Central Indiana

Southern Indiana

Small Organizations

Medium Organizations

Large Organizations

Associations

### Membership Positions

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

More than 350 members between 2017-2024 were directly involved with the researching, planning, implementing and evaluating the 2021 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. In a timeframe that spans less than seven full years, no other state has accomplished this much from a voluntary cybersecurity Council. The results of this State of the Cyber Report (2021-2024) is, once again, 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.

**80**

Total Deliverables

66 Completed

10 In Progress

2 Put on Hold

2 Not Started

**151**

Total Objectives

118 Completed

26 In Progress

3 Put on Hold

7 Not Started

# Best Practices of the IECC

The Council has accomplished an unprecedented amount of work for the citizens and businesses of Indiana since its inception 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. Cybersecurity is something that cannot be done by one entity alone. It is achieved by working to address the comprehensive ecosystem that the state will not only address its own technology and information environment, but also by increasing 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.

Following the tenure of Chetrice Mosley-Romero as Indiana's Cybersecurity Program Director, which ended in 2023, David Ayers took over the day-to-day administration of the Council on an interim basis. Additionally, Ayers served as the communications manager for the IECC and manager of the Indiana Cyber Hub website, which featured a blog and multiple social media channels.

### State agencies work together

For the better part of a decade, the Chief Information Officer (CIO) of the State and the Executive Director of the Indiana Department of Homeland Security have been working hand-in-hand on cybersecurity. There is not one agency in charge. In fact, much of what Indiana has done is seek to understand every agency's role in cybersecurity and embrace it within the process, not fight about it. When agencies are heard and respected, they are more willing to come to the table. This has been true with the state agencies on the Council. It is also important that the Governor has encouraged this collaboration because that is the only way we can be successful as a state.

### Set expectations early and often

Every year the Council reviews the membership and the Charter. And every year, the Council leadership ensures that the members are aware of the time expectations, the deadlines, the priorities and the challenges to problem solve together. That is why meeting quarterly as a whole Council is important to its communication efforts and success.

### Templates are key

With so many committees and working groups and so many executives providing a volunteer service, providing templates to guide discussions and communicate what each team is doing is important to the organization, effectiveness and efficiency of the Council.

### Respect time

From the beginning, it was made very clear that if a member felt like a meeting was a waste of time to be open about that frustration and the program director will see what can be 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 in 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 everyday 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*

| 30K | 57K | 111K | 127K |
|---|---|---|---|
| *2021 Visits* | *2022 Visits* | *2023 Visits* | *2024 Visits* |

**Cyber Blog** - *Launched December 2020*

| 495 | 1,300 |
|---|---|
| *2021 Subscribers* | *2024 Subscribers* |

### Top 5 Most Visited Web Pages

1. Indiana Cyber Hub — Main Page
2. Report a Cyber Incident
3. Cyber Blog - Cyber Compliance 101
4. Cybersecurity Training and Events
5. Cyber Careers

### Top 3 Most Downloaded Documents

1. Emergency Manager Cybersecurity Toolkit — Scorecard
2. Healthcare in a Box Toolkit
3. Cyber Insurance Toolkit

# Deliverable Results of the 2021 Cybersecurity Strategic Plan

## State and Local Government Committee

### Deliverable: Indiana's Cybersecurity Hub Website

| | |
|---|---|
| Objective 1: Increase website traffic to www.in.gov/cyber by 100% by Sept. 2023. | ✓ |
| Objective 2: Conduct an annual review and update the Cyber Hub website by September of every year. | ✓ ONGOING |

### Deliverable: Indiana's Cybersecurity Hub Website

| | |
|---|---|
| Objective 1: The Indiana Office of Technology with the assistance of partners will re-launch a Local Government regional listening tour by March 2023. | ✓ |
| Objective 2: The Indiana Office of Technology will conduct a Local Government regional listening tour in 12 regions by Dec. 2023. | ✓ |
| Objective 3: The Indiana Office of Technology with the State and Local Cybersecurity Grant Program state commission will submit a state strategy to USDHS CISA by July 2023. | ✓ |
| Objective 4: The IECC will develop a report of the CRC Pilot by Fall 2023. | ✓ |

### Deliverable: Cyber Emergency Resiliency and Response State Guide Update

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

# State and Local Government Committee
*Continued*

### Deliverable: Local Officials Cybersecurity Guidebook 2.0

| | |
|---|---|
| Objective 1: The State and Local Government Committee will update and distribute the Indiana Local Government Cyber Guidebook. | ✓ |
| Objective 2: The State and Local Government Committee will encourage the downloading of 1,000 Indiana Local Government Cyber Guidebooks. | IN PROGRESS |

### Deliverable: Identity Management State Roundtable

| | |
|---|---|
| Objective 1: Indiana Department of Workforce Development (DWD) and Indiana Office of Technology (IOT) will lead a round table discussion with other key state agencies about best practices with defending against identity theft and fraud in 2023. | IN PROGRESS |

### Deliverable: Local Government Cybersecurity Podcast Series ("Days of Our Cyber Lives")

| | |
|---|---|
| Objective 1: Completion of a 15-minimum episode podcast series on cybersecurity topics for a Hoosier local unit of government audience over the course of one year, available via audio-only (e.g., Apple podcasts) or video and audio (YouTube) by Oct. 2021. | ✓ |
| Objective 2: Realizing greater than or equal to 900 combined views and listens for the series by Oct. 2021. | ✓ |

# Finance Committee

### Deliverable: Board Leadership Education Plan

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

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

### Deliverable: Refine Committee Membership to be Better Aligned with Statewide Financial Institutions and Associated Agencies

Objective 1: IECC Finance Committee will manage an outreach campaign to add representative members willing to provide their business operations, information technology, financial and education leadership related to cybersecurity threats and opportunities by June 2023. ✓

Objective 2: Define a more effective information waterfall approach from the federal and state level to the organization, market and ATM level to help to formalize communication around disruption. ✓

### Deliverable: Top Security Tips Material 2.0

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

# Energy Committee

### Deliverable: NARUC Cybersecurity Training for Regulators

| | |
|---|---|
| Objective 1: The Indiana Utility Regulatory Commission will advocate for training to be hosted in Indianapolis, Indiana, by Q3 2022. | ✓ |

### Deliverable: Critical Infrastructure Information (CII)

| | |
|---|---|
| Objective 1: IECC Energy Committee will provide a review of the July 2018 definitions by Oct. 2021. | ✓ |
| Objective 2: IECC Energy Committee will review potential state policy changes to protect critical infrastructure information while maintaining public access and freedom of information by Dec. 2021. | ✓ |
| Objective 3: The cybersecurity contact for each small gas utility will be provided to USDHS CISA and TSA by May 2022. | ✓ |

### Deliverable: Training

| | |
|---|---|
| Objective 1: Develop a survey to determine whether there are new training needs specific to the energy industry following the Pandemic by Q3 2022. | IN PROGRESS |
| Objective 2: Identify and recommend opportunities at the state, vocational, or higher education level by Q3 2022. | IN PROGRESS |

### Deliverable: IURC Cybersecurity Forum

| | |
|---|---|
| Objective 1: Indiana Utility Regulatory Commission (IURC) will host a cybersecurity forum for small natural gas utilities to share industry information and best practices by Dec. 2021. | ✓ |
| Objective 2: Indiana Utility Regulatory Commission (IURC) will host cybersecurity briefings for large investor-owned natural gas and electric utilities by Oct. 2022. | ✓ |

# Energy Committee
*Continued*

### Deliverable: Resource Guide

| | |
|---|---|
| Objective 1: The IECC Energy Committee will define emerging technology and supply chain issues related to the grid by Q3 2022. | ✓ |
| Objective 2: The IECC Energy Committee will determine whether best practices and information are widely available by Q3 2022. | ✓ |
| Objective 3: The IECC Energy Committee will develop an industry specific resource guide by Q4 2022. | ✓ |

### Deliverable: Workplace IT

| | |
|---|---|
| Objective 1: The IECC Energy Committee will develop a survey to identify challenges in the workplace for the energy sector in Q3 2022. | DETERMINED TO BE OUT OF SCOPE |
| Objective 2: The IECC Energy Committee will identify issues stemming from the work from home environment by Q3 2022. | DETERMINED TO BE OUT OF SCOPE |
| Objective 3: The IECC Energy Committee will share best practices and coordinate with other sectors as needed in Q4 2022. | DETERMINED TO BE OUT OF SCOPE |

# Water and Wastewater Committee

### Deliverable: Cyber Contact List

| | |
|---|---|
| Objective 1: Indiana Department of Environmental Management (IDEM) maintains a cybersecurity contact information list for 85% of Indiana water and wastewater organizations to be reviewed annually. | ✓ |

### Deliverable: Cyber Risk Model (Plan) Update

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

### Deliverable: Risk Tool

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

### Deliverable: Training Plan

| | |
|---|---|
| Objective 1: The Water/Wastewater Committee will develop an initial training plan by June 2021 and full training plan within three months of funding. | ✓ |
| Objective 2: Seventy percent of Indiana Water and Wastewater companies incorporate the training plan as part of their operational resources within 24 months of deployment of training plan. | ✓ |

### Deliverable: Cyber Plan Template Update

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

# Water and Wastewater Committee

*Continued*

### Deliverable: Water/Wastewater Exercise and Response Education

| | |
|---|---|
| Objective 1: IECC Water and Wastewater Committee and partners will participate in USDHS/CISA Exercise in Aug. 2021. | ✓ |
| Objective 2: IECC Water and Wastewater Committee and partners will participate in the INNG Hoosier Defender Exercise in Aug. 2021. | ✓ |
| Objective 3: Working with partners, the IECC Water and Wastewater Committee will develop a water/wastewater virtual workshop launch by Oct. 2021. | ✓ |
| Objective 4: The IECC Water and Wastewater Committee will promote a virtual workshop that results in at least 100 registrants by Oct. 2021. | ✓ |

### Deliverable: Improve the Knowledge and Capabilities of Water/Wastewater Utility Operators in the State of Indiana

| | |
|---|---|
| Objective 1: Work collaboratively with IFA and Indiana Section American Water Works Association to provide free cyber security training for Water and Wastewater utilities. | ✓ |
| Objective 2: Establish and manage a website to provide information and links to critical cyber security information for water/wastewater utilities by utilizing the State of Indiana website. | ✓ |

# Communications Committee

### Deliverable: Establish Indiana Communications Industry Contact List

| | |
|---|---|
| Objective 1: IECC Communications Committee will develop a form and process to collect a central cyber industry contact list by Q2 2023. | ✓ |

