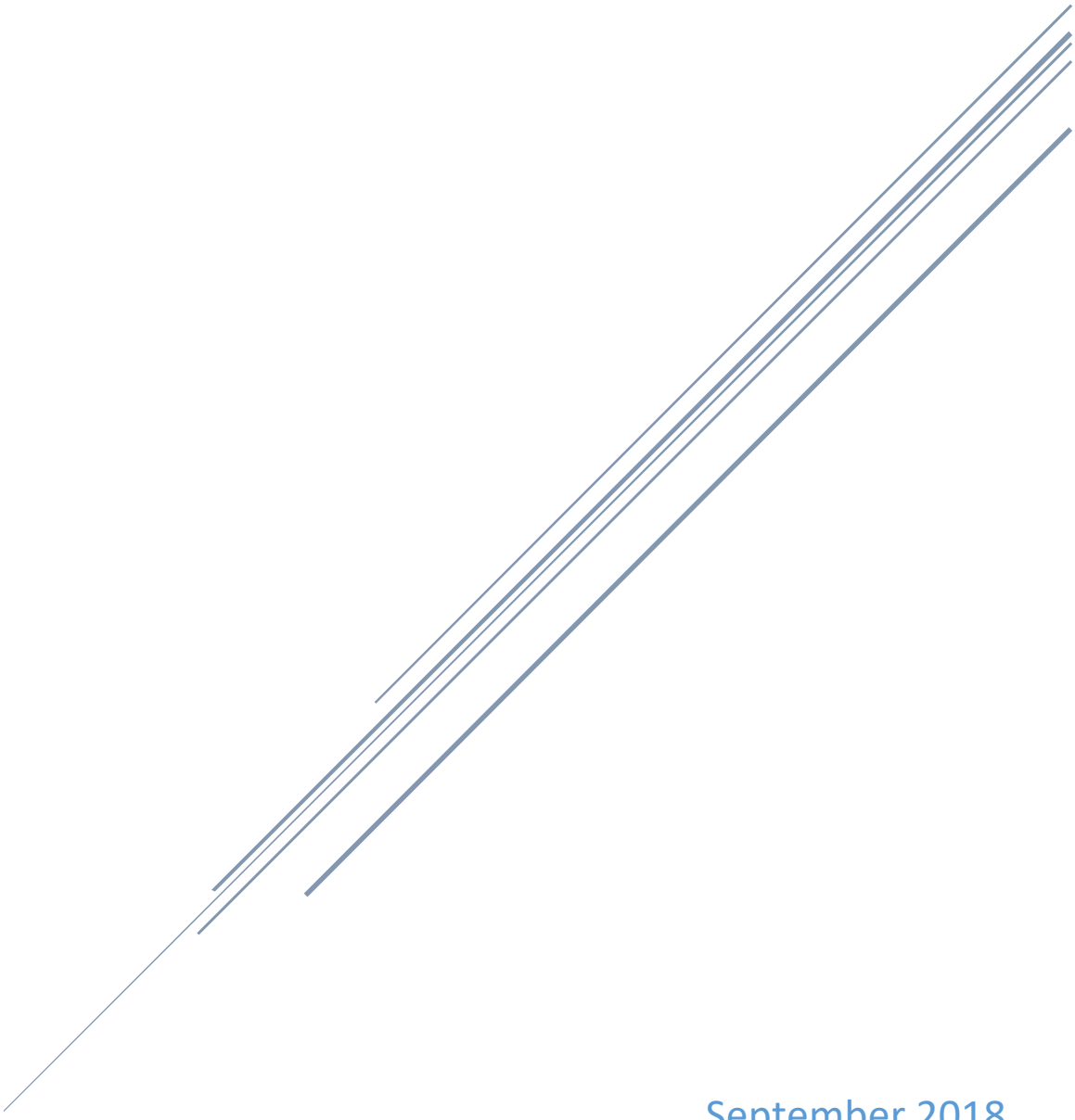
WORKFORCE DEVELOPMENT COMMITTEE STRATEGY PLAN

Chair: Commissioner Fred Payne | Co-Chair: Dr. John Keller



September 2018

Indiana Executive Council on Cybersecurity

Workforce Development Committee Plan

Contents

Committee Members

Committee Members

Name	Organization	Title	Committee Position	IECC Membership Type
Fred Payne	Indiana Department of Workforce Development	Commissioner	Chair	Voting
Jeff Tucker	Indiana Department of Workforce Development	Chief Information Officer	Chair Proxy	Voting Proxy
Dr John Keller	Indiana Department of Education	Chief Technology Officer	Co-chair	Advisory
Sean Roberts	Code.org	Director of State Government Affairs	Full Time	Advisory
David Greer	Project Lead The Way	Senior Vice President and Chief Program Officer	Full Time	Advisory
Benjamin Carter	Indianapolis Public Schools	Director of Career & Technical Education	Full Time	Advisory
Jim Goldman	Salesforce	VP, Security Governance, Risk Management & Compliance	Full Time	Advisory
Geanie Umberger, PhD	Purdue University	Associate Dean for Engagement	Full Time	Advisory
Nick Taylor	E-gineering	Owner	Full Time	Advisory
Shane Springer	Indiana Department of Workforce Development	Director of Government & Legislative Affairs	Full Time	Advisory
Matt Etchison	Ivy Tech	Vice President of Information Technology	Full Time	Advisory
Dan Calarco	Indiana University	Chief of Staff,	Full Time	Advisory
Doug Rapp	Cyber Leadership Alliance	President / CEO	Full Time	Advisory
Michael Hawryluk	Indiana Commission for Higher Education	Chief Technology Officer	Full Time	Advisory
Teresa Lubbers	Indiana Commission for Higher Education	Commissioner	As Needed	Voting
Jim Weber	Raytheon	Cyber Security and Specialty Engineering Department Manager	Full Time	Advisory
Matt Norris	Krieg DeVault LLP		Full Time	Advisory
Walt Grudzinski	Vectren Corporation	Director of Information Security and Business Continuity	Full Time	Advisory

Introduction

Introduction

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) and its mission was continued. With the ever-growing threat of cyberattacks, the IECC has been tasked with developing and maintaining a strategic framework to establish goals, plans, and best practices for cybersecurity to protect Indiana's critical infrastructure. The IECC is comprised of twenty committees and working groups who worked together to develop a comprehensive strategic plan and implementation plans. This implementation plan is one of the twenty specific plans that make up the complete 2018 Indiana Cybersecurity Strategic Plan.

Executive Summary

Executive Summary

- **Research Conducted**
  - Searched for:
    - Valid and complete list of all cybersecurity courses/programs/degrees/etc
    - Source for current and future demand for cybersecurity workers in Indiana
    - List of all cybersecurity-related jobs and the skills required to fill those jobs
    - Info on how easy/difficult it is to fill cybersecurity jobs, currently
    - List of programs designed to generate interest in cybersecurity and a career in cybersecurity
    - What has happened in the recent past in this area in Indiana
    - Existing data on cybersecurity programs/courses/degrees/certifications and the capability of that data

- **Research Findings**
  - It is difficult in most cases to quickly fill cybersecurity-related jobs with people who have the required skills
  - International Economic Development Council (IEDC) Cyber Initiative report provided a starting point for many of our committee's desired deliverables – framework, program list, job demand challenges, etc.
  - The National Institute of Standards and Technology's (NIST) National Initiative for Cybersecurity Education (NICE) has developed a Cybersecurity Workforce Framework. This framework provides a common language to be used to describe tasks, knowledge, skills, and abilities needed for each cybersecurity work role. This framework is being reviewed by other states and has been adopted by at least two states.
  - There are many existing and effective programs to generate interest in cybersecurity, measure aptitude, provide needed skills and/or certifications, etc. This committee's initial efforts on many of our deliverables will be to develop effective ways to leverage these existing initiatives before trying to create something new.
  - There are other closely related programs to which cybersecurity content could be added to further promote the field of cybersecurity and generate interest.
  - Existing data on cybersecurity programs/courses/degrees/certifications may not be granular enough to satisfy all of our committee goals. Needs further investigation.

- **Committee Deliverables**
  - Generate Interest Plan
  - Job Demand Tool
  - K-12 Offering Cyber Security Content
  - Best Practices and NICE Framework Standard
  - Incentivized Cybersecurity Certifications
  - Program Data Tool

Research

Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity**?
    a. Not Applicable

2. **What (or who) are the most significant cyber vulnerabilities in your area?**
    a. Near-term challenge – a shortage of people with needed skills to fill open cybersecurity positions. The longer-term challenge will be the strategic filling of the pipeline to ensure Indiana is well positioned not just to fill open cybersecurity positions, but to also provide a workforce that would aid in attracting cybersecurity firms to locate in Indiana.

