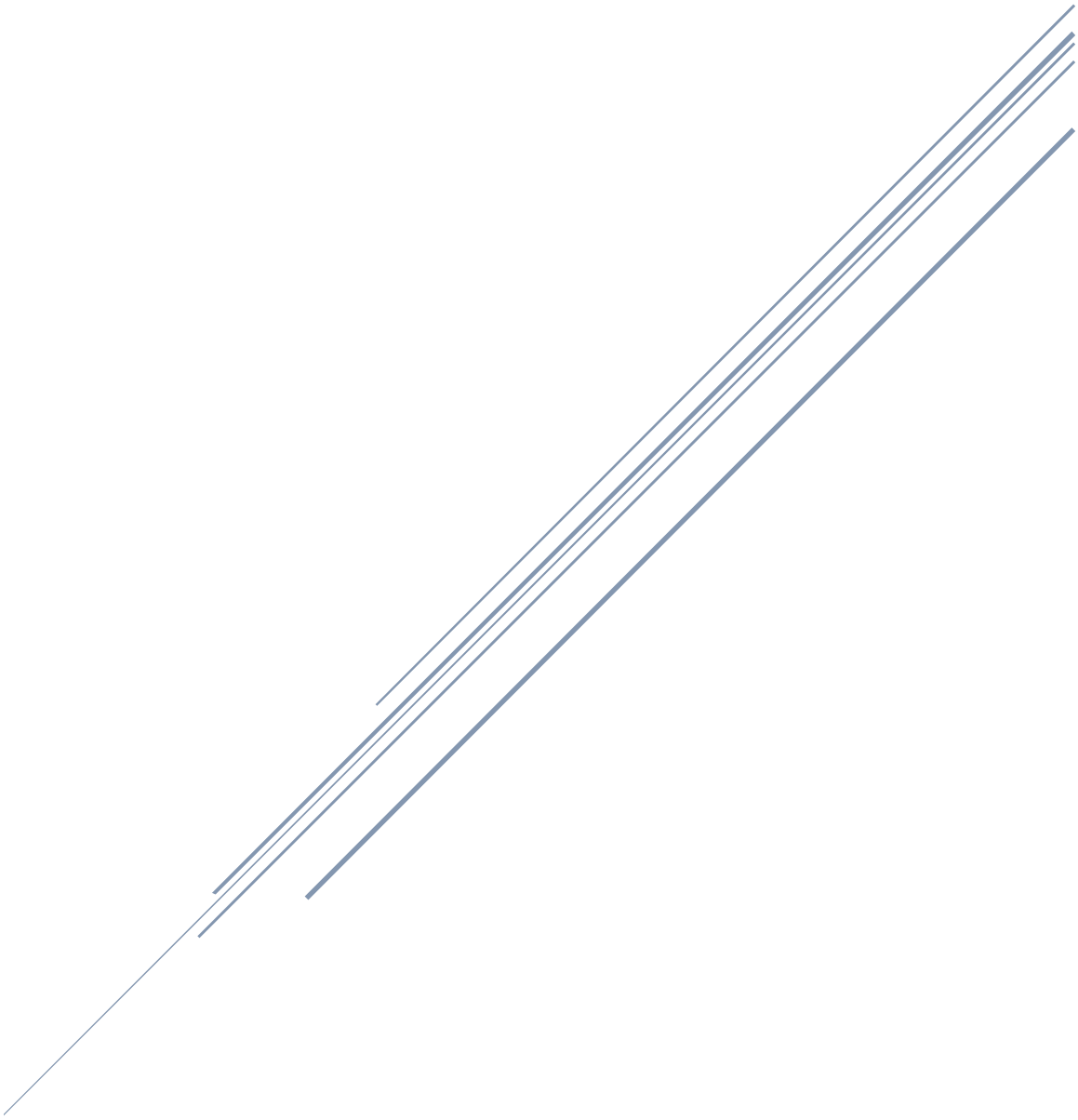
DEFENSE INDUSTRY COMMITTEE STRATEGIC PLAN

Chair: Danielle Chrysler | Co-Chair: Kyle Werner



September 2018
Indiana Executive Council on Cybersecurity

Defense Industry Committee Plan

Contents

Committee Members

Committee Members

Name	Organization	Title	Committee/Workgroup Position	IECC Membership Type
Danielle Chrysler	IODD	Executive Director	Chair	Voting
Kyle Werner	Crane	Strategic Director	Co-Chair	Advisory
Kurt Huff	Raytheon	Director	Full Time	Contributing
Andrew Baker	Rolls Royce	Director	Full Time	Contributing
Sandeep Allam	St. logics	Owner	Full Time	Contributing
Ryan Metzing	Ice Miller (Began work under Aerospace & Defense Council)	Director	Full Time	Advisory
JJ Thompson	Rook Security	Owner	Full Time	Advisory
Tony Vespa	Vespa Group	Owner	Full Time	Advisory
Dave Roberts	IEDC	Director	Full Time	Voting Proxy
General Cliff Tooley	NCCO	Director	Full Time	Advisory
Colonel Pfaff	Indiana Guard	Director	As Needed	Contributing
Dr. Templeman	Crane	Director	As Needed	Contributing

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**
  - The Defense Industry Committee leveraged a recently completed Indiana Office of Defense Development (IODD)/Sagamore Institute study of Indiana's defense market, insights provided by state small and large cybersecurity business leaders, a review of the State's current cybersecurity-related web presence, and defense cybersecurity-related academic programs to establish a baseline for how the defense industry might contribute to the effort to enhance the cybersecurity posture of the State of Indiana and its critical assets.
    - Sagamore / IODD detailed Defense Report (current standings in Defense programs)
    - Other State's Cybersecurity Defense Industry
    - Other State's Current Programs supporting Defense Industry
    - Current Asset Inventories of programs, partnerships and current contract proposals
    - Sensitive Compartmented Information Facility (SCIF) Inventory
    - Current cybersecurity industry numbers

- **Research Findings**
  - Our analysis of the defense cybersecurity industry landscape in Indiana led to three conclusions:
    - The defense cybersecurity industry ecosystem within the state provides the Governor with a potentially potent weapon in his kitbag to promote the State as a leader in cybersecurity locally, regionally and nationally.
    - Indiana's defense industry has a strong desire to support the Governor's effort to enhance the cybersecurity posture of the State and its critical assets.