### Deliverable: Fusion Operations Engagement Guide

| | |
|---|---|
| Objective 1: IECC Communications Committee and partners will develop a Fusion Operations Engagement Guide.<br>• *Committee continuing to coordinate with IN-ISAC to create this guide.* | IN PROGRESS |

### Deliverable: Terminology Guide

| | |
|---|---|
| Objective 1: IECC Communications Committee will update Communications Sector Terminology Guide by Dec. 2021. | ✓ |
| Objective 2: IECC Program Communications Manager will publish the Communications Sector Terminology Guide to IECC website. | IN PROGRESS |

### Deliverable: Analyze FCC Emerging Organizations and Rules

| | |
|---|---|
| Objective 1: IECC Communications Committee will provide an analysis of FCC emerging organizations and rules. | ✓ |

### Deliverable: Broadband and Local Government Education

| | |
|---|---|
| Objective 1: IECC Communications Committee will complete the rural broadband education packages. | IN PROGRESS |
| Objective 2: IECC Program Communications Manager will publish the rural broadband education packages. | IN PROGRESS |
| Objective 3: Working with identified partners, provide cyber 101 tips for 1,000 individuals and organizations who are learning to operate with high-speed internet. | IN PROGRESS |

# Communications Committee

*Continued*

### Deliverable: Cyber Incident Response Engagement Guide

| | |
|---|---|
| Objective 1: IECC Communications Committee will develop the Communications Sector Engagement Guidance. | **IN PROGRESS** |
| Objective 2: Communications sector partners will distribute the Communications Sector Engagement Guidance to 80% of identified industry and key stakeholders. | **IN PROGRESS** |

# Healthcare Committee

### Deliverable: Long-Term Education

| | |
|---|---|
| Objective 1: IECC Healthcare Committee will update Indiana-focused versions of security education in 2022. | ✓ |
| Objective 2: IECC Healthcare Committee and partners will provide updated Indiana-focused versions of security education to 80% of Indiana healthcare providers in 2022. | ✓ |

### Deliverable: Healthcare Cyber In A Box Toolbox

| | |
|---|---|
| Objective 1: The IECC Healthcare Committee will create a “Healthcare Cyber in a Box” of security education designed for small- to medium-size offices and systems in 2022. | ✓ |
| Objective 2: The Healthcare Committee will update Healthcare Cyber in a Box to incorporate the Healthcare Industry Cyber Practices (HICP). | ✓ |
| Objective 3: Complete revisions by July 1, 2023 (Version 2.0). | ✓ |
| Objective 4: Complete additional revisions by April 2024. | ✓ |

### Deliverable: Vendor Management – Healthcare IT Security, Risk and Compliance Handbook

| | |
|---|---|
| Objective 1: IECC Healthcare Committee will draft the initial document including key outline of processes and procedures Indiana providers need to implement by Q3 2022. | ✓ |
| Objective 2: Circulate the document among the members of the IECC Healthcare Committee for revisions and edits by Q4 2023. | ✓ |
| Objective 3: The Healthcare Committee will release a Vendor Management guidance document by July 1, 2024. | ✓ |

### Deliverable: Post HSCC Cyber Training

| | |
|---|---|
| Objective 1: Post “Cybersecurity for the Clinician” videos and training on the in.gov/cybersecurity site by July 1, 2023. | ✓ |

# Healthcare Committee
*Continued*

### Deliverable: Exercise

Objective 1: Working with partners, participate in a statewide cyber exercise that affects healthcare industry by Aug. 2021. ✓

Objective 2: Working with partners, participate in an exercise with the Indiana National Guard at Muscatatuck by Aug. 2021 that addresses a known cyber vulnerability. ✓

### Deliverable: Tabletop Exercises

Objective 1: The Healthcare Committee will work with CISA and the Suburban Health Organization to host a tabletop exercise by Dec. 31, 2023. ✓

- IU Health Bloomington — December 2022
- IU Health Arnett — August 2024

### Deliverable: Cyber Sharing Platform

Objective 1: IECC Healthcare Committee will beta test with the Cyber Awareness and Sharing Working Group by Q1 2022. ✓

# Defense Committee

### Deliverable: Cyber Market System

| | |
|---|---|
| Objective 1: IECC Defense Development and partners will review the current cybersecurity market pursuit plan and system in 2021. | ✓ |

### Deliverable: Cyber Digital Platform

| | |
|---|---|
| Objective 1: IEDC Defense Development and partners will develop a pilot of the Indiana defense cybersecurity market development and capture plan and system (digital platform) in 2021. | ✓ |
| Objective 2: Indiana increases to 2% (about $300M) of the Department of Defense (DOD) cybersecurity market share ($15B plus) by FY 2025. | ON HOLD DUE TO FUNDING |

### Deliverable: Cyber Statewide Testbed

| | |
|---|---|
| Objective 1: Establish a nationally recognized cybersecurity test bed in Indiana by June 2021. | ✓ |
| Objective 2: Indiana captures 5% of the international cybersecurity market share of cybersecurity test, training and demonstration plan and capability by Dec. 2025. | IN PROGRESS |

### Deliverable: Cybersecurity Capability Maturity Model (CMMC) Program

| | |
|---|---|
| Objective 1: IEDC and partners will develop a Cybersecurity Capability Maturity Model framework in Indiana by Dec. 2021. | ✓ |
| Objective 2: IEDC and partners will promote Cybersecurity Capability Maturity Model (CMMC) in Indiana to 80% of key stakeholders and associations by Jan. 2022. | ✓ |

# Defense Committee

*Continued*

### Deliverable: K12 Engagement

| | |
|---|---|
| Objective 1: IECC Defense Industrial Committee will identify K12 e-sports event partner(s) by Fall 2024. | ON HOLD DUE TO FUNDING |
| Objective 2: IECC Defense Industrial Committee will participate in at least one e-sports event that helps students understand their e-sports skills and abilities are transferrable to cybersecurity and other STEM careers by May 2025. | ON HOLD DUE TO FUNDING |
| Objective 3: IECC Defense Industrial Committee will work with the Workforce Development committee on any potential policy recommendations for its plans in 2025. | ✓ ONGOING |

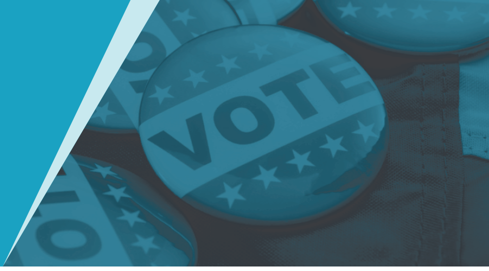
### Deliverable: Student Enrollment Mix in University STEM/Cyber Programs

| | |
|---|---|
| Objective 1: IECC Defense Industrial Committee will research and analyze the ratio of U.S. students in key Indiana post-secondary STEM/cyber programs and identify the root causes of student enrollment ratios with select universities. | IN PROGRESS |
| Objective 2: IECC Defense Industrial Committee will determine best courses of action to improve the ratio of U.S. students in key Indiana post-secondary STEM/cyber programs to feed into the 2024 plan. | IN PROGRESS |

### Deliverable: Remain in Indiana After Graduation

| | |
|---|---|
| Objective 1: IECC Defense Industrial Committee will partner with other groups (i.e., TechPoint's Mission41k initiative) to help identify and propose potential courses of action to increase the percentage of Indiana students that remain in the state after graduation from post-secondary institutions. | IN PROGRESS |

# Elections Committee



### Deliverable: Collaboration with State, Federal and Sector Communities

Objective 1: The Secretary of State will continue active engagement with allied organizations indicated in the state's strategic plan.

✓ ONGOING

Objective 2: The Secretary of State will continue to engage in election cybersecurity collaboration with allied organizations every year as appropriate.

✓ ONGOING

### Deliverable: Integration of Cybersecurity Professionalism, Awareness and Practice

Objective 1: The Secretary of State will promote integration of experienced, trained and professionally certified cybersecurity resources into all phases of election administration by Nov. 2024.

✓

Objective 2: More than 80% of state and local election officials and administrators will be provided ongoing cybersecurity awareness, training and/or certification opportunities by Nov. 2024.

✓

### Deliverable: Election Infrastructure Monitoring, Hardening, Testing and Auditing

Objective 1: The Secretary of State will promote election infrastructure monitoring, hardening, testing and auditing improvements every year until Dec. 2024.

✓

### Deliverable: Public Engagement and Confidence

Objective 1: The Secretary of State will maintain a high level of public engagement regarding election security and public confidence by Nov. 2024.

✓

### Deliverable: Continuity, Coordination, Maintenance of Effort and Oversight

Objective 1: Indiana Statewide Voter Registration System Core Team will begin formally coordinating and overseeing the deliverables of the IECC Elections Committee Strategic Plan by Dec. 31, 2022.

DETERMINED TO BE OUT OF SCOPE

Objective 2: Indiana Statewide Voter Registration System Core Team will assist with all the deliverables and objectives in the IECC Elections Committee Strategic Plan and report the progress to the IECC by Dec. 31 each year.

✓ ONGOING

# Economic Development Committee

### Deliverable: Investment

| | |
|---|---|
| Objective 1: The Economic Development Committee with the Indiana Economic Development Corporation (IEDC) will develop an economic development support framework for Indiana companies to thrive in the cybersecurity landscape. | ✓ |
| Objective 2: Companies that move, start, or grow here will have a framework economic development support. | ✓ |

### Deliverable: Leadership — Cybersecurity Influencers

| | |
|---|---|
| Objective 1: IEDC will work to identify potential partners, activities and initiatives of cybersecurity influencers in the State of Indiana. | ✓ |
| Objective 2: Measure the effectiveness of IEDC supported activities and initiatives in the cybersecurity space. | ✓ |

### Deliverable: Leadership — Technical Assistance Plan

| | |
|---|---|
| Objective 1: IEDC and partners will develop a cybersecurity technical assistance plan in Indiana. | ✓ |
| Objective 2: Measure the effectiveness of the Cybersecurity technical assistance plan by the number of participants (40). | IN PROGRESS |

### Deliverable: Local and Regional Outreach

| | |
|---|---|
| Objective 1: Connect local and regional economic development resources with the developed Cyber Toolkit and other resources.<br>• Expand committee membership<br>• Identify local and regional needs<br>• Establish needs through 2024 | ✓ ONGOING |

# Workforce Development Committee

### Deliverable: Enhance CyberSeekIN.org Data Tool — Workplace Pillar

| | |
|---|---|
| Objective 1: Indiana Department of Workforce Development (DWD) will add credential engine certifications data to CyberSeekIN.org by June 2022. | ✓ |
| Objective 2: DWD to continue data enhancements to CyberSeekIN.org including continual updates to training providers, apprenticeship data/ opportunities and promote opportunities, training and events surrounding cybersecurity in Indiana by Oct. 2022. | ✓ |