3. **What is your area's greatest cybersecurity need and/or gap?**
    a. Biggest need is people with cybersecurity skills to fill open cybersecurity jobs.

4. **What federal, state, or local cyber regulations is your area beholden to currently?**
    a. Not Applicable

5. **What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?**
    a. From a workforce perspective – there is a Cybersecurity Workforce Framework that has been developed by the National Initiative for Cybersecurity Education (NICE) which is a part of NIST. This framework provides a common language to be used to describe tasks, knowledge, skills, and abilities needed for each cybersecurity work role. This framework has begun to be adopted by other states and tools are being developed to facilitate the implementation of the framework (e.g, a job description writing tool).

6. **What research is out there to validate your group's preliminary deliverables? This could be surveys, whitepapers, articles, books, etc. Please collect and document.**
    a. Indiana has plenty of data about the current state of affairs at various levels of the cybersecurity pipeline including data from Indiana Department of Education (IDOE), Department of Workforce Development (DWD), and Commission for Higher Education (CHE). The IEDC Cyber Initiative report provided a starting point for many of our committee's desired deliverables – framework, program list, job demand challenges, etc.

7. **What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?**
    a. See answer to #5 above.
    b. Cybersecurity course being developed by Project Lead the Way for 10th graders.

8. **What does success look like for your area in one year, three years, and five years?**
    a. Sufficient quantity of skilled workers to fill all cybersecurity positions. Ability to see current and future demand for all cybersecurity jobs. Ability to understand the skills associated with all jobs that make up the demand. Ability to see all students in the pipeline that are in programs that provide them the needed skills to fill that demand. A better alignment of activity in the K-12 system and the nurturing that needs to happen to progress from broad competencies in early grades to focused skills and proficiency as students move through high school and into college.

9. **What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?**
    a. This is what our committee is working on as part of the IECC.

10. **What is the total workforce in your area in Indiana? How much of that workforce is cybersecurity related? How much of that cybersecurity-related workforce is not met?**
    a. Due to limitations in how this data is gathered, an accurate number is difficult to determine. Anecdotal data suggests that there are not enough cybersecurity workers to fill all open positions. It is likely that in many cases, employers are filling these positions and providing or arranging for the appropriate training. A key deliverable for our team is to develop methods/models to identify the current and future demand for all cybersecurity jobs in Indiana – the types of cybersecurity jobs and the required skills. It is reasonably assumed that the need for cybersecurity-skilled workers will grow and one specific need will be for K-12 instructors – this may provide an opportunity to look into the feasibility of engaging individuals with cybersecurity expertise as instructors even though they don't have teaching licenses.

11. **What do we need to do to attract cyber companies to Indiana?**
    a. The primary requirement from our Committee's perspective - provide a capable and skilled workforce.

12. **What are your communication protocols in a cyber emergency?**
    a. Not Applicable

13. **What best practices should be used across the sectors in Indiana? Please collect and document.**
    a. National Initiative for Cybersecurity Education Cybersecurity Workforce Framework – provides a common language for all cybersecurity work roles and the tasks, knowledge, skills, and abilities needed for each.

Deliverable: Generate Interest Plan

Deliverable: Generate Interest Plan

General Information

1. **What is the deliverable?**
    a. Increase awareness and interest in cybersecurity careers and degree attainment
    b. Increase the number of Indiana high school graduates with an industry-recognized cybersecurity-related certification
    c. Incentivize and encourage participants to seek education, live and work in Indiana
    d. Provide a pipeline of students that are prepared to successfully achieve post-secondary career goals in cybersecurity.
    e. Utilizing the National Governors Association (NGA) Policy Academy work, develop a proposal to fund and sponsor the rollout of an initiative with the goal of creating a program centered on Cybersecurity, or sponsor a program the covers Pre-K through postsecondary. The Academy also identified the need to pilot professional development programs across the state to increase student interest, awareness, and efficacy in cybersecurity.
    f. Develop and support workforce development programs that provide:
        i. A robust technology platform that includes portals for primary to secondary teachers, instructors and students with career pathways, curricula, and project-based resources
        ii. Resources for teachers related to professional development
        iii. Assessment tools for companies, employees, government for assessing cybersecurity aptitudes and abilities of employees
        iv. Apprenticeship programs for preparing the cybersecurity workforce
        v. Co-ops and internships programs available across the state.
        vi. Middle/high school level network of cybersecurity camps, clubs, and competitions that can incorporate industry-recognized certification curriculum into classroom instruction, with opportunities for students to receive certifications upon completion.
        vii. Fund the curricula development for high school students to graduate with a certificate in cybersecurity, instructed by teachers who have received professional development in cybersecurity.
        viii. Create access and opportunity for underserved and underrepresented populations
    g. Examples include Cyber Patriot (listed in the following planning pages), IN CyberPath, and GEN Cyber.

2. **What is the status of this deliverable?**
    a. In-progress; 25% Complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
   - ☐ Establish an effective governing structure and strategic direction.
   - ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
   - ☐ Strengthen best practices to protect information technology infrastructure.
   - ☐ Build and maintain robust statewide cyber-incident response capabilities.
   - ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
   - ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   - ☒ Ensure a robust workforce and talent pipeline in fields involving cybersecurity**.**

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
   - ☐ Research – Surveys, Datasets, Whitepapers, etc.
   - ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   - ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   - ☒ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   - ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   - ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

---

5. **What is the resulting action or modified behavior of this deliverable?**
   a. Per the NGA Academy, need to develop a system that instills cybersecurity understanding, education, and ethics throughout a student's entire journey, from Pre-K through post-career.
   b. Provides a mechanism to generate interest among grades Pre-K through 12th grade globally in computer science and specifically in Cybersecurity.
   c. Offers the opportunity for advanced students to graduate high school with a cybersecurity certification, qualifying them for entry-level cybersecurity jobs.

6. **What metric or measurement will be used to define success?**
   a. Number of programs state-wide
   b. Number of participants statewide in the program.
   c. Number of cyber camps state-wide
   d. Creation of statewide cyber competition

7. **What year will the deliverable be completed?**
   a. 2020

8. **Who or what entities will benefit from the deliverable?**
    a. Students
    b. Universities (potentially broaden the pool of degree seekers in cybersecurity).
    c. Private and government sector job market
    d. Industries and general public (greater security for their private information)

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. Programs such as these would probably be in line for funding for STEM (Science, Technology, Engineering, and Math) grants from either state, federal or philanthropic sources with missions aimed at increasing attainment in these areas.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Other high-level cybersecurity program developers. Cyber Patriot is one of a number of programs that could increase informal opportunities for middle and high school students.
    b. Indiana CyberPath program developed collaboratively between Purdue University (Career Makers) and Indiana University (Center for P-16 Research and Collaboration).
    c. A cybersecurity framework that can be adopted in other states.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Potentially the IDOE (state agency)
    b. Indiana Economic Development Corporation (IEDC)
    c. Lieutenant Governors (LG) Office
    d. The Cyber Leadership Alliance
    e. Any number of private organizations, industry professional and industry associations, and non-profits could have a funding interest in Cyber Patriot, Indiana CyberPath, or other similar programs.
    f. Other state universities as necessary to ensure a robust plan

12. **Who should be main lead of this deliverable?**
    a. The Cybersecurity program developers
    b. Appropriate state agencies (e.g. DWD, IDOE, IECC) provide implementation support from an organization with domain expertise and implementation know how.

13. **What are the expected challenges to completing this deliverable?**
    a. Funding
    b. Logistics
    c. Coordination with broader interest generating efforts
    d. Dissemination of the deliverables across the state

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. One-time deliverable (two-year initiative)

Tactic Timeline – Sample Program: Cyber Patriot

Tactic	Owner	% Complete	Deadline	Notes
Prep & Plan	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	80%	Award of funding (A)+2	
Awareness (Marketing campaign)	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	0%	A+3	
Identify Schools	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	10%	A+4	There are 70 existing programs in Indiana
Club Sponsor /Faculty Training event	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	0%	A+5	Regional
Camps yr. 1	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	40%	Jun18-Aug18	Venues and sponsors for camps identified
Training event (certification curriculum)	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	0%	Jun18-Aug18	
Club yr. 1	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	0%	Aug18-May19	
Regional & State finals @ MUTC	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	20%	Jan19/Feb19	Commitment from the Indiana National Guard to host and sponsor
Camps yr. 2	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	40%	June19-Aug19	Venues and sponsors for camps identified