### Deliverable: Cybersecurity Talent Pipeline and Job Openings Dashboard — Workplace Pillar

| | |
|---|---|
| Objective 1: DWD to create cybersecurity workforce dashboard metrics measuring Indiana's job demand, talent pipeline, apprenticeships and training opportunities by Dec. 2022. | ✓ |

### Deliverable: Cybersecurity Talent Pipeline — Workplace Pillar

| | |
|---|---|
| Objective 1: Workforce Development Committee (WDC) will create cybersecurity apprenticeship and internship guidelines aligning to 2023 House Bill 1002 by Dec. 2023. | NOT STARTED |
| Objective 2: WDC will inventory and curate apprenticeship opportunities and resources relevant to cybersecurity by Dec. 2023. | NOT STARTED |
| Objective 3: WDC will develop a toolkit for organizations looking to begin an apprenticeship program for cybersecurity utilizing curated resources by Dec. 2024. | NOT STARTED |

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

| | |
|---|---|
| Objective 1: Governor's Workforce Cabinet with support from Indiana Department of Education (IDOE) will develop and promote a high school CTE Program of Study in Cybersecurity by June 2022. | ✓ |
| Objective 2: IDOE will develop a menu of cybersecurity-related professional development and resources, including K-12 computer science offerings by June 2022. | ✓ |
| Objective 3: IDOE and Cybersecurity Program Director will edit and distribute the Cybersecurity for Education Toolkit 2.0 by Aug. 2023. | ✓ |

# Workforce Development Committee

*Continued*

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

| | |
|---|---|
| Objective 1: The Joint Cybersecurity Task Force will ensure more than 75,000 staff and students are delivered training and phishing support through the KnowBe4 platform by Dec. 2024.<br>• *As of Sept. 17, 2024, there are 129,417 users.* | ✓ |
| Objective 2: The Joint Cybersecurity Task Force will raise awareness of schools to digital threats to the educational process by raising awareness through regular newsletters and by working with partners to provide professional development for school IT staff by Dec. 2024. | ✓ |
| Objective 3: DOE will work to encourage all schools to appoint one staff member to monitor information releases from the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the Indiana Information Sharing and Analysis Center (IN-ISAC) by Dec. 2023. | ✓ |
| Objective 4: Create a DOE Moodle Community to share school cybersecurity information with public, religious and private schools as well as provide opportunities for secure collaboration and sharing of best practices by Dec. 2021. | ✓ |
| Objective 5: WDC will support the IECC Defense Committee's Cybersecurity esports event (this event is now planned for Q1 2025). | IN PROGRESS |

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

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

# Cyber Resiliency and Response Working Group

### Deliverable: State Cyber Exercises

| | |
|---|---|
| Objective 1: The State of Indiana will develop and execute a Cross-Sector Critical Infrastructure Cyber Tabletop Exercise by Aug. 2021. | ✓ |
| Objective 2: IECC will work with INNG to incorporate a cyberattack with a natural disaster exercise during the Homeland Defender Exercise by Aug. 2021. | ✓ |
| Objective 3: The State of Indiana will develop and execute a Cross-Sector Critical Infrastructure Cyber Operational Exercise. | IN PROGRESS |

### Deliverable: Cyber Emergency Education to Local Law Enforcement

| | |
|---|---|
| Objective 1: Indiana State Police (ISP) and Cybersecurity Program Director will work to develop the Cyber Emergency Response Education for Local Law Enforcement by May 2022. | ✓ |
| Objective 2: ISP and IECC partners to distribute the Cyber Emergency Response Education to 80% of Local Law Enforcement. | IN PROGRESS |

### Deliverable: Emergency Manager Cybersecurity Toolkit 2.0 (Annual Update)

| | |
|---|---|
| Objective 1: IECC Resiliency and Response Working Group will update the Emergency Manager Cyber Response Toolkit every year. | ✓ ONGOING |
| Objective 2: Indiana Department of Homeland Security will launch a workshop using the Emergency Manager Cyber Response Toolkit every year. | IN PROGRESS |

### Deliverable: Cyber Annex and Cyber Liaison

| | |
|---|---|
| Objective 1: Indiana Office of Technology (IOT) and IDHS will edit and distribute the IDHS Cyber Annex to appropriate parties by Q4 2022. | ✓ |
| Objective 2: IOT and IDHS will edit and distribute the Cyber Liaison Officer role's standard operating procedures by Q4 2022. | ✓ |
| Objective 3: IOT, IDHS and IECC partners will exercise the IDHS Cyber Annex with the cyber liaisons. | IN PROGRESS |

# Cyber Resiliency and Response Working Group

*Continued*

### Deliverable: INNG State Cyber Capabilities

| | |
|---|---|
| Objective 1: The Indiana National Guard will inform state leadership and committee of their cyber response capabilities to a statewide cyber emergency when directed by a federal disaster declaration or ordered to State Active Duty by the Governor. | **IN PROGRESS** |

# Cyber Awareness and Sharing Working Group

### Deliverable: Public Relations Campaign Plan Update

| | |
|---|---|
| Objective 1: The IECC Communications Program Manager will use the 2018 Statewide PR Cybersecurity Campaign Plan and develop a phased approach to the tactics as resources allow by June 2023. | ✓ |
| Objective 2: IECC Program Communications Manager will leverage the assets of Indiana's cybersecurity program to create an increasingly larger presence on social media channels including X, LinkedIn and Facebook, increasing its subscription by 30% each fiscal year. | ✓<br>ONGOING |
| Objective 3: The IECC Program Communications Manager will utilize a weekly blog as a tool for measurably increasing public awareness by further positioning Indiana as a leader in cybersecurity and increasing its subscription by 25% each fiscal year. | ✓<br>ONGOING |

### Deliverable: Inventory of Cyber Sharing Resources

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

### Deliverable: MS-ISAC Member Recruitment

| | |
|---|---|
| Objective 1: Indiana-ISAC will work to increase MS-ISAC membership by 25% each calendar year. | ✓<br>ONGOING |

### Deliverable: Best Practices

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

# Cyber Awareness and Sharing Working Group

*Continued*

### Deliverable: Cyber Sharing Maturity Model

| | |
|---|---|
| Objective 1: IECC Cyber Awareness and Sharing Working Group will edit and post Indiana's updated cyber sharing maturity model by Sept. 2024. | ✓ |
| Objective 2: IECC Cyber Awareness and Sharing Working Group will distribute Indiana's updated cyber sharing maturity model to critical infrastructures through 90% of Indiana's associations by Aug. 2025. | IN PROGRESS |

### Deliverable: Cyber Sharing Community Slack Channel

| | |
|---|---|
| Objective 1: IECC Cyber Awareness and Sharing Working Group will create the Slack Channel by Dec. 2021. | ✓ |
| Objective 2: IECC Cyber Awareness and Sharing Group and the IECC Healthcare Committee will conduct a beta test of the Slack Channel by Dec. 2021. | ✓ |
| Objective 3: Complete the Live Production Launch of the Slack Channel. | ✓ |

# Privacy Working Group

### Deliverable: Indiana PII Guidebook

Objective 1: IECC Privacy Working Group to update the Indiana PII Guidebook for government and general public by May 2024. ✓

### Deliverable: Indiana Privacy Toolkit

Objective 1: IECC Privacy Working Group to develop an Indiana Privacy Toolkit for the Indiana business community, public sector and local government by May 2024. ✓

Objective 2: At least 200 users have accessed/downloaded the Indiana Privacy Toolkit for the Indiana business community, public sector and local government by Dec. 2024. ✓

# Legal and Insurance Working Group

### Deliverable: Cyber Insurance Toolkit

Objective 1: IECC Legal and Insurance Working Group will develop a Cyber Insurance Toolkit to be provided to local government and businesses by May 2023. ✓

Objective 2: With an effective communications plan, the IECC Legal and Insurance Working Group will help point more than 1,000 users to access the Cyber Insurance Toolkit. ✓

### Deliverable: Policy Review

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

### Deliverable: Funds Transfer Fraud Fact Sheet

Objective 1: IECC Legal and Insurance Working Group will develop a Funds Transfer Fraud Fact Sheet to be provided to government and businesses. ✓

### Deliverable: Incident Response Seminar

Objective 1: IECC Legal and Insurance Working Group will conduct an Incident Response Seminar. ✓

### Deliverable: Cyber Insurance Survey — Post-COVID

Objective 1: IECC Legal and Insurance Working Group with Indiana University will conduct a post-Covid survey of businesses for insurance coverage and cybersecurity insurance coverage. ✓

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

# Strategic Resource Working Group

### Deliverable: Policy Research Report

| | |
|---|---|
| Objective 1: IECC and partners will update a report of state and federal cybersecurity legislation by April 2023. | ✓ |

### Deliverable: IECC Scorecard 2.0

| | |
|---|---|
| Objective 1: IECC, along with Purdue University and Indiana State University, will develop a Scorecard 2.0 with a Level Up Guide to improve cybersecurity posture by April 2023. | ✓ |
| Objective 2: IECC will pilot Indiana's Cybersecurity Scorecard 2.0 with Level Up Guide with local governments by April 2023. | ✓ |
| Objective 3: IECC will relaunch an updated downloadable version of the Indiana Cybersecurity Scorecard 2.0 with the Level Up Guide by April 2023. | ✓ |

### Deliverable: Indiana Cyber Success Report (2017-2021)

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

### Deliverable: IECC 2021 Strategic Plan

| | |
|---|---|
| Objective 1: IECC will develop a 2021 Strategic Plan for the Council by Oct. 29, 2021. | ✓ |

### Deliverable: Outreach to Underrepresented Sectors

| | |
|---|---|
| Objective 1: With key partners, identify cybersecurity awareness needs in additional Indiana industries (manufacturing, transportation, small business and agriculture) by May 2025. | ✓ ONGOING |
| Objective 2: Provide industry contacts with education materials and set up a regular communication cadence by Oct. 2025. | ✓ ONGOING |

# Cybersecurity Achievements Occurring in Every Corner of the Hoosier State

The accomplishments that follow are just a key example of what Indiana has to offer its citizens, the nation and the world as we all become even more connected every day. The impact and reach of these achievements positively impact virtually every aspect of our daily lives and provide an added measure of protection for our personal and financial information.

## State of Indiana Agency Collaborations

### Multiple Agencies – Cybertech Midwest

The State of Indiana was pleased to host Cybertech Midwest in 2018, 2019 and 2022.

Cybertech is described as the one of the cyber industry's foremost B2B networking platforms 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.