Club yr. 2	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	0%	Aug19-Jun20	
Regional & State	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	0%	Jan20/Feb20	
Identify corporate sponsors	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	50%	A+9	Cyber Leadership Alliance members have made tentative commitments
Refine established baseline metrics	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	0%	A+11	Initial metrics
Grant winner training	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	0%	A+17	Top performing clubs will receive small grant to offset cost of State competition & training
Competition/ Training event	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	0%	A+18	
Program Review	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	0%	A+24	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Line Item	Price	In Kind	Description
Marketing	$20,000.00		ad space, social media campaign, events
Collateral	$10,000.00		physical & virtual materials to support campaign
Messaging	$10,000.00		strategy & messaging of campaign
Training/Kick-off Event	$12,000.00		train-the-trainer event
Regional	$8,000.00		CLA to travel regionally and provide 4 hr seminar in 4 locations
Registration	$22,960.00		Cover cost of registration to incentivize participation. 5% Yr1 & 10% Y2
Supplies	$11,200.00		general supplies
Stipend	$44,800.00		Incentivize teacher participation
Equipment Grant	$10,000.00		free and reduced lunches, ensuring underserved communities meet technical requirements
Certification Grant	$15,000.00		25 grants to top 5% students based upon market penetration
Curriculum	$7,500.00		5 Camps, 1 week of pre-packaged CyberPatriot curriculum
Staff	$15,000.00		2 instructors, $1500 a week
F&OH	$7,000.00		5 locations, $1000 week to cover facility & lunch
Team Scholarship	$10,000.00		20 team scholarships @ $500/team to offset travel expenses
MUTC Facility & OH	$15,000.00		2 day in-person, cyber physical competition @ IN Nat'l Guard MUTC. F&OH, Range Access
Exercise Director	$125,000.00	$ (125,000.00)	Exercise director, all-inclusive cyber-exercise. Scenario & exercise design, red-team, on-site technical support
Coordinator	$35,000.00		50% of full-time implementation coordinator
Project MGMT & Leadership	$65,000.00		50% of full-time project manager/senior consultant
Subtotal	$443,460.00		
In Kind	$ (125,000.00)		
Grand Total	**$ 318,460.00**		

- Funding sources: Request funding from State of Indiana with a significant match from private industry.

Benefits and Risks

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

a. This initiative will educate, grow, and help to retain an Indiana based workforce by focusing on pre-K through 12th grade students, community college and university students, underrepresented and underserved populations, veterans, incumbent workers requiring re-training, minor offenders, and more.

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

a. [No Response]

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

a. According to the Indiana Department of Workforce Development (DWD), Indiana needs to fill more than one million jobs over the next decade. Of those million jobs, more than a third will be new or growth occupations within the state. As the nature of work continues to change at an accelerated pace, the workforce will need new skills to meet the challenge at all levels of education. It is estimated that nearly 30,000 job openings per year will require an industry-recognized certificate/certification in addition to a high school diploma. Without this initiative, Indiana will continue to leave approximately 2,500 cybersecurity jobs statewide unfilled creating an incalculable risk to industry, wealth, and citizenry.
b. Indiana students will continue to graduate from high school lacking the necessary background to successfully achieve cybersecurity career goals, much less an understanding of cyber hygiene.

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

a. Success is defined as a significant increase in the following areas:
    i. Increase to the number of cybersecurity clubs throughout Indiana middle and high schools (anticipated 130% growth within two years).
    ii. Increase the number of students registered in the clubs.
    iii. Number of cybersecurity camps conducted; there are zero in Indiana currently.
    iv. Number of industry certifications awarded to high school students.
    v. Establishment and success of statewide competitions.
    vi. Number of underserved and underrepresented students choose cybersecurity careers.
    vii. Number of students who successfully complete higher education career goals (two or four-year degree).
    viii. Number of participants in cyber apprenticeships, internships, and co-ops.
    ix. Number of participants who moved from any of the programs sponsored, as detailed by this document, and employed in a cyber-job in Indiana.
    x. Reduction in the number of job openings that cannot be filled (for example, determining if is there a decrease in the number of unfilled cyber positions as a result of these programs).

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

a. Yes
b. **If Yes, please list states/jurisdictions**
    i. Indiana has created a similar program focusing on robotics; however, it does not include industry certifications.

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No

Other Implementation Factors

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

a. Ability to procure funding match from government, industry, and private entities.
b. Funding for K-12 and higher education to continue to support the programs once implemented.

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

a. No

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

a. It is anticipated that this initiative will become self-sustaining.

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

a. The coalition for this initiative currently includes 40 formal partners at the local, State, and national levels.

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
    i. All

Communications

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

a. All

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

a. Yes

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

a. This initiative will demonstrate leadership from DWD, DOE, Academia and Industry engaged with the IECC.

Evaluation Methodology

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

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: Launch a statewide cybersecurity program centered for K-12 stakeholder by August 2019.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Job Demand Tool

Deliverable: Job Demand Tool

General Information

1. **What is the deliverable?**
    a. Proposal to modify and adopt Cyberseek as the source for cybersecurity-related job demand. The work group recommends infusing the Cyberseek tool with Indiana specific job demand, among other requirements, to assist Indiana job seekers and employers make more informed decisions.
    b. IN CyberPath will co-develop the Cyberseek tool for Indiana with an education portal that identifies all educational resources in the state and those that map to the NICE Cybersecurity Workforce Framework. The tool will have data analytics portal for industry to access their current workforce and for predicting future needs based on the NICE Framework. The Job Demand Tool will be designed for educators of cybersecurity to input data on the number of students enrolled in cybersecurity education for collecting metrics. Once completed, the mapping will allow for the council to determine the gaps in education, number of students being educated, and plan for future development of curricula through collaboration with providers.

2. **What is the status of this deliverable?**
    a. Not Started

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☐ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☒ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☒ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Will provide all stakeholders (state agencies, educators / training providers, employers) a single-source for cybersecurity-related job demand and education resources in Indiana. This will include the emerging skills, certifications, educations, etc. that employers are looking for from potential job candidates identified through the tools assessment portal. This can then be one additional tool that educators and training providers use as they assess how many cybersecurity-related offerings they provide and the required content that is mapped to the NICE Framework. The tool will also provide a portal for professional development for teachers and access to curricula for K-12.

6. **What metric or measurement will be used to define success?**
    a. Ability of the State to fill the demand for cybersecurity-related jobs. We will work with DWD to design a measurement tool that would include using data from Burning Glass identifying average days to fill cybersecurity-related jobs.
    b. Determine gaps in educational curricula needed across the state which will allow for the committee to plan to fill the gaps and address the lack of educational resources.

7. **What year will the deliverable be completed?**
    a. 2019

8. **Who or what entities will benefit from the deliverable?**
    a. Employers, students, job seekers and educators

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. Bureau of Labor Statistics occupation projections.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. IN CyberPath (Purdue University and Indiana University)
    b. Burning Glass
    c. Public-private partnership proposed via Cyber Economic Development Committee

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. DWD, DOE, CHE, Burning Glass Technologies, IN CyberPath, Cyber Leadership Alliance, Public-private partnership (see above), Purdue University, Indiana University, Ivy Tech Community College

12. **Who should be main lead of this deliverable?**
    a. DWD – R&A Team
    b. IN CyberPath Team

13. What are the expected challenges to completing this deliverable?

a. Building out the required data gathering and technology solution(s) to incorporate Indiana specific data to integrate with Cyberseek and IN CyberPath.
b. Incorporating Cyberseek job demand data and IN CyberPath educational resources tool and assessment portals into our existing eco-system of jobs / workforce data while ensuring data consistency and a cohesive user experience.
c. Marketing/promotion and training for use of the tools and programs

Implementation Plan

14. What is the deliverable?

a. Implementation plan to, modify, and adopt Cyberseek and IN CyberPath as the source for cybersecurity-related job demand and educational resources and assessments for career pathways for Indiana. The Cyberseek data and website can then be enhanced with Indiana specific data pertaining to job demand and salary.

15. Is this a one-time deliverable or one that will require sustainability?

a. Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Procure Cyberseek for Indiana	DWD	0	2019	Awaiting costs/license fees for tool
Procure statement of work from IN CyberPath to provide mapping of state educational recourses and development of the assessment tool for industry				
Develop IN specific data for integration with Cyberseek	DWD	20	2019	
Enhance Cyberseek with Indiana Data from IN CyberPath	DWD	0	2019	
Develop integration plans for consumption of the Cyberseek data across various job seeker, employer, and education platforms utilizing sources from IN CyberPath.	DWD/DOE	0	TBD	Explore how cyberseek will be accessed. (example: direct links and/or API feeds into partner systems.)