CYBERTECH
THE GLOBAL EVENT FOR THE CYBER INDUSTRY

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. In 2022, following a two-year absence due to the COVID-19 pandemic, the event returned to Indiana, attracting more than 600 attendees, with an informative agenda that featured presentations by a multitude of Hoosier leaders in cybersecurity, government and the private sector. The conference also served as a showcase for Indiana's multi-faceted cyber capabilities and executive leadership.

https://midwest.cybertechconference.com/

## Indiana Economic Development Corporation Secures $1 Million Cyber Grant for Small Businesses

The Indiana Economic Development Corporation (IEDC) secured a $1,000,000 grant from the Small Business Administration to enhance the cybersecurity posture of small businesses throughout the state of Indiana. Utilizing this funding, the IEDC offers free cybersecurity resources to small businesses, including CMMC L1 assessments, cybersecurity training workshops, and one-on-one cybersecurity implementation sessions. The program is scheduled to conclude in August 2025 and aims to benefit at least 250 small businesses. To access these resources, small businesses can learn more at the IEDC website.

*- Updated December 10, 2024*

## Indiana Statewide 911 Board

At the beginning of 2023, the Indiana Statewide 911 Board invited directors and IT staff from the state's Public Safety Answering Points (PSAPs) to its Annual Directors Summit to announce a comprehensive cyber assessment of Indiana's 117 PSAPs.

Following the summit, regional meetings were conducted to further clarify the assessment's details and scope. The evaluation concentrated on each PSAP's cybersecurity policies, procedures, and recovery plans to identify vulnerabilities and improve resilience against cyber threats. Upon completion of the assessment, each PSAP received a detailed report outlining specific findings, suggestions, and resources for enhancement. The assessment was intended to be constructive, not a pass/fail evaluation.

In support of this initiative, IN911 has engaged in cyber workshops with the National Association of 911 Administrators (NASNA) and the Cybersecurity and Infrastructure Security Agency (CISA). Additionally, IN911 offers ongoing training through its monthly 911 Connects webcast, addressing critical topics such as cybersecurity, call swatting, and the significance of a Continuity of Operations Plan (COOP). These efforts are designed to strengthen the security and operational readiness of Indiana's emergency communication infrastructure.

*- Updated December 10, 2024*

## 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 nearly 7 million Hoosiers.

As part of its ongoing commitment, IOT provides a variety of services for local governments that are free, easy to access and implement and they help reduce the burdens that come with the massive responsibility local governments face. This enables local governments to deliver government services more effectively and efficiently, saving time and money for the higher priority projects. Among the services available include:

- Access Indiana
- Cybersecurity Risk Assessments
- **Cybersecurity Awareness Training**
  - KnowBe4 Administrator Toolkit
  - KnowBe4 Video Demonstration
- **Indiana State and Local Cybersecurity Grant Program Planning Committee (SLCGP Committee)** — Formed in response to the federal Infrastructure Investment and Jobs Act (IIJA), the SLCGP Committee is continuing its work. The committee is involved with the development, approval, implementation, as well as monitoring, reviewing and revising, as appropriate, a strategic plan that establishes funding priorities and approves cybersecurity projects.
- **Virual Town Halls** — Conducted virtually on the second Tuesday of each month, the Town Hall meetings feature notable experts in cybersecurity as a way to inform government officials, as well as interested citizens, with timely information and the latest trends in an effort to help people stay secure in an ever-changing digital world.
- 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 state law, enacted in 2022, 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. Beginning in 2020,

IOT began offering inexpensive website hosting for local governments. Not only are citizens getting a top-notch digital experience, but local government is also receiving the same cybersecurity protections behind state government websites. So far, more than three dozen sites are in process or deployed.

## Cybertrack Partnership with Indiana University and Purdue University

In late 2022, Indiana University (IU) and Purdue University (PU) jointly launched an initiative to build Indiana's local government cybersecurity assessment program. This program is being performed in partnership with the Indiana Office of Technology (IOT) as a part of the State's Whole-Of-State Cybersecurity initiatives.

The ultimate purpose of this work is to make Indiana more secure and resilient, with particular emphasis on cybersecurity at local governments. With this purpose in mind, the program has three goals:

1. Inform the State's Local Government Cybersecurity Policy and Strategy
2. Inform Local Cybersecurity Priorities
3. Improve the Overall Security Posture of the State

The joint IU/PU team developed a standardized assessment methodology and conducted over 100 local government assessments since launching Cybertrack.

The assessments provide local entities with high-quality cybersecurity recommendations and State insights into the local cybersecurity environment in Indiana. The assessment work also informed two Aggregate Analysis & Results reports. These reports provide a striking picture of the state of cybersecurity across local governments and identify clear areas where collective action is needed.

Additionally, the reports describe the Cybertrack assessment methodology, including what we assess, why we assess it  and how we assess it, as well as how we aggregated and analyzed the data from those assessments. Those reports — released in November 2023 and June 2024, respectively — are available without restriction on the Cybertrack website.

The program developed the Cybertrack Assessment Impact Questionnaire as an instrument to begin measuring whether and how assessments are impacting the participating entities.

Initial data from the questionnaire show 94% of participants strongly recommend other local governments participate in the program and 88% have taken some action on recommendations as well as shared the report with their leadership.

Some questionnaire respondents provided thoughts about the program:

- "The assessment removed the fear of the unknown from leadership and gave them a position to begin planning for the future."

- “You don’t know what you don’t know and even if you do know, it never hurts to have another set of eyes.”
- “The City of South Bend very much appreciated participating in the Cybertrack Assessment, it’s never fun being audited but the team was respectful and focused on gaps, areas for improvement, not finding fault or errors. We have continued to self-promote this assessment within IOT and at every summit and meeting we attend. Participants should not be afraid of it. The result will be to be better prepared!”
- “The assessment process was easy and the assessment team was knowledgeable on the topic. The interaction was pleasant and non-judgmental. This is a worthy task.”

Finally, over the program’s short history, the Cybertrack methodology gained notoriety beyond state borders. This shows value the State is deriving beyond Cybertrack’s intended purpose. The following bullets highlight captured since launching the program:

- **September 2023** — The Cybertrack methodology was featured at CISA’s Region 5 meeting in Bloomington.
- **December 2023** — Govtech.com published an interview with Tracy Barnes that highlighted the program.
- **January 2024** — Cybertrack was among the topics discussed when team members Craig Jackson and George Bailey visited the University of Cincinnati-based Ohio Cyber Range Institute. This was a worthwhile meeting leaving the door open for continued engagement.
- **February 2024** — Lawfare published an article prominently featuring Cybertrack. Team members Craig Jackson, Emily K. Adams and Scott Russell were among co-authors contributing to the article.
- **March 2024** — Ann Cleaveland, described the program as a model for what all cybersecurity clinics should be chasing during an IU Center for Applied Cybersecurity Research (CACR) Speaker Series presentation. Cleaveland is a leader in The Consortium for Cybersecurity Clinics and Executive Director of UC Berkeley’s Center for Long-Term Cybersecurity (CLTC).
- **March 2024** — The Wall Street Journal published an article referencing the “Transformative Twelve” set of controls developed as a component of the Cybertrack program.
- **March 2024** — Team member Craig Jackson presented a talk on the Transformative Twelve and Cybertrack findings at NSF’s 2024 Research Infrastructure Workshop.
- **June 2024** — Craig Jackson also served on a panel at the Cyber Civil Defense Summit presented by CLTC. The panel, called “Academia’s Role in Cyber Defense” about the Cybertrack program and lessons learned about how Higher-Ed programs like Cybertrack can help bolster cyber resilience in local communities.”
- **June 2024** — Trusted CI Webinar Series: Craig Jackson presented a talk, The Transformative Twelve: Taking a Practical, Evidence-Based Approach to Cybersecurity Controls.

## Indiana Department of Homeland Security (IDHS)

The Indiana Department of Homeland Security works closely with the Indiana Office of Technology to support a strong posture of protection regarding cybersecurity in Indiana. This includes regular collaboration to discuss real-time incidents when they occur across Indiana as well as integrating county-level protections to prevent against future incidents. The statewide reporting requirements help both state agencies and the State Emergency Operations Center stay poised to respond, recover and protect moving forward.

IDHS and IOT have been extremely active in traveling the state and promoting/supporting the State and Local Cybersecurity Grant Program, a federally funded cyber program designed to protect critical infrastructure and provide critical support to public entities. The program has been successful by working closely to identify gaps and vulnerabilities and maximizing the federal dollars allocated to Indiana. Each visit to local governments created valuable connections and allowed for educational opportunities regarding the true cyber threats facing Indiana and beyond. IDHS and IOT have created a road map of how the grants should be distributed to counties to mitigate threats and provide access to critical training to strengthen the network of end users through education. The ancillary benefits have included better relationships with local governments, better reporting outcomes and a stronger Hoosier presence in the cybersecurity realm.

Other IDHS activities to strengthen Indiana's cyber posture include:

- Partnering with Indiana State Police, CISA and the FBI and other cyber experts to provide resources to specific counties that have experienced a hack or ransomware incident. The communities understand the state is here to support them and help them explore potential actions and protections for the future. Public and private entities in Indiana have been a target for cyber criminals in recent years and each incident has been mitigated and resolved positively through collaborative efforts across the state.
- Working with all 92 county Emergency Managers (EMAs) to provide cybersecurity templates and other resources to conduct assessments in their communities and share resources provided in the Indiana Cyber Hub website that are available for public consumption. These resources include content from IOT and CISA and incorporate the latest protections and guidance for local governments. IDHS continues to prioritize education to EMAs on this subject and provide tools necessary for EMAs to play a critical role in protecting their communities.
- Conducting six regional tabletop exercises through a collaboration between IDHS, IOT, the Indiana Secretary of State, CISA and others to help local communities evaluate their cybersecurity posture.
- Providing additional training through the statewide Acadis portal. The training leveraged national first responders' consortiums approved by FEMA to host cybersecurity courses for state and local government entities.

- Working closely with the Indiana Secretary of State, CISA, the Indiana Elections Board and others to support #Protect2024, the national election security initiative throughout the primary and general election cycles. These collaborative meetings have proven extremely beneficial in dispelling rumors and better communicating cybersecurity concerns from the national to the local level during one of the most intense election cycles in history.
- Distributing the 2024 Presidential Election and Polling Place Security Guidance to all EMAs and local elected officials. This first-of-its-kind document for Indiana provides essential knowledge and resources for securing the election process and specific physical locations during the election season, including cyber-related safeguards.

## Indiana Utility Regulatory Commission (IURC)

Cybersecurity is a fundamental part of a utility's business operations. Cyberattacks on utilities can lead to disastrous consequences, including physical equipment damage, power outages and breach of confidential information. Recognizing this, the IURC continues to engage utilities on cybersecurity to ensure utilities and grid operators provide safe and reliable service to Hoosiers.

### Cybersecurity and Physical Security Meetings

The IURC has continued to conduct confidential briefings with utilities and grid operators to learn about their ongoing efforts against physical and cyber threats. In October 2022, the IURC hosted a briefing from the state's five investor-owned electric utilities, Citizens Energy Group and the state's two grid operators regarding their cybersecurity plans and preparedness. Representatives from the Indiana Department of Homeland Security, Indiana Army National Guard, Federal Bureau of Investigation, Transportation Security Administration, Cybersecurity and Infrastructure Security Agency and Indiana Executive Council on Cybersecurity also attended the briefing. In February 2023, the IURC hosted informational briefings with the electric investor-owned utilities on their efforts related to physical security. Finally, in September 2023, the IURC hosted cybersecurity briefings with the same investor-owned utilities to follow up on the discussions in the October 2022 forum and any updates to their preparedness that had occurred since that time.

## Water Utility Outreach & Training

In 2022, the IURC distributed a cybersecurity questionnaire to the Commission's jurisdictional water utilities with fewer than 10,000 customers to assess their cybersecurity capabilities, efforts and readiness. The responses were gathered to help the IURC understand current capabilities in the areas of threat identification, protection, detection, response and recovery. In 2024, the IURC's Water and Wastewater Division plans to provide resources, compiled from the Cybersecurity and Infrastructure Agency and other organizations, to strengthen their cyber defenses and further protect against threats.

The IURC also facilitated a cybersecurity training session with the Cybersecurity and Infrastructure Security Agency for regulated small water utilities during the 2022 and 2023 Small Utility Workshop.

https://www.in.gov/iurc/water-and-wastewater-division/small-utility-workshop/

The IURC is hosting a series of meetings in fall 2024 to gain a better understanding of the cybersecurity practices employed by larger jurisdictional water/wastewater utilities in the state.

## State Energy Assurance Plan

In 2022, the IURC partnered with the Indiana Office of Energy Development, Indiana Department of Homeland Security and other state agencies to update the State Energy Assurance Plan for Indiana, per guidance issued by the U.S. Department of Energy. The plan is a requirement under the Infrastructure Investment and Jobs Act to receive federal funds and included an assessment of Indiana's energy security landscape and suggestions on how to strengthen utility cybersecurity statewide.

https://www.energy.gov/scep/state-energy-security-plans

## Cybersecurity Tabletop Exercises

IURC staff continue to engage with stakeholders and have been involved in multiple exercises to enhance emergency and cybersecurity preparedness in the energy sector. In July 2023, IURC staff participated in a tabletop exercise with the Indiana Department of Homeland Security — which ran parallel to the Federal Emergency Management Agency Region 5 Power Outage Incident Annex Functional Exercise scenario — in an effort to review and update the state's response strategies concerning long-term power outages. IURC staff also observed a utility's participation in GridEx VII in November 2023, which simulated a real-world cyber and physical threat and was designed to stress-test crisis response and recovery plans.

https://www.nerc.com/pa/CI/ESISAC/Pages/GridEx.aspx

### National Committee on Critical Infrastructure

In 2023, IURC Commissioner David Veleta was appointed as Co-Vice Chair of the National Association of Regulatory Utility Commissioners' (NARUC) Committee on Critical Infrastructure, which provides state regulators a forum to analyze solutions to utility infrastructure security and delivery challenges, as well as share best practices and build collaboration with federal and private sector counterparts. The IURC also has representation on NARUC's Staff Sub-Committee on Critical Infrastructure.

https://www.naruc.org/core-sectors/critical-infrastructure-and-cybersecurity/

### Outreach with Jurisdictional Municipal Utilities

In August 2023, the IURC shared information with jurisdictional municipal utilities regarding the free cybersecurity offerings by the Indiana Office of Technology. Those resources include online training for employees, cybersecurity assessments and incident reporting. The goal of the effort was to provide an added layer of protection and help municipal utilities and local units of government identify/explore potential vulnerabilities.

https://www.in.gov/iot/local-government-services/

## Indiana Department of Education (IDOE)

Indiana DEPARTMENT OF EDUCATION

### Cybersecurity for Education Toolkit

The Cybersecurity for Education toolkit was created 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 worked with the IECC program director and communications manager in developing a turnkey resource.

Updated in 2023, the Cybersecurity for Education Toolkit 2.0 is an easy-to-understand resource complete with the latest tips and trends to help schools be cyber safe. In August 2023, the toolkit was prominently featured as part of a national educational summit at The White House.

https://www.in.gov/cybersecurity/files/Indiana-Cybersecurity-for-Education-Toolkit-2.0-FINAL-AUGUST-7.pdf

## Indiana's Cybersecurity Collaboration in K-12 Education Cited as Key Finding in Nationally Recognized Report

The following is from the 2024 State EdTech Trends survey and report. This report provides insights on the top priorities in this field and shines a spotlight on the work being done in many states, including Indiana.

**Spotlight on Indiana: Strengthening Cyber Security through Collaboration**

As technology becomes an integral part of K-12 school systems and classrooms, state leaders have been empowered to help district leaders — particularly those in small and resource challenged communities — secure those systems from cyber attacks. The state of Indiana has been tackling this work since 2018, when the state launched a cybersecurity taskforce through a partnership with the Indiana Consortium for School Networking chapter. For the Indiana Department of Education (IDOE), collaboration across school systems and with other state leaders has been central to this work.

For Director of Educational Technology at IDOE, Brad Hagg, "It all begins with building good relationships and establishing trust to create an environment where people are vulnerable enough to share where their current challenges lie and are also willing to work with colleagues to get better." In 2021, IDOE established a secure online community for verified school personnel. Built on the cybersecurity task force's earlier efforts, the online community provides a platform for local tech directors to post alerts, discuss strategies and distribute educational materials statewide.

Importantly, IDOE collaborated with state leaders, the cybersecurity task force and the Indiana Office of Technology (IOT), in launching several impactful initiatives to support the state's K-12 community:

- Providing a cybersecurity awareness platform to all schools to provide training for their employees on key cybersecurity concepts.
- Bringing together over 1000 city officials and district tech directors from all 92 counties to explore opportunities to collaborate and share services to lower costs and provide quicker access to offline data backups.
- Partnering with Purdue University and Indiana University to offer school systems training and free cybersecurity assessments.
- Ensuring that K-12 education received the necessary funding and programmatic support through the federally funded State and Local Cybersecurity Grant Program

Acknowledging the impact of the work of IOT and IDOE on improving overall cybersecurity in the state, including K-12 schools, Governor Holcomb awarded the team the Governor's Public Service Achievement Award last October. As noted by

Tracy Barnes, the Chief Information Officer at the Indiana Office of Technology: “The Indiana Office of Technology has been fortunate to collaborate with the Indiana Department of Education (IDOE) and together, we have completed transformative cybersecurity initiatives across our state’s educational landscape, forging partnerships with and between city officials and district tech directors that have spawned an innovative culture of collaboration and shared resources, leading to both cost savings and enhanced security measures.”

In Indiana, K-12 cybersecurity really has been a team sport, which has been critical to ensuring that the state’s efforts benefit every community. “Our partnership with IDOE has been instrumental in fortifying the cybersecurity landscape across K-12 schools in our state,” said Pete Just, the executive director of the Indiana Chief Technology Officer Council and the chair of the Cybersecurity Task Force, “By bringing together resources, expertise and a shared commitment to protecting our educational institutions, we’ve been able to extend critical support to districts that might otherwise struggle to implement robust security measures.”

## Treasurer of State’s Office, Indiana Bond Bank

### Cybersecurity Podcast Series: “Days of Our Cyber Lives”

Over a series of 18 podcast episodes, in 2020 and 2021, Indiana Bond Bank, State Treasurer Kelly Mitchell, the IECC and a rotating panel of expert guests highlighted timely cybersecurity issues and tips for local units of government.  The Treasurer of State’s Office believes this is the first and only podcast of its kind in the U.S. generated by the public sector for the public sector on cybersecurity.

www.in.gov/cybersecurity/home/days-of-our-cyber-lives-podcast-series-its-must-see-cyber-tv/

## Purdue University

### Purdue earns superior rating for industrial security from DCSA

Earlier this year, the Defense Counterintelligence and Security Agency (DCSA) conducted a day-long industrial security review, rating Purdue University as "superior" and establishing Purdue among the top 2% in industry for industrial security compliance and effective counterintelligence programs and measures.

https://it.purdue.edu/newsroom/articles/240614-purdue-earns-superior-rating-from-defense-counterintelligence-and-security-agency.php

### Purdue earns certification from the International Organization for Standardization/International Electrotechnical Commission

Purdue University has achieved certification in ISO/IEC 27001, the internationally recognized standard for information security management systems, which provides the framework and guidelines for information security of software development, enterprise services, support services and product development.

https://it.purdue.edu/newsroom/articles/240613-purdue-earns-iso-certification-in-three-areas.php

### Purdue Applied Research Institute partners with Cybersecurity Youth Academy for Jordan

The Purdue Applied Research Institute (PARI), a wholly owned non-profit subsidiary of Purdue University, in partnership with CERIAS and the Princess Sumaya University for Technology launched the Cybersecurity Youth Academy for Jordan (Cyber Academy). The goal of this academy is to support the strengthening of Jordan's overall cybersecurity posture through increasing resilience to cyberattacks and cyber workforce strengthening.

https://www.cerias.purdue.edu/site/jordanyouth

## Purdue Nuclear Engineering startup wins top tech prize from the Venture Club of Indiana

In July 2024, Purdue-based startup Covert Defenses garnered the top prize of $10,000 in the digital tech category at the 2024 Innovation Showcase pitch competition hosted by the Venture Club of Indiana.

https://engineering.purdue.edu/Engr/AboutUs/News/Spotlights/2024/2024-0709-ne-covert-defenses-venture-club

## Purdue professor chairs external board for Sandia Labs digital assurance campaign

Eugene H. Spafford, professor of computer science and internationally recognized authority on cybersecurity, has been chosen to help Sandia National Laboratories in its campaign to manage digital risks to high-consequence systems.

https://www.cerias.purdue.edu/site/news/view/spafford_to_chair_external_board_for_45m_sandia_labs_digital_assurance_camp/

## Defense award launches Purdue project to strengthen cyber-physical systems

A group of Purdue University researchers has launched a multidisciplinary project to model, simulate and analyze cyber-physical systems (CPS), with the goal of rendering such systems more robust and making analysis of the systems more scalable and effective. Code named FIREFLY, the multiphase $6.5 million project is sponsored by the Defense Advanced Research Projects Agency (DARPA) under its FIRE program (Faithful Integrated Reverse-engineering and Exploitation).