Resources and Budget

16. Will staff be required to complete this deliverable?

a. Yes

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
1	0.25	Project manager	State		
1	0.5	Data analyst	State		Data ETL, curation
0.5	0.5	Dev Engineer	State		Software automation
1		Systems analyst	State		Requirement/tech writing/testing

17. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
Data/Compute server	Compute IN specific data	$10k				
Job Scheduler	Automation engine	$1k				

Benefits and Risks

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

a. Cyberseek and the build out with IN CyberPath is a ready-made powerful tool that can be used by employers, educators, policy makers, and job seekers looking to understand cybersecurity-related jobs data within their geographic metro area. Adopting this tool will consolidate our collective efforts and understanding of cybersecurity-related jobs and their corresponding skill needs.

b. Infusing the Cyberseek tool with Indiana specific data and build out with IN CyberPath data and portals will further enrich the tool with data relevant to Indiana job seekers. Enabling better, more informed decisions as they consider cyber pathway options and cybersecurity needs.

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

a. Informing users of employer needs and available openings. The tool can help reduce talent gaps and help direct the supply of cybersecurity workers.

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

a. The risk is continued misalignment between employers, job seekers, policy makers, and training providers. Without the adoption of this tool, these constituents will continue to seek information about cybersecurity jobs from multiple sources which can and often does lead to misunderstanding of the cybersecurity job demand. This tool will also ensure that the State is aligning with the federal Cybersecurity Workforce Framework developed by NICE.

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

a. Reduction in average time to fill for cybersecurity jobs.
b. Measurements of hard-to-fill and expensive-to-fill metrics for these jobs as sourced from Burning Glass technologies and employer feedback.
c. Number of educational recourses in the State for cybersecurity,
d. Gaps in education that exist.
e. Assessment of industry needs for cybersecurity workforce.
f. Level of cyber and general computer science understanding and skills.
g. Number of teachers getting instruction in cyber and computer sciences.
h. Number of cyber internships, apprenticeships, and co-ops at baseline.

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

a. No

23. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No

Other Implementation Factors

---

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

a. The data and software is proprietary and may be subject to scrutiny as competitors enter the market.
b. Understanding the Return on Investment (ROI) across the various constituents may be uncertain as it will take time to measure.

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

a. Yes
b. **If Yes, what is the change and what could be the fiscal impact if the change is made?**
    i. To the extent Indiana adopts Cyberseek as the tool to better understand cybersecurity jobs and skills needed to fill those jobs, then policy could be updated to reflect that

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

a. A commitment to the tool, or comparable one in the future, as a guide to understanding cybersecurity jobs and the skills needed to fill those jobs.
b. Received a plan from IN CyberPath for the mapping and assessment portions of the tool.

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

a. We have reached out the Burning Glass technologies with initial cost estimates for licensing.

28. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
    i. Since career pathway options are illustrated in this tool, then individuals from other sectors looking for a job could benefit by using this tool. Common feeders include legal and business administration (auditors, financial analysts, etc).

Communications

---

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

a. DWD/DOE/CHE

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

a. Yes

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

a. Some competing data providers may develop a similar tool with a focus of cybersecurity-related jobs.
b. As always, and in particular if or when this happens, Indiana will need to be prepared to defend the use of this tool along with the information coming out of it as competitors may raise concerns about the information and lobby for their tool/data to be used instead.

Evaluation Methodology

Objective 1: State of Indiana adopts Cyberseek as the source for cybersecurity-related job demand and career pathways for the state by August 2019.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: State of Indiana will develop integration plans for consumption of the Cyberseek data across various job seeker, employer, and education platforms by December 2019.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: K-12 Offering Cybersecurity Content

Deliverable: K-12 Offering Cybersecurity Content

General Information

1. **What is the deliverable?**
    a. Proposal to ensure an appropriate level of cybersecurity content is included in K-12 computer science offerings (per the Governor's Next Level Plan) and other initiatives, as appropriate (e.g. Hour of Code). On the one hand, this deliverable could be as simple as adding a layer of coordination across existing initiatives. On the other hand, it could be as expansive as creating formal expectations about cybersecurity in the K-12 curriculum with clear connections between the knowledge and skills students should have, when they should have them, and how they can be obtained.
    b. Identify, map and vertically align cybersecurity curricula to state and national standards.
    c. Pilot and scale up IN Cyberpath programs for P-16 and other postsecondary programs to increase student content knowledge and experience in cybersecurity.
    d. Create access and opportunity for underserved and underrepresented populations
    e. Increase the number of individuals going into cybersecurity jobs

2. **What is the status of this deliverable?**
    a. In-progress; 25% Complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☐ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☒ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☒ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Ensures that Hoosiers get exposure to Cybersecurity concepts early. This knowledge will help them decide if they might be interested in pursuing further education and a career in cybersecurity. At a minimum, this makes people more aware of good cybersecurity practices that will benefit them their entire life. The concepts relevant to cybersecurity in the workforce should be mapped back to the K-12 curriculum including broadly relevant content at early grades that would provide foundational understandings, dispositions, and skill development necessary to more focused skill development at the middle and high school levels.

6. **What metric or measurement will be used to define success?**
    a. Number of programs statewide offering with verifiable alignment to cybersecurity concepts and content.
    b. Scope and sequence showing development/articulation of cybersecurity concepts across grades K-12.
    c. Increase in professional development for teachers at all levels.
    d. Development of computer science strategic plans by schools with particular emphasis on the growth and development of students with strong preparation in cybersecurity.
    e. Number of postsecondary courses stood up that allows individuals to receive badges or certificates for indicating course completion.
    f. Number of individuals receiving badges or certificates from completing cybersecurity classes (post graduation)
    g. Number of individuals participating in educational and experiential programs

7. **What year will the deliverable be completed?**
    a. 2023+

8. **Who or what entities will benefit from the deliverable?**
    a. The workforce would be the ultimate beneficiary of this long-range development.
    b. Near-term, students would benefit from more opportunities for science attainment.
    c. Underserved and underrepresented populations will be more evenly represented in STEM careers.
    d. Could also be some benefit of a more informed citizenry—from the more intentional inclusion of cybersecurity in the K-12 curriculum.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. Any funding targeting the development of STEM programming at the K-12 level.

Additional Questions

10. What other committees and/or working groups will your team be working with to complete or plan this deliverable?

a. No plans for work with other groups at the moment. This deliverable will require substantial vision and investment from policymakers and will take years to implement.
b. IN CyberPath via Purdue University and Indiana University

11. Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?

a. DOE along with those who provide content/training for the proposed K-12 computer science offerings across the state.
b. IN CyberPath Team
c. NICE
d. Burning Glass
e. Because of the scale of the work, there could be many contributors but there must be a goal, a shared vision, and an organization anointed to lead the charge.

12. Who should be main lead of this deliverable?

a. IDOE
b. IN CyberPath team

13. What are the expected challenges to completing this deliverable?

a. Ensuring that consistent (and correct) content is included in all of the various offerings/programs statewide.
b. Training teachers
c. Identifying funding
d. Writing curriculum and balancing the proposed additions with other content areas vying for attention within the K-12 curriculum.
e. Integrating cybersecurity curriculum into existing classroom practices
f. Statewide implementation

Implementation Plan

14. Is this a one-time deliverable or one that will require sustainability?

a. Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Increase the number of schools certified through Common Sense Media to 200.	IDOE	80%	Fall 2019	16-17 school year there were 167 Indiana Schools Certified (https://d1e2bohyu2u2w9.cloudfront.net/education/sites/default/files/certified_schools_16_17_final.pdf) There were
Develop K-12 appropriate emphasis for Cybersecurity Month in October	IDOE	0%	October 2018	Could use the cybersecurity month as a platform for promoting an array of options for schools.
Develop an annotated curricular resources hub for K-12 teachers	IDOE	0%	September 2019	This could be at least partially met through the new CyberSecurity programming to be launched by the IDOE.
Develop and implement IN CyberPath	IN CyberPath	0%		This is a three phase program. Phase one include focus groups and development of the cyberseek took for Indiana. Phase two implements pilot programs both K-12 and CareerMakers. Phase three rolls programs out full scale across state.
Identify links between the professional development Code.org is offering to Indiana teachers and the cybersecurity domain.	IDOE	0%	September 2019	
Promote the development of a Cybersecurity Graduation Pathway	SBOE	0%	TBD	The State Board of Education has a process for reviewing Locally Created Pathways as part of the programming they are developing around Graduation Pathways.
Pilot Beta Offering of PLTW CyberSecurity course for 10th graders	IDOE	10%	September 2018	IDOE to fund participation by up to 10 schools interested in piloting this course.
Pilot phishing simulations with students through the state procured platform (Media Pro)	IDOE	0%	September 2019	IDOE is working to make the MediaPro platform available to all Indiana Schools. This platform includes access to a phishing simulation and training content.