https://www.cerias.purdue.edu/site/news/view/defense_award_launches_purdue_project_to_strengthen_cyber-physical_systems/

## Purdue University researchers develop new algorithm that may help prevent power blackouts

No single power utility company has enough resources to protect the entire grid, but maybe all 3,000 of the grid's utilities could fill in the most crucial security gaps if there were a map showing where to prioritize their security investments.  Purdue University researchers developed an algorithm to create that map. Using this tool, regulatory authorities or cyberinsurance companies could establish a framework that guides the security investments of power utility companies to parts of the grid at greatest risk of causing a blackout if hacked.

https://www.cerias.purdue.edu/site/news/view/as_ransomware_attacks_increase_new_algorithm_may_help_prevent_power_blackou/

## CERIAS experts coached guardians of Ukrainian critical infrastructure

https://www.cerias.purdue.edu/site/news/view/cerias_coached_guardians_of_ukrainian_critical_infrastructure/

## Purdue maintains collaborative partnership with national research institute

Purdue University's Center for Education and Research in Information Assurance and Security (CERIAS) is continuing with its partnership with members of the national Cybersecurity Manufacturing Innovation Institute (CyManII), which is focused on cybersecurity and energy efficiency for American manufacturing. Purdue is one of five founding university members of CyManII. The effort is funded by the U.S. Department of Energy.

https://cymanii.org/

## CERIAS technical lead for the newly established ACTION (Agent-based Cyber Threat Intelligence and Operations) Institute

https://www.purdue.edu/newsroom/2023/Q2/nsf-funds-institute-to-research-ai-powered-cybersecurity/

## High-ranking White House representatives attend the 2024 CERIAS Annual Security Symposium

In attendance were Daniel Ragsdale, deputy assistant national cyber director of the White House Office of the National Cyber Director and Heidy Shyu, under secretary of defense for Research and Engineering (U.S. Department of Defense).

https://www.cerias.purdue.edu/site/symposium/

## Lionfish establishes strategic partnership with Purdue University

Lionfish Cyber Security recently announced a strategic partnership with Purdue University's Center for Education and Research in Information Assurance and Security (CERIAS).

https://www.lionfishcybersecurity.com/2022/11/03/lionfish-cyber-security-announces-strategic-partnership-with-purdue-university/

## Purdue University continues involvement in the Indiana Statewide Academic Alliance for Cybersecurity

Co-organized by the NSF CyberSMART Center Project, the Indiana Statewide Cybersecurity Summit aims to equip business professionals with advance cybersecurity skills and knowledge. Shawn Huddy, director of strategic partnerships for Purdue's Center for Education and Research in Information Assurance and Security (CERIAS), served as session chair.

https://indianacybersummit.org/#e09fe4fd-18e3-4d1d-949e-2ea4274e99aa

## Purdue University sends representatives to NATO advanced research workshop in Washington, D.C.

In July, 2024, the Cyber-Physical-Social Infrastructure Climate Change (CPSICC) Nexus workshop was conducted with an aim to identify the building blocks of risk that lie at the nexus of climate change cybersecurity, critical physical infrastructure with an emphasis on food-energy-water (FEW) systems and social systems with an emphasis on policy, legal frameworks, institutions and migration. It was co-directed by Matthew Huber, Director of Purdue University's Institute for a Sustainable Future (ISF).

https://cpsiccnexusworkshop2024.org/

## Purdue University's Managing Director for CERIAS serves on panel at the 2024 RSA conference

Joel Rasmus, the managing firector of the Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University, served as an expert contributor during the 2024 RSA Conference, giving a presentation titled "Art of Possible: Transforming How We Develop the Next-Gen Cyber Workforce."

https://www.rsaconference.com/experts/joel-rasmus

## Niche-Filling new course meets aircraft, spacecraft industries' workforce need

Offering "Cyber + X" program that assembles students from multiple departments and majors to work as an interdisciplinary team addressing problems/opportunities presented by corporate partners.

https://www.purdue.edu/newsroom/2022/Q4/niche-filling-new-course-meets-aircraft-and-spacecraft-industries-workforce-need/

## Purdue, IU, Notre Dame join to create state wide consortium for national defense

https://www.cerias.purdue.edu/site/news/view/purdue_iu_notre_dame_join_to_create_statewide_consortium_for_national_defen/

## Purdue University's Computer and Information Technology program creates framework to support implementing data governance in small and medium enterprises

Purdue's Computer and Information Technology PhD program investigated the effects of the Lean Six Sigma (LSS) quality approach in supporting the implementation of data governance and data privacy in small and medium enterprises (SMEs). Working in conjunction with Indiana's Indiana Executive Council on Cybersecurity (IECC), the research team created a framework for implementing and improving operations in data governance, utilizing Lean and Six Sigma tools.

The impact of this study is a practical approach to serve the approximately 534,000 business and 1.2 million employees that comprise Indiana's small and medium enterprise business profile.

https://polytechnic.purdue.edu/departments/computer-and-information-technology

*- Updated December 10, 2024*

## Ivy Tech Community College

### Shelby Senior Services "Cybersecurity with Pam Schmelz"

Utilizing her skills and experience as a professor of cybersecurity at Ivy Tech Community College, Pam Schmelz donated her time by leading a series of free seminars designed to help senior citizens with helpful tips to protect themselves when they are online and keep their personal data and financial information secure.

## REN-ISAC – Information Sharing and Analysis Center for the Higher Education Sector

The REN-ISAC is the information sharing and analysis center for the higher education sector and it serves more than 750 member institutions across the globe through promoting cybersecurity operation protections and response. The organization also acts as the Computer Security Incident Response Team (CSIRT) for the research and education community of North America. The following information includes its achievements for 2021-2024.

- **Celebrating 20 Years of REN-ISAC** — 2023 marked the 20th anniversary of the founding of the REN-ISAC at Indiana University.
- **Membership Growth** — Since 2021, our membership has continued to grow from 677 member institutions in Jan 2021 to 772 at the end of July 2024. While the institutions are the members, their relevant staff make up our community, which has grown from 2,871 to 3,690 people during that same period.
- **CSIRT Notifications** — REN-ISAC serves as CSIRT for the research and education community of North America. Our team monitors, receives, and analyzes concerning trends and questionable incidents 24 hours a day and 7 days a week. Timely information is then disseminated to the affected institution. CSIRT recipients do not have to be REN-ISAC members.
    - 2021: REN-ISAC sent out a combined total of 45,748 CSIRT notifications, including:
        - 28,649 Notifications for compromised hosts
        - 14,854 Compromised credentials
        - 351 Spam and phishing messages
        - Contacting an average of 927 unique institutions per month
    - 2022: Sent 162,053 CSIRT notifications, including:
        - 145,291 Compromised hosts
        - 14,226 Compromised credentials
        - 561 Spam and phishing messages
        - Contacting an average of 1,287 unique institutions per month

- 2023: Sent 150,659 CSIRT notifications, including:
  - 56,751 Compromised hosts
  - 92,358 Compromised credentials
  - 122 Spam and phishing messages
  - Contacting an average of 1,792 unique institutions per month
- 2024 (first half): Sent 11,804* CSIRT notifications, including:
  - 289 Compromised hosts
  - 10,908 Compromised credentials
  - 266 Spam and phishing messages
  - Contacting an average of 633 unique institutions per month

  **Numbers were lower than average due to technological issues not industry trends.*

- **Ransomware Tracking** — In 2022, REN-ISAC began tracking ransomware incidents in higher education across the US.
  - 2022: Tracked 55 incidents
    - Top three ransomware groups: Vice Society, Cl0p, and LockBit 3.0
  - 2023: Tracked 58 incidents
    - Top 3: Vice Society, Cl0p, and LockBit 3.0
  - 2024 (first half): Tracked 9 incidents
    - No top 3. All institutions tracked were hit by different ransomware groups.
- **Daily Watch Report** — Consistently our top-rated member service, the Daily Watch Report (DWR) is a situational awareness report covering the latest vulnerabilities, attacks, malware, alerts, and much more. Every business day our DWR editors scour hundreds of news, patches, and alerts feeds to create a comprehensive yet digestible report of the day's top stories in higher ed information security. From Jan 1, 2021, to July 30, 2024, we have delivered 660 reports to over 3,000 readers.
- **Webinars** — We offer a wide selection of public, and members only informational webinars presented by staff, member representatives, and sponsors.
  - 2021: 7 webinars
    - 4 public, 3 members only
    - 157 recorded registrations, 476 participants
  - 2022: 12 webinars
    - 9 public, 3 members only
    - 756 registrations, 555 participants
  - 2023: 7 webinars
    - 6 public, 1 members only
    - 646 registrations, 432 participants
  - 2024 (first half): 5 webinars
    - 3 public. 2 members only
    - 943 registrations, 570 participants

- **Information Sharing Initiatives** — Our members and the higher education community rely on timely, up-to-date information to bolster their information security posture. The REN-ISAC is honored to work with some of the nation's most trusted cyber intelligence organizations to keep our community informed on:
    - Concerning trends and questionable incidents, such as data dumps, sinkholed domains, and phishing campaigns
    - Indicators of compromise from a variety of threat vectors, including phishing, brute force attacks, and compromised credentials
    - Malicious IP addresses and domain name histories
    - Reliability and viability of cloud services, especially focusing on security and privacy issues unique to higher education
    - Education and training in a broad range of information security, privacy, and policy topics
- **Information Security Assessment and Advisory Services (ISAAS)** — For the past 5 years, the REN-ISAC has offered an information security assessment service for higher education organizations. From Jan 2021 through July 2024, we have served 24 unique institutions with our assessment service, performing 29 assessments and 7 pen tests.

  Just this past month (July 2024), we have rebranded and expanded those services as REN-ISAC's Information Security Assessment and Advisory Services (ISAAS). ISAAS offers an expanded catalog of services, including:
    - Comprehensive General Assessments: Utilizing the NIST Cybersecurity Framework, these assessments provide a thorough evaluation of an institution's security posture, offering objective evaluations, actionable recommendations, and an executive summary to support budget proposals and improve security measures.
    - Policy, Process, and Compliance Reviews: Focused reviews of policies, processes, and compliance efforts—including HIPAA, FERPA, GLBA, and NIST SP 800-171 Gap Analysis — that strengthen overall compliance and security operations. Policy, process, and compliance reviews can be purchased individually or bundled with a Comprehensive General Assessment at a discounted rate.
    - Penetration Testing: Simulated attacks conducted to identify vulnerabilities in both on-premises and cloud environments resulting in a detailed report with recommendations for improving security controls.
    - Kickstart Engagements: An affordable, high-value service created to help smaller institutions rapidly enhance their security posture with currently available resources. These engagements provide tactical, operational, and strategic guidance to help build a robust foundation for a successful information security management program.
    - Incident Response Tabletop Exercises: Customized exercises to test and improve an institution's incident response plans. These simulations help identify weaknesses and provide actionable recommendations for enhancing response strategies.