Create and adopt a formal set of standards for cybersecurity across the K-12 curriculum	IDOE	0%	September 2019	This is a big lift but would really help to lay the foundation for moving from the piecemeal approach we have now to a more full-court press so all students have basic awareness and understanding about cybersecurity matters—a new essential skill to be an educated citizen.
Create cybersecurity summer camp for k-12 students.	IU	90%	Summer 2018	Indiana University will run the Security Matters Cybercamp for interested students from throughout the state and use the workforce development subcommittee to help promote the camp.
Create CareerMaker course for post-secondary training, offering certificates and/or badges for completion.	IN CyberPath Team	0%	TBD	This is part of the IN CyberPath project with Purdue and IU

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
1.0	1.0	Management coordination, advocacy	State		There are bits and pieces of the tactics enumerated above that are already underway, what is needed is an individual who has the coordination and expansion of these efforts as a primary responsibility.

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
Consultation	Guidance and project management to develop Cybersecurity standards for K-12	TBD	TBD	State/Federal	grants	
Travel	See exemplar programs in action in other locations.	TBD	TBD	State		
IN CyberPath framework	Cyberseek tool developed for Indiana	TBD	TBD	Grants	Industry donations	

Benefits and Risks

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

a. The most important benefit of this deliverable would be the coordination of disparate efforts and the contribution that coordinated efforts could make toward keeping the pipeline of talent full.
b. A statewide cybersecurity interactive tool for Indiana
c. Industry-aligned post-secondary student programs at Purdue University's CareerMakers sites.
d. And assessment tool for collecting metrics from industry

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

a. This would reduce the cybersecurity risk or impact in two ways
    i. Ensuring that all students receive basic exposure to cybersecurity content throughout their time in Indiana schools. We rely on schools to create an educated citizenry. We need our citizenry to have awareness of cybersecurity topics and challenges that is developmentally appropriate.
    ii. Provide aligned exposure to cybersecurity topics throughout the K-12 curriculum including both formal and informal learning opportunities so that more students will consider careers in the area of cybersecurity.
    iii. Provide the opportunity for individuals in the workforce to increase their knowledge in cybersecurity and job opportunities by furthering their education.

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

a. The risk is having uncoordinated investment in many good things that could have greater effect if considered together. Also, if there is no real attention given to cybersecurity awareness and training at the younger ages of the spectrum, we will have to keep putting out fires and being reactive to real and immediate shortages in the job market.

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

a. A clearly articulated cybersecurity program for K-12 that shows the critical path and skills for cybersecurity and how various opportunities, experiences and curricula can fulfill those critical needs. In addition, optional extensions of core concepts in cybersecurity should also be articulated. Indiana should have a clear map of critical cybersecurity content that clearly shows what topics will be encountered at what ages.

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

a. No

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. Yes
b. **If Yes, please list states/jurisdictions**
    i. Indiana would be among the first to implement a cybersecurity curriculum or even to map cybersecurity concepts across the curriculum.

Other Implementation Factors

---

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

a. This thinking requires a long view.
b. The actual return on investment is not as direct as some may like.
c. Any results with direct impact to the economy are years away.

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

a. Yes
b. **If Yes, what is the change and what could be the fiscal impact if the change is made?**
    i. The policy change here would be a formal expectation regarding content and skills about cybersecurity that should be encountered during the K-12 experience.

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

a. An ongoing commitment to revising and amending the cybersecurity curriculum to keep it relevant and responsive to the needs of the workforce and to the needs of society as a whole.

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

a. No formal contacts have been made regarding a coordinated effort on this front although members of the committee are aware of episodic efforts underway.

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
    i. If this deliverable is well-executed, other sectors could experience direct and indirect benefit

Communications

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

a. K-12 Schools

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

a. Yes
b. If formal steps were taken in this area, it should definitely be part of the overall effort outlined on the cybersecurity web site.

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

a. Not all families welcome the use of computers in the classroom and some resist the provision of devices to students. If cybersecurity becomes a curricular emphasis, there will need to be some care given to the education of parents who are concerned that their children are safe and are also concerned about the age-appropriateness of what they know about cybersecurity threats.

Evaluation Methodology

Objective 1: Indiana Department of Education will develop a menu of cybersecurity content and initiatives that includes K-12 computer science offerings by September 2019.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☒ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: Eighty percent of Indiana Schools adopt one or more cyber initiatives by August 2020.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☒ Quantifiable Measurement
☐ Other

☐ Peer Evaluation/Review

Deliverable: Best Practices and NICE Framework Standard

Deliverable: Best Practices and NICE Framework Standard

General Information

1. **What is the deliverable?**
    a. Working with the Nationa Governors Association, the IECC Workforce Development Committee will develop a detailed implementation plan for Indiana adopt cybersecurity workforce best practices and standards, such as the National Initiative for Cybersecurity Education(NICE) Cybersecurity Workforce Framework, and provide tools to the full ecosystem of Indiana's workforce (K-12, educators, students, underemployed, employers, etc.).

2. **What is the status of this deliverable?**
    a. In-progress; 25% Complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☐ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☒ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☒ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. All entities will use the framework as a common language when describing cybersecurity-related jobs, skills, knowledge, abilities, and tasks.

6. **What metric or measurement will be used to define success?**
    a. Ability of the State to fill the demand for cybersecurity-related jobs. We will work with DWD to design a measurement tool that would include using data from Burning Glass identifying average days to fill cybersecurity-related jobs. Determine what educational resources exist that are mapped to NICE (National Initiative for Cybersecurity Education) Cybersecurity Workforce Framework.
    b. Determine what gaps exist in education and curricula.
    c. Ability to assess the needs of industry related to the number of employees that currently exist and future needs based on advancement of technology.

7. **What year will the deliverable be completed?**
    a. 2019

8. **Who or what entities will benefit from the deliverable?**
    a. Any that need to develop cybersecurity-related job description, education curriculums, apprenticeships and resumes. This includes at least: job seekers, educators/training providers, and employers.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. Potentially, any entity with adoption of other NIST standards.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Any entity or group necessary to codify this adoption.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. DOE, DWD, CHE, NIST

12. **Who should be main lead of this deliverable?**
    a. DWD

13. **What are the expected challenges to completing this deliverable?**
    a. Providing various tools to allow users to more easily utilize the framework. Research ongoing to determine priority for what tools may be needed (e.g. job description writing tool) in conjunction with the NICE consortium of various state reps and NGA. Developing curriculum to describe and teach the knowledge, skills, and abilities (KSAs) and Tasks as outlined within the NICE Framework.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. On-going Deliverable

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Begin implementation planning for making NICE the standard across Indiana	IECC Workforce Development Committee / National Governors Association (NGA)	100%	August 2018	See Supporting Documentation for NGA Workshop Materials.
Create and implement statewide outreach program for cybersecurity training that follows best practices and standards, such as the NICE Framework, to underserved communities, minorities, women, veterans, disables, and minor offenders	IECC Workforce Development Committee/NGA	20%	December 2019	
Create and implement statewide program that will provide educators and businesses resources for meeting best practices and standards, such as the NICE Framework, by December 2019.	IECC Workforce Development Committee/NGA	20%	December 2019	
Procure statement of work from IN CyberPath to provide mapping of state educational recourses and development of the assessment tool for industry	Partners	20%	2019	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
[No Response]					

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
[No Response]						

Benefits and Risks

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

a. [No Response]

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

a. [No Response]

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

a. According to DWD, Indiana needs to fill more than 1 million jobs over the next decade. Of those million jobs, more than a third will be new or growth occupations within the state.

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

a. [No Response]

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

a. No

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No

Other Implementation Factors

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

a. [No Response]

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

a. [No Response]

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

a. [No Response]

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

a. [No Response]

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
    i. All sectors benefit from this initiative.

Communications

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

a. All.

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

a. Yes

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

a. None at this time.

Evaluation Methodology

Objective 1: Indiana formally establishes NICE Framework as the cybersecurity standard for the state by October 2019.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: Working with the National Governors Association, the IECC Workforce Development Committee will create and implement statewide program that will provide educators and businesses resources for meeting best practices and standards, such as the NICE Framework, by December 2019.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 3: Working with the National Governors Association, the IECC Workforce Development Committee will create and implement statewide outreach program for cybersecurity training that follows best practices and standards, such as the NICE Framework, to underserved communities, minorities, women, veterans, disables, and minor offenders by December 2019.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Incentivized Cybersecurity Certifications

Deliverable: Incentivized Cybersecurity Certifications

General Information

1. **What is the deliverable?**
    a. Utilizing the NICE framework, provide incentivized cybersecurity certifications to industry across the State of Indiana. This initiative will provide a minimum of 200 industry certifications within two years. On average, certifications will be provided at a 50% cost savings.
    b. Goals:
        i. Create statewide cybersecurity certification training program
        ii. Reduce barriers to entry for cybersecurity education to individuals & Indiana businesses
        iii. Create access and opportunity for underserved and underrepresented populations
    c. IN Cyberpath will utilize resources from Purdue University, Indiana University, Vincennes University, Ivy Tech, and other state institutions of higher education to develop the curriculum for cybersecurity certificates under the IN Cyberpath program.

2. **What is the status of this deliverable?**
    a. In-progress 75%

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☐ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☒ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☒ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. All entities will use the framework as a common language when describing cybersecurity-related jobs, skills, knowledge, abilities, and tasks.

6. **What metric or measurement will be used to define success?**
    a. Ability of the state to fill the demand for cybersecurity-related jobs. We will work with DWD to design a measurement tool that would include using data from Burning Glass identifying average days to fill cybersecurity-related jobs.
    b. Fully developed IN CyberPath Framework is adopted by state and used by educators and industry.
    c. K-12 schools across the state offer cybersecurity courses that align with IN CyberPath framework.
    d. CareerMakers have cybersecurity courses stood up across the state that aligns with IN CyberPath framework.

7. **What year will the deliverable be completed?**
    a. 2019
    b. 2019 for IN CyberPath phase one, 2021 for phase two and 2025 for phase three

8. **Who or what entities will benefit from the deliverable?**
    a. Any that need to develop a cybersecurity-related job description, education curriculums, and resumes. This includes, at least, job seekers, educators, training providers, and employers.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. Potentially any entity with adoption of other NIST standards.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Any entity or group necessary to codify this adoption.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. DOE, DWD, CHE, NIST
    b. Purdue University, Indiana University, Burning Glass

12. **Who should be main lead of this deliverable?**
    a. DWD

13. What are the expected challenges to completing this deliverable?

a. Providing various tools to allow users to more easily utilize the framework. Research ongoing to determine priority for what tools may be needed (e.g. job description writing tool) in conjunction with the NICE consortium of various state reps and NGA. Developing curriculum to describe and teach the KSAs and Tasks as outlined within the NICE Framework.

Implementation Plan

14. Is this a one-time deliverable or one that will require sustainability?

a. One-time deliverable (two-year program)

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Preparation and Planning	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	80%	Award of Funding (A)+1	
Identify Candidates	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	50%	A+2	Cummins, KAR, Wabash, Rofori, etc.
Form first 4 cohorts (G1)	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	0%	A+3	
Finalize Regional Locations	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	80%	A+4	Select university locations statewide
Train First Cohorts (G1)	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	0%	A+6	
Progress Review & Refinement	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	0%	A+7	
Form Second Cohorts (G2)	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	0%	A+8	
Train Second Cohorts (G2)	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	0%	A+10	

Form Third Cohorts (G3)	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	0%	A+13	
Train Third Cohort (G3)	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	0%	A+17	
Form Forth Cohort (G4)	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	0%	A+19	
Train Forth Cohort	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	0%	A+22	
Review	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	0%	A+23	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
[No Response]					

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Line Item	Cost	Detail
Certification Camps	$451,000.00	All-inclusive certification boot camp (lab, exam voucher, materials, labs, instructor, facility). 16, 20-person cohorts for CISA, CISM, CISSP, CEH. 1, 11-person cohort for CIPP). Total 331 spots. Based upon DWD demand data and partner input.
Outreach	$50,000.00	Underserved community outreach, 5 groups: Women, Minority, Hispanic, Veteran, Disabled
Advertising	$20,000.00	Print, Video, Virtual ad space. Social media
Coordinator	$21,000.00	30% of full-time coordinator for implementation & integration
Project MGMT & Leadership	$39,000.00	30% of full-time project manager/senior consultant
Total	$581,000.00	
Private Match	($342,200.00)	CLA: $240,000 - curriculum development. Purdue: $23000 facility EC Council: $68000 vouchers. ISACA: $11,200 vouchers

- Funding sources: Request funding from State of Indiana with a significant match from private industry.

Benefits and Risks

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

a. The initiative will deliver a potential economic impact of over $130 million from activities executed over the two-year period. This claim is based upon the results of the completed Outcomes Worksheet (originally submitted to the Skill-Up committee) with jobs data from Burning Glass and Indiana Department of Workforce Development (DWD). In addition to the significant economic impact by increasing the number of Hoosiers attaining high-paying jobs, making cybersecurity training available and affordable to small and medium-sized businesses reduces barriers to entry and reduces the largest cybersecurity risk surface. Not only will open job requisitions be filled, but it is projected that more companies will relocate high-paying cyber jobs to Indiana to capitalize on the enhanced talent pipeline.

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

a. Refer to previous questions.

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

a. According to DWD, Indiana needs to fill more than 1 million jobs over the next decade. Of those million jobs, more than a third will be new or growth occupations within the State. As the nature of work continues to change at an accelerated pace, the workforce will need new skills to meet the challenge at all levels of education. It is estimated that nearly 30,000 job openings per year will require an industry-recognized certificate/certification in addition to a high school diploma. Indiana will continue to leave approximately 2,500 cybersecurity jobs statewide unfilled creating an incalculable risk to industry, wealth, and the citizenry.

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

a. Success will be measured by using metrics from CyberSeek/Burning Glass/DWD. Currently, there are 1,606 Indiana jobs posted requesting six different cybersecurity industry certifications. This initiative is estimated to conservatively provide over 200 certifications over the next 2 years reducing the demand by a minimum of 14% across the State.

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

a. No

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No

Other Implementation Factors

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

a. The ability to secure funding.

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

a. No

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

a. It is anticipated that this initiative will become self-sustaining by the end of the initial 2-year funding period.

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

a. The coalition for this initiative currently includes of 40 formal partners at the local, State, and national levels.

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
    i. All sectors benefit from this initiative.

Communications

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

a. All.

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

a. Yes

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

a. Marketing assets from CLAC partners will be leveraged to ensure the success of the program.

Evaluation Methodology

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

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Program Data Tool

Deliverable: Program Data Tool

General Information

1. **What is the deliverable?**
    a. Develop mechanism to gather data on all cybersecurity programs and offerings across the state and the number of participants. A report on the students that are attending Indiana public, private, and for-profit post-secondary institutions in cybersecurity related fields so that the Indiana Executive Council on Cybersecurity can more fully understand the supply of qualified graduates and their credentials/degrees to make better informed policy decisions. A goal would be to collect Major and Minor-level data.
    b. Use the cyberseek portals to collect and analyze data to iteratively develop IN Cyberpath programing.

2. **What is the status of this deliverable?**
    a. In-progress 25%

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☐ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☒ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☒ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Will provide the state the ability to see all available programs and the number of people that are current in the "pipeline". This information along with the information from the Job Demand Tool proposal will allow stakeholders to understand if the state is producing enough skilled people to meet the anticipated demand.
    b. This tool will be used as:
        i. Portals for primary to secondary teachers, instructors and students with Career Pathways, curricula, project based resources.
        ii. Recourses for teachers related to Professional Development.
        iii. Assessment tools for companies, employees, government for assessing cybersecurity aptitudes and abilities of employees.
        iv. Apprenticeships programs for preparing the cybersecurity workforce.
        v. Identify co-op and internship programs available across the State.

6. **What metric or measurement will be used to define success?**
    a. Ability to accurately measure (e.g. ensure data available from public institutions, 3rd party training providers, and private institutions).
    b. Number of hits on the website portal.
    c. Number of apprenticeship programs stood up.
    d. Number of coop and internship programs.
    e. State science test scores related to cybersecurity/computer science.
    f. Number of companies participating in the programs.

7. **What year will the deliverable be completed?**
    a. 2020

8. **Who or what entities will benefit from the deliverable?**
    a. Having a pipeline report on cybersecurity degrees and certifications that is complete and well-trusted could be a tool of economic development and could make Indiana more attractive to business wanting to locate to the state.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. State and federal programs aimed at developing capacity in cybersecurity and related fields would advocate for this data.
    b. Not sure if other states face similar reporting challenges in the area of majors vs. areas of academic emphasis.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. The workforce group is currently not coordinating with other committees on this deliverable.
    b. IN CyberPath team (Indiana University and Purdue University)

11. Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?

a. CHE
b. DWD
c. Indiana Management Performance Hub (MPH)
d. Purdue University
e. Indiana University

12. Who should be main lead of this deliverable?

a. CHE

13. What are the expected challenges to completing this deliverable?

a. Gathering accurate data (without significant effort) across all of the providers/educators. And being able to do it periodically.
b. We don't want this effort to be a labor-intensive survey each time data is needed. There is an existing process for data gathering from public higher education institutions that can be utilized for that segment of providers.

Implementation Plan

14. Is this a one-time deliverable or one that will require sustainability?

a. Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
CHE Policy & Research Team meet with Institution Research Teams	Michael Hawryluk	50%	April 2018	Meeting is/was scheduled for 4/11/2018.
Develop Initial Survey for Institutions to Report Cybersecurity related students/degrees/programs	CHE	0%	TBD	
Analyze/Synthesize Data from Institutions on Students/Degrees/Programs and Develop Report on Findings	CHE	0%	TBD	
Develop Ongoing Plan for Future Recurring Collection	CHE	0%	TBD	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
0.15		Data Analysis			This effort will be to develop the survey, analyze/synthesize the results and provide a report to the IECC. This can likely be accomplished using existing Exempt FTE/Staff. Depending on the ongoing requirements of collecting this data regularly, this is subject to change.