- **RIMM Conferences** — The REN-ISAC Member Meeting (RIMM) is an exclusive event for REN-ISAC members that offers space for networking, knowledge sharing, and discussing cybersecurity operational protection and response. The conference features updates around existing REN-ISAC resources, previews of new services, and presentations from colleagues in the industry.
- **Public Advisories and Publications** — REN-ISAC alerts and notifications are normally conducted within the private membership, but there are times when public alerts are necessary. Since Jan 2021, we have published ten alerts and advisories on topics such as high impact vulnerabilities, a ransomware incident case study, the impact DHS CISA "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements" would have on colleges and universities, and more. We also regularly communicate with the public through our blog and social media channels.

*- Updated December 10, 2024*

## Lionfish Cyber Security

Lionfish Cyber Security is a mission-driven, disabled veteran-owned company that brings a unique approach to cybersecurity by adopting the Green Beret philosophy of "By, With and Through." This strategy focuses on collaboration and empowerment to deliver comprehensive risk management solutions tailored for clients across critical infrastructure, local governments and small- to mid-sized businesses.

Among the achievements Lionfish Cyber Security accomplished:

- Jeremy Miller, CEO of Lionfish Cyber Security, was honored as a Tech Exec of the Year by the Indianapolis Business Journal (IBJ). This prestigious award recognizes Miller's visionary leadership in the cybersecurity industry and his commitment to fostering innovation and growth within Lionfish.
- Launch of a groundbreaking initiative, the first-of-its-kind Cyber Awareness Training that Rocks. This innovative program transforms traditional cybersecurity education by integrating the power of music to create an engaging, memorable learning experience. By leveraging familiar tunes and rhythms, the training aims to make critical cybersecurity concepts more accessible and enjoyable for participants.
- Introduction of a Cyber Sentinel program, providing high school students with early IT and cybersecurity classes and connecting the students (from Purdue University) with college level "cyber guardians" using a mentor-mentee model to help them gain critical career skills in the cybersecurity field and use it as a scalable model for schools across the country.
- Selection as a Best of Tech nominee for the 2024 TechPoint Mira Awards in the categories of Tech Innovation Team of the Year, Talent Impact Award, Digital Transformation Award and Startup of the Year.
- Publication of four significant papers in the IEEE Journal, recognized as the world's largest technical professional organization.
- Approval secured from the Cybersecurity Maturity Model Certification Accreditation Body (CMMC AB) to become a Licensed Training Partner (LTP).

- Introduction of the world’s first Cyber Cybersecurity Workforce Development Platform at Scale.
- Agreement to provide its High School Cyber Pre-Apprentice Internship and Apprenticeship Programs under The New Pursuit Institute in Hamilton County, Indiana.
- Granted Patent Pending status for its AI Training Methodology for optimizing employee training and compliance audits.
- Leading the establishment of the Indiana Chapter of the Armed Forces Communications and Electronics Association (AFCEA), with Miller serving as the founding president.

## CDW Education – Cybersecurity Coalition for Education

Designed as a free cybersecurity maturity assessment for K-12 schools the Cybersecurity Coalition for Education is a group of leading EdTech organizations, including CDW Education, committed to making cybersecurity preparedness and training more accessible for schools.

The coalition pioneered a groundbreaking education-focused approach to measuring and improving cybersecurity readiness, the Cybersecurity Rubric (CR) for Education. Along with the rubric, the coalition provides training and certification designed to guide schools to cybersecurity readiness. Tom Ashley, an advisory member of the IECC, is involved with the effort as a Certified Cybersecurity Rubric Evaluator (CCRE). In doing so, Ashley offers free assisted cybersecurity assessments and works with his colleagues to build other specific, affordable complementary assessments to help improve the security posture of K-12 districts across the United States.

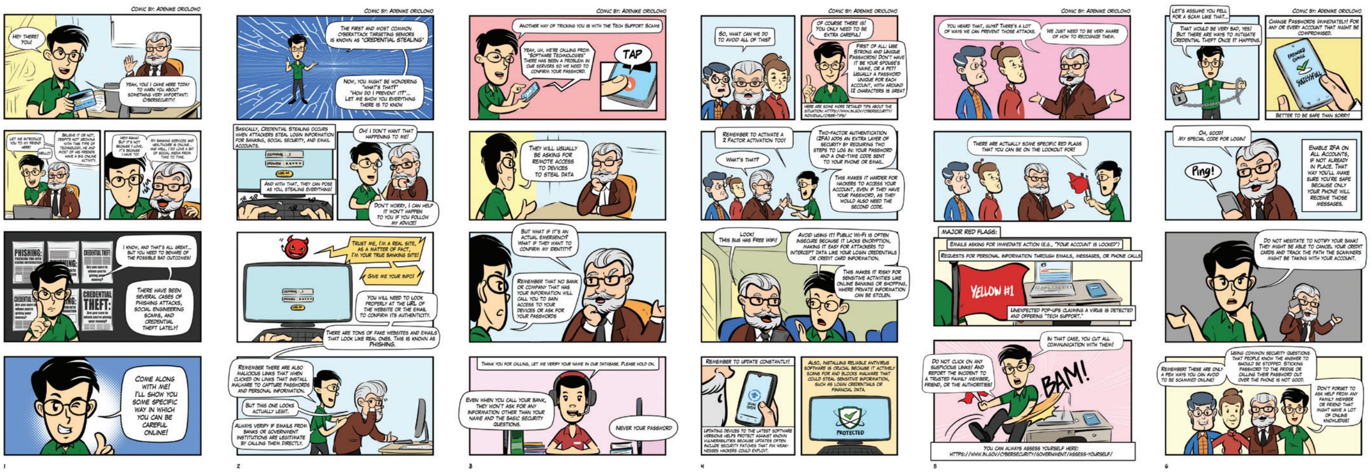
CR CYBERSECURITY RUBRIC

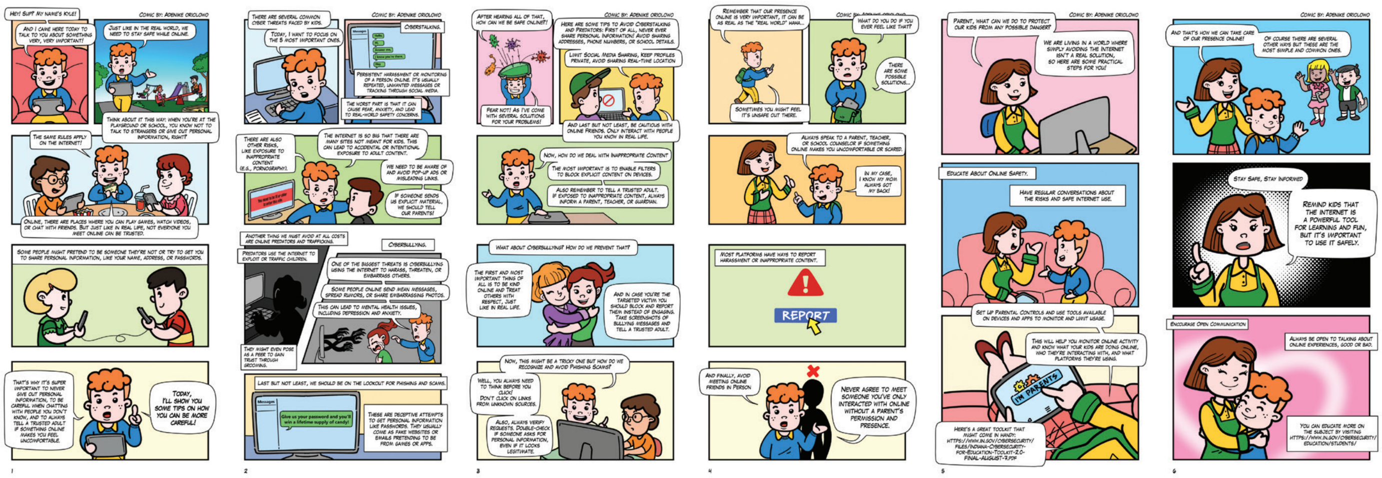
# IECC Advisory Member Creates Comic Strips to Illustrate Importance of Cybersecurity

By day, Adenike Oriolowo works as a cybersecurity engineer for the City of Indianapolis and as a member of the digital strategy team for the Indianapolis Public Schools. She also serves the state and her community as an advisory member of the Indiana Executive Council on Cybersecurity.

As part of her work and perhaps, by night, it could be said that she is working to help educate senior citizens and school-aged children, teens and young adults with a series of comic strips she's created to help people learn about cybersecurity in a way that's fun, informative and engaging.

And while there's nothing funny about the realities involved with a cybercrime or a scam that targets an older adult, a child, or a teenager, Oriolowo sought to find a way to positively share a cyber-friendly message. Hence, the idea to use (and create) the comic strips; something that, for a lot of us, we either grew up reading in a newspaper or we were told stories about the comics that were read by our parents or grandparents when they were growing up. To learn more about Adenike and her comic strip adventures, visit the Indiana Cyber Hub blog.

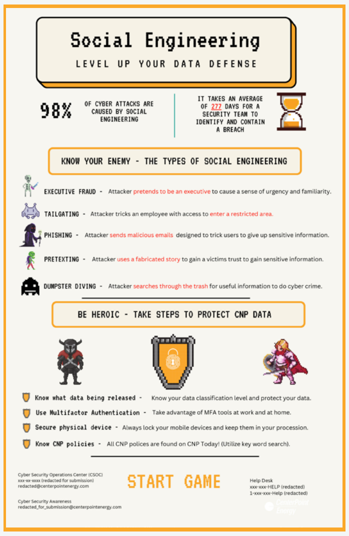




## CenterPoint Energy's "Level Up Your Data Defense" Poster Earns Top Award in Federal Competition

A poster submitted by CenterPoint Energy's Cybersecurity Awareness program was selected as the winner of the National Institute of Standards and Technology's (NIST) 2024 Federal Information Systems Security Educators' Association (FISSEA) Poster Contest. The entry, titled "Level Up Your Data Defense," is recognized as the best poster in this annual competition by the FISSEA committee, which celebrates outstanding creativity and effectiveness in cybersecurity communication.

*- Updated December 10, 2024*



Social Engineering

LEVEL UP YOUR DATA DEFENSE

98% OF CYBER ATTACKS ARE CAUSED BY SOCIAL ENGINEERING

IT TAKES AN AVERAGE OF 277 DAYS FOR A SECURITY TEAM TO IDENTIFY AND CONTAIN A BREACH

KNOW YOUR ENEMY - THE TYPES OF SOCIAL ENGINEERING

EXECUTIVE FRAUD - Attacker pretends to be an executive to cause a sense of urgency and familiarity.

TAILGATING - Attacker tricks an employee with access to enter a restricted area.

PHISHING - Attacker sends malicious emails designed to trick users to give up sensitive information.

PRETEXTING - Attacker uses a fabricated story to gain a victims trust to gain sensitive information.

DUMPSTER DIVING - Attacker searches through the trash for useful information to do cyber crime.

BE HEROIC - TAKE STEPS TO PROTECT CNP DATA

Know what data being released - Know your data classification level and protect your data.

Use Multifactor Authentication - Take advantage of MFA tools at work and at home.

Secure physical device - Always lock your mobile devices and keep them in your procession.

Know CNP policies - All CNP polices are found on CNP Today! (Utilize key word search).

Cyber Security Operations Center (CSOC)
xxx-xx-xxxx (redacted for submission)
redacted@centerpointenergy.com

Cyber Security Awareness
redacted_for_submission@centerpointenergy.com

START GAME

Help Desk
xxx-xxx-HELP (redacted)
1-xxx-xxx-Help (redacted)

CenterPoint Energy

## Water Sector Cyber Training

Joint Effort by the Indiana Section of the American Water Works Association, American Water Works Association, Indiana Finance Authority and the Indiana Executive Council on Cybersecurity (IECC).

- The purpose of the collaboration is to provide training for water/wastewater sector companies, vendors, agencies, and operators. Nearly 350 individuals representing more than 200 entities, including eight agencies, 174 public water systems and 19 vendors.
- The trainers utilize the AWWA (American Water Works Association) cyber training and risk assessment web-based training.  The outputs of this training are a cyber security plan (that meets the Indiana State Law requirements, and a risk plan that meets the requirements of AIWA).

*- Updated December 10, 2024*

## Cybersecurity Infrastructure and Security Agency (CISA)

The Cybersecurity and Infrastructure Security Agency works with partners to defend against today's threats and collaborates with industry to build more secure and resilient infrastructure for the future. The programs and services CISA provides are driven by their comprehensive understanding of the risk environment and the corresponding needs identified by our stakeholders. CISA's advisors who service Indiana seek to help organizations better manage risk and increase resilience using all available resources, whether provided by the federal government, state government, or their own capabilities. CISA also:

- fosters innovative and collaborative partnerships that enable stakeholders in the government and the private sector to make informed and voluntary risk management decisions and investments.
- shares information with critical infrastructure partners and serves as the national hub for cybersecurity and communications information, physical threats like bombings, and active shooter situations, and data sharing in near-real time.
- provides capacity building, technical assistance, tools, exercises, training programs, and awareness efforts that improve understanding of common risks and possible mitigation strategies for the critical infrastructure community, especially with cybersecurity education and resilience programs.
- serves as the federal lead for cyber incident response activities with the private sector, state, local, tribal, and territorial governments (SLTTs).
- coordinates with public and private sector partners to support National Security Special Events, like the Indianapolis 500, and offers risk management strategies to help stakeholders manage the consequences of emerging and future risks.
- collects and analyzes risk data to inform and prioritize risk management activities to prioritize critical infrastructure and associated National Critical Functions.
- uses processes, tools, and technologies to assess cyber and physical threats to people and property, and the potential consequences of those threats.
- enhances public safety interoperable communications at all levels of government.

With respect to the role CISA plays in Indiana's cybersecurity efforts, CISA continues to partner with the leadership of the Indiana Executive Council on Cybersecurity (IECC) and leading collaborative efforts within industries to assure the security, resilience, and reliability of the nation's cyber systems.

CISA drives national efforts through collaboration with private sector, academia, and government partners to build a diverse cyber workforce, foster development, and use of secure technologies, and promote best practices. Indiana saw this with the 2024 elections where CISA provided cybersecurity and physical security services to more than 80 percent of all Indiana counties, which further secured them for the presidential elections.

CISA also detects and prevents cybersecurity risks where possible by sharing information, deploying detective and preventative technologies, publishing technical products and guidance, and providing incident response and "hunt" capabilities to minimize impacts of identified incidents and an evolving threat landscape. CISA also plays a key advisor role for the State and Local Grant Cybersecurity Program (SLCGP), led by the state's Chief Information Officer.

*- Updated February 20, 2025*

## Transportation Security Administration (TSA)

- Since the Colonial Pipeline cybersecurity incident in 2021, TSA Surface Operations nationally and in Indiana have made significant strides in cybersecurity for pipeline and freight rail owner/operators, including issuing pipeline and rail Security Directives (SDs) and conducting cybersecurity outreaches and training:
- Pipeline SDs: TSA issued cybersecurity mitigation Pipeline Security Directives (SDs) that required pipeline owner/operators to submit Cybersecurity Implementation Plans (CIPs) to TSA for approval and inspection, Cybersecurity Assessment Plans (CAPs), Cybersecurity Incident Response Plans (CIRPs) and Cybersecurity Vulnerability Assessments (CVAs). Additionally, operators must ensure all measures are assessed/audited within a three-year cycle and provide an annual report to TSA. TSA inspected all pipelines subject to the SDs for compliance with cybersecurity requirements.
- Rail SDs: In October 2022, TSA issued SDs that required cybersecurity measures mirroring those required of pipelines to mitigate cyber threats to rail transportation systems. The SDs require operators to identify cybersecurity coordinators, report cybersecurity incidents and submit a CIP and CAP, among other measures. As of August 2024, 100% of CIPs in this TSA region (Region 3) have been fully approved (for those with and without Critical Cyber Systems). By September 2024, TSA will have inspected all covered railroads for compliance with SD requirements.
- Cybersecurity outreaches and training: TSA hosted three virtual meetings with the freight rail industry to ensure pipeline operator inspection readiness and understanding of SD changes. Performed facilitated cybersecurity assessments with a railroad and a school

bus corporation using the publicly available Cyber Security Assessment Tool (CSET). TSA also hosted three virtual meetings with the pipeline industry to ensure pipeline operator inspection readiness and understanding of SD changes. TSA also conducted cybersecurity "Five Non-technical actions to take in 5 days" (5N5) workshops with multiple pipeline owner/operators to enhance understanding of cybersecurity threats and mitigations.

- TSA established a Security Operations-Compliance Cybersecurity Inspection Team (SCIT) nationally to perform inspections and outreaches with regulated aviation entities regarding TSA's cybersecurity requirements. The Indianapolis International Airport (IND) has adhered to cybersecurity incident reporting requirements mandated by TSA and CISA. IND has also designated a cybersecurity coordinator who is available to TSA and Cybersecurity and Infrastructure Security Agency (CISA) 24/7 to address any cybersecurity incidents and concerns. IND has also developed a CIRP designed to mitigate the risk of operational and business disruption if the airport is impacted by a cybersecurity incident. Fort Wayne International Airport (FWA) and South Bend International Airport (SBN) have also both appointed cybersecurity coordinators for their respective airports.
- In July 2022, the TSA Indiana Compliance Field Office (TSA IND Compliance) and Surface Operations hosted a 5N5 workshop with 18 representatives of Indiana transportation and other entities, including airports, all-cargo aircraft operators, energy/utility companies, indirect air carriers/freight forwarders (IACs), maritime ports, mass transit bus operators and pipelines. The Federal Bureau of Investigation (FBI) gave a threat briefing; CISA also participated.
- In November 2023, TSA IND Compliance hosted webinars for certified cargo screening facilities (CCSFs) and indirect air carriers (IACs). Both webinars hosted a cybersecurity advisor from CISA, who gave an overview of services that CISA can provide for stakeholders. Five CCSFs and 17 IACs attended.
- In April 2024, TSA IND Compliance hosted a cargo symposium for 40 representatives of aircraft operators, CCSFs, IACs, third-party canine companies (3PK9) and their authorized representatives. CISA again presented on its services.

# What's Next for Indiana

At a time when society experienced a record-setting 72% increase in the number of data breaches from 2021 to 2023, it is clear from this report that protecting our critical infrastructure continues to be among the highest priorities for Indiana.

Achieving many of the 80 deliverables and 151 objectives, as defined in the 2021 Indiana Cybersecurity Strategic Plan, 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.

As outlined in our charter, together with the collective body of work that has been achieved since its inception in 2017, the IECC is firmly committed to continuing with its strong relationships and its dedication to collaboration with our partners in the private and public sectors, academic institutions and the military from all over the state, nation and world to develop and maintain our "first of its kind" proven strategic framework that establishes goals, implements plans and shares best practices with Hoosier citizens and businesses.

Likewise, Indiana will continue to support in any way it is able those organizations that are willing to join the IECC and state in the arena. And as President Theodore Roosevelt said, we will join everyone "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 knew 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 that need it most within the state, it 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 the IECC leadership throughout Indiana, Hoosiers will continue to be safer and businesses will continue to thrive.

As Indiana prepares for a change in administration, the Council welcomes the opportunity to continue with the progress it has achieved in cybersecurity. Additionally, the Council looks forward to beginning, in earnest, the work needed to create the 2025 Indiana Cybersecurity Strategic Plan.

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

# Addendum/Updates

**October 25, 2024** - First version of The State of Cyber Report 2021-2024 released.

**December 10, 2024** - This report was updated with the following:

- State of Indiana Agency Collaborations
  - Indiana Economic Development Corporation Secures $1 Million Cyber Grant for Small Businesses
  - Indiana Statewide 911 Board
- Academia
  - Purdue University's Computer and Information Technology program creates framework to support implementing data governance in small and medium enterprises
  - REN-ISAC – Information Sharing and Analysis Center for the Higher Education Sector
- Private/Public Sector
  - CenterPoint Energy's "Level Up Your Data Defense" Poster Earns Top Award in Federal Competition
  - Water Sector Cyber Training

**December 19, 2024** - This report was updated with the following:

- Opening Letter
  - The percentages of completed deliverables and objectives were updated to reflect new stats based on the additional completed objective below
- Privacy Working Group
  - The Indiana Privacy Toolkit deliverable's second objective was updated from in progress to completed

**February 20, 2025** - This report was updated with the following:

- Opening Letter
  - Updated to include the Secretary of the Indiana Office of Public Safety
- National
  - Cybersecurity Infrastructure and Security Agency (CISA)