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

a. This can be accomplished using email and productivity software (e.g. Excel, Word) for the near-term collection. Depending on the ongoing efforts, additional resources or modifications to existing software systems may be required.

b. Software as related to the Cyberseek tool.

Benefits and Risks

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

a. Regularly reported data on supply of cybersecurity-related degree seekers and completers will give the IECC the insight into the supply-side of the equation for post-secondary institutions to understand if policy changes are necessary.

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

a. Our ability to insource cybersecurity expertise will provide less financial risk as we will be better able to recruit graduates from Indiana colleges to work for Indiana companies.

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

a. If we don't know the supply-side of the equation, we may have to outsource cybersecurity jobs/contracts to other states, countries and/or have to pay higher prices/premiums to accomplish necessary work. If we are unable or unwilling to pay for this work, the State of Indiana and its businesses may be subject to additional risk.

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

a. We need to have major-level data on cybersecurity-related degrees. We currently do not have major-level data.
b. Minor-level data would also be helpful to understanding the supply.

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

a. No

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No

Other Implementation Factors

---

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

a. If additional deliverables are placed on staff slated to work on this, it could move the timeline back or risk causing other deliverables to slip in schedule. Having additional resources available would mitigate this, especially for the analysis/report writing part. Potentially, we should have available resources across the entire IECC that can assist in these tasks for various sub-committees and working groups.

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

a. Yes
b. **If Yes, what is the change and what could be the fiscal impact if the change is made?**
    i. We may want to require Institutions to report more granular data than degree-level. This could be codified, but likely will require much deeper conversations than have been had at this point.

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

a. To support this deliverable in the future, CHE will need to modify its CHEDSS system to account for major-level data and Indiana post-secondary institutions will need to modify their processes to report on these data. It's unclear what the exact effort or financial implications of these changes will be.

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

a. At this point, the implementation of this deliverable has been discussed internally at CHE at least through the collection of the data. Staff at CHE has contacted research teams at some Indiana public institutions to determine the feasibility of collecting major-level data and the initial result was positive. Now, we need to develop a survey, send it out, and report on the findings.
b. IN CyberPath

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
    i. If we do expand the collection of this major-level data to non-cybersecurity fields, it could potentially be used by a multitude of additional sectors.

Communications

---

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

a. Indiana post-secondary institutions should be notified regarding the output of the deliverable.

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

a. Yes

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

a. None.

Evaluation Methodology

Objective 1: Indiana Commission for Higher Education will develop and launch survey for post-secondary to report on cybersecurity-related programs by March 2019.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

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

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Supporting Documentation

Supporting Documentation

This section contains all of the associated documents that are referenced in this strategic plan and can be used for reference, clarification, and implementation details.

- National Governor's Association Policy Academy – Indiana 1st Workshop Notes August 2018

National Governor's Association (NGA) Policy Academy

Indiana 1st Workshop Notes

August 2018

August 22: Cybersecurity Workforce Development

Panel 1

Rodney Peterson, NICE

- Need to make sure we are reaching out to all populations: women, minorities, veterans
- There is an online tutorial on how to use the NICE framework
- Main goal is to have a common language that everyone can use
- Can work with Cyberseek to see where the NICE framework aligns to the current job openings
    - Also contains information on how many individuals have specific certifications and how that aligns to specific NICE positions

Stephen Schneiter, COMPTIA

- Need to work with K-12 more so that they understand the certificates that are needed for employment opportunities
- El Paso Texas case study
    - Trained veterans on security certifications
    - All of them who went through the program became employed
- Cannot overlook the end-users. Cybersecurity starts with the end-users
- Really a need for basic awareness/cybersecurity training

Sarah Benczik, Deloitte

- Talent Lifecycle: There is a workforce that is available; then there is an analysis of who we need to bring into the organization and who we currently have in the organization; then organizations start recruiting; once employee is in the organization, there is skill development (skills are only as good as 3-5 years); then you have performance management so that employees understand what is expected of them and what kind of skills they require; and then employees know where to go for the rest of the day. The NICE framework follows this track and allows employees and organizations to easily

Josh Drumwright, Deloitte

- How do we perform work more efficiently
- Started a gig system: identifying tasks that could be outsourced;
- Having a passion for the subject is very important; thinking more broadly on how to bring in the people you need to address those challenges
- How do you revision the work and scope it broader so that you are appealing and finding the best applicant pool

Q&A

- The framework is still a work in process;
- Don't want to have a compliant exercise in which you simply check the box of the qualifications that you need; but how you can use those qualifications to overcome the risks
- The Framework helps to accelerate your workforce; the challenge is that the Framework has a lot of detail

- Encourage using the common vocabulary
- Need to encourage hands on learning/experience based learning
- Worry about the NICE framework becomes a certification/compliance factor. Don't want to say that because we have the NICE framework implemented we are secure

- What are the barriers
    - High school and community colleges are very attuned to getting their students jobs, so the buy-in is very high. But there are universities that are more concerned about life long careers as opposed to just a "job." So the language needs to change to account for that
        - Teach people about how to think intellectually;
    - Need to prepare people how to be lifelong learners because they will need new certifications
    - There are always constant needs or gaps that are changing; need for strong skillset and managers to work with the current workforce on how they can improve, the skills they need to improve, and the organization can help them. Need to ensure that you don't shirk managerial skills
    - Need to get over the feat that training leads to mobility because it will be worse if they stay and don't get trained
- Did you subscribe to a framework to create the NICE Framework?
    - This was a community activity
    - A lot of focus groups and existing materials that we used.
- Have you seen examples of universities using apprenticeships?
    - These are very important for students and workers to accelerate the trainings/knowledge
    - A lot of organizations are sponsoring cyber competitions
    - Crowdsourcing is becoming very popular
    - California: have a lot of businesses working with High school

Facilitation: First Session

Group 1 First Session: Employers

1. What are the tasks that your organization needs to perform its mission?
    a. Educating non-specialists (cyber hygiene)
    b. Supply chain management
    c. Foster research and education in cybersecurity
    d. Hands on experience
    e. Planning for the future
    f. Data identification and classification
    g. Recruitment strategies
    h. Winning leadership buy-in
    i. Building awareness
    j. Creating talent pipeline (including internal skill development)
    k. Career education
    l. Information system acquisition
    m. Evidence-based strategic planning

n. Threat modeling
o. Performance development
p. Organizational change management
q. Security for financial aid distribution (for schools)
r. Hardening of hardware

2. What are employees' knowledge, skills, and abilities (KSA) strengths to perform those tasks?
    a. Hands on experience
    b. Human/behavioral focus
    c. Creative thinking
    d. Cyber intelligence analysis
    e. System perspective
    f. Knowledge of the difference between risk and security
    g. Ability to "think in the grey"
    h. Threat modeling
    i. Data analysis and business context
    j. Knowledge to navigate issues/concerns
    k. Understanding of hardware
    l. Understanding the entire stakeholder ecosystem (outside of organization)
    m. Knowledge of security by design
    n. Mentality for lifelong learning
    o. Soft skills
    p. Data science

Group 2 First Session: Employers

1. What are the tasks that your organization needs to perform its mission?
    a. Defend the network
    b. Knowledge on the need to defend the network
    c. Identify risks and intelligence gathering
    d. There is a need to identify the spectrum of roles needed and which roles and responsibilities can be outsourced
    e. Educational institutions need to identify the skills needed to teach students
    f. Threat assessments
    g. Need a sector driven cybersecurity education development
    h. Need to message why cybersecurity is important
    i. Employees need to report suspicious activities
    j. Auditing vendors
    k. *Unrelated thought: need to make sure the message is being pushed down to locals*
2. What are employees' knowledge, skills, and abilities (KSA) strengths to perform those tasks?
    a. Difficult to assess because there are shifting priorities
    b. Need to react to unplanned circumstances
    c. Meet the need of stakeholders
    d. Ability to pivot
    e. IT personnel are very responsive to customer requests

Our conversation started to discuss overall weaknesses and what organizations would like to see:

- Need to convey that cybersecurity is everyone's problem

- The state should host cyber boot camps for teachers to teach them on Cybersecurity 101 to effectively teach students
- Need to teach about the ethics of cybersecurity. This should be a priority and not an afterthought
- In order to attract more women and girls to cybersecurity, we should message it as a "protector" role
- If we institute the NICE framework and adopt their credentials, we have to make sure we avoid complacency
- Need to emphasize and invest in continuing cybersecurity education and credentialing
- We have to make sure that we convey how these skills are adaptable and transferable
- There is a lack of investment in trainings
- Lack of record/performance management on what credentials/trainings are better than others
- IT needs to be proactive instead of reactive and we need to learn from attacks
- IT responsive
- We need a culture change to highlight that cybersecurity cross-cuts all industries. Just because you get a degree/certificate in cyber, doesn't mean you have to go to an IT industry. You can work for a hospital or nonprofit to practice your education. Likewise, we need to think about how to recruit individual's with non-IT backgrounds into cybersecurity roles because they are just as valuable
- Need to make sure don't rely on traditional IT degree/qualification
- Need to train service desk employees to talk about cybersecurity in layman's terms when talking with customers

Facilitation: Second Session

Group 1 Second Session: Students, Job Seekers, Workers

1. What factors inhibit/deter potential workers?
    a. Pay
    b. No clearance
    c. Remote working offered by companies on the coasts
    d. Company reputation
    e. Lack of awareness of possibilities in cybersecurity community
    f. Chicken and egg problem: companies ask for a lot of experience even for entry level positions
    g. Poor branding for the cybersecurity business
    h. Too much emphasis on 4 year degrees instead of skills
    i. Location, location, location
    j. Fear of math and computer skills
    k. Difficult for hiring managers to sell sensitive duties that they cannot discuss in detail
    l. People misunderstand what cybersecurity jobs entail
2. What encourage students/job seekers/workers to get involved or apply to jobs?
    a. Flexibility
    b. Seeing a career path that is NOT necessarily in management
    c. Pay

   d. Travel
   e. Illustrate the many journeys available
   f. Family
   g. Niche offerings
   h. Employer interest in employees' lives over their work product
   i. Access to resources/training
   j. Making cybersecurity sexy and meaningful
   k. Career development opportunities
   l. Seeing diversity, and people like them, in the industry
3. Why don't young people even consider cybersecurity?
   a. No cybersecurity pop culture for children
   b. We do not condition cybersecurity knowledge at a young age
   c. Lack of general education for consumers
   d. Terms like "security" turn people off early
   e. Cyber still taught as a separate subject—not integrated into normal curriculum
   f. Tangible examples of "cyber heroes" are not part of childhood
   g. No cybersecurity toolkits for teachers of very young students
4. Which promising talent is the community failing to reach?
   a. People who lack digital connectivity
   b. Non-cyber specialists who nevertheless have a role in cybersecurity
   c. Trained employees from the inside who understand the broader business context
   d. Non-cyber workers with an aptitude

Group 2 Second Session: Students, Job Seekers, Workers

1. What factors currently exist that inhibit or deter potential workers from applying to jobs or accepting job offers?
   - Gender bias profile
   - Companies need to articulate that their open job is cyber related. In other words, for those companies that are not traditional IT companies, they need to convey to cybersecurity professionals or students that they can utilize their skills at the company
   - This job is a high risk job with a lot of accountability; so there may be a fear that if a mistake is made, one can be fired very quickly
   - Work/life balance
   - There is a lack of clarity/expectations on what type of education requirements an applicant should have
   - Lack of diverse mentors
   - Need to make apprenticeships more accessible to minority communities and women
   - need to expand applicant pool by thinking about non-IT degrees
   - Currently, there is a belief that if I get this degree or that certificate in cybersecurity then I am restricting myself to a strictly cybersecurity career

2. What factors currently exist that encourage job seekers to apply or accept job offers?
   - Money
   - Altruism
   - Job mobility
   - Not a boring career

3. Other than money, what are "perks" that your organization could offer?
- The sense of mission
- National Guard can provide real world experience
- Placement rate/ability to get a job
- being part of a larger cybersecurity community

4. What are your current outreach efforts? Are there applicant pools you are not reaching? *(this conversation turned into outreach strategies we should consider creating)*
- Need to convey and develop a message on why cyber professionals should work in Indianapolis and that they don't have to move to San Francisco for work. This message could entail the salary purchasing power and cost of living comparisons between Indiana and San Francisco
- Need to increase awareness of associations/clubs/competitions for cybersecurity and their impact
- For K-12: To engage them and to show why cybersecurity would be an interesting career, create examples on the impact a cybersecurity event can have on their life (e.g. would be unable to go online and play videogames, access their favorite apps)
- For K-12, need to be explicit on what exactly cybersecurity is
- Engage teachers to develop cybersecurity curriculum in pre-existing computer science classes
- Need to identify potential federal funding to conduct outreach or to pay for these outreach initiatives
- Do a fieldtrip with teachers/students to the cyber range

Facilitation: Third Session

Group 1 Third Session: Educators/Trainers

1. What are current partnerships between educators and non-educators?
    1. Cyber Corps Scholarship for Service
    2. Retraining veterans with clearances
    3. Cooperative education programs
    4. Michigan's "Marshall Plan"
    5. Workplace Simulation Project
    6. Faculty-Designed Courses for Industry
    7. Employers getting into the classroom any way possible
2. How do current curriculums reflect employer's needs? If not, why not?
    1. By accident
    2. Field experience of the instructor
    3. Industry advisory boards to help design curriculums
    4. Faster approval of courses
    5. Lack of focus on non-cyber skills
    6. Industry does not know what they want
3. For non-educators, what education or training programs do they utilize?
    1. Offer free credentialing
    2. Job shadowing
    3. TIGS
    4. Align with client needs
    5. Train to compliance

6. Training on elements of general career success

4. For educators, do you have sufficient students enrolled in your programs? If not, what needs to be done to increase the student pipeline?
    1. Change the branding
    2. Emphasize problem solving
    3. Use influencers
    4. Tie into core introduction for new students
    5. More access to labs and hands-on equipment
    6. Emphasize the element of cybersecurity in maximizing personal SAFETY and HEALTH
    7. Explain that students really can be cyber warriors
    8. Consolidate all available resources into one place

Group 2 Third Session: Educators/Trainers

5. What are current partnerships between educators and non-educators?
    1. Cyber Start
    2. Cyber Siege
    3. Cyber Patriot
    4. Gen Cyber
    5. START Engineering
    6. NSA-CCEL
    7. NetSmart
    8. National Centers for Forensic Institute
    9. Grid-Ex
    10. Cyber Storm
    11. Need to engage and partner with the fusion center more
    12. Need to have more partnerships between industry and K-12 and to bring volunteers from industry to engage with students
6. How do current curriculums reflect employer's needs? If not, why not?
    1. Teachers and universities need to know what industry is training its employees so they know what to train students on
    2. Need to foster collaboration with other industries (e.g. health) to see if there are best practices within their curriculum that can be applicable to cybersecurity curriculum
    3. A huge weakness is that most curriculum haven't been tested or vetted, so we don't know if what we are teaching is useful/effective
    4. Have to make sure we are including ethics.
7. For non-educators, what education or training programs do they utilize?
    1. We need to make sure that employee trainings lead to credentialing
    2. Need to do a better job highlighting what type of trainings are available for workers
8. For educators, do you have sufficient students enrolled in your programs? If not, what needs to be done to increase the student pipeline?
    1. We have to be cognizant of teachers' capacities and realize that they are being asked to teach several different topics

<u>Facilitation: Fourth Session (Both groups combined)</u>

1. Employers
    a. Rewrite job descriptions according to NICE

   b. Tool for small businesses to design job descriptions
   c. Using NICE Framework to design performance management
   d. Share IBM/Purdue partnership successes
   e. Differentiate NICE Framework from Department of Labor categories
   f. Socialize NICE Framework with HR offices
   g. Develop incentives to encourage adoption of NICE Framework by smaller employers
   h. Use NICE Framework to organize companies/school discussions
2. Educators
   a. Incorporate risk management into curriculums
   b. Creating sector-specific instruction
   c. Expand academic advisory boards
   d. Process for developing aptitude testing
   e. Collect best practices on academic advisory boards
   f. Don't forget the business focus of cybersecurity
   g. Design attacker mindset into curriculums
3. Generate Interest
   a. Get commitment from IN companies for a PR campaign around cyber jobs
   b. Understand why underserved individuals are not engaged
   c. Assistance to offset time & money needed to retrain for cyber
   d. Naviance tool for cyber
   e. Popularize "cyber" heroes
   f. Use games relevant for cyber
   g. Layer degrees with certifications
   h. Roadshows are key—get to those who will not come to large convenings
   i. Get unemployment offices information on available resources
   j. Dual credit program for adults
   k. Create basic guide for those who know NOTHING
   l. Approach K-12 in different components (not as one block, but as low, mid, and high components)
   m. Veterans → trailing spouse (?)
   n. Incorporate cybersecurity into existing degree programs
   o. Align disabilities to NICE roles→involve appropriate advocacy organizations to promote the connections