    - As it is at the national level, the foundation of Indiana's cybersecurity is a strong state economy supported by 21st Century public policy that provides the environment, resources and impetus to reposition Indiana as a thought and action leader in the cybersecurity space nationally and internationally.
  - These conclusions led the committee to establish preliminary declarations of its group ethos and mission that reads as follows:
    - The foundation of Indiana's security is a strong economy. In the 21st Century, that economy is defined by a digital world wherein cyber threats pose a clear and present danger. The first protection principle for Indiana's security is the existence of a robust defense cybersecurity industry whose presence and participation serves as a natural inoculation against threats emerging from the cyber vector.
    - Therefore, the mission of the Defense Committee is to seek, encourage and promote programs and projects that lead to the growth of a vibrant cybersecurity defense industry-related economy within the State of Indiana.

- **Additional Findings**
  - The committee's initial research established the following as preliminary facts related to the State's cybersecurity defense industry:
    - The state's private sector cybersecurity defense industry is limited when compared to other states claiming leadership nationally with only thirteen companies identified as being current players in this market segment. However, those companies are extremely motivated to play a larger role at the state, regional and national levels, but require the support of the state in doing so.
    - The state's federal sector cybersecurity footprint represents great potential for leveraging via public-private partnerships in advancing Indiana's interests with the inventory including Naval Surface Warfare Center Crane, the Indiana National Guard's Muscatatuck training and testing facility, the Indiana National Guard's Stout Field Special Compartmented Information Facility (SCIF) and cybersecurity support team, and Grissom Air Reserve Base's cyber team.
    - Under the leadership of the Lieutenant Governor, the state has taken the initial first steps towards repositioning Indiana in the defense cybersecurity market through the commissioning of a statewide defense industry study directed towards framing a way ahead for the state in establishing itself as a thought and action leader in this market and has initiated the implementation of that study's principle recommendations which include:
      - The establishment of a statewide defense market development and capture system.
      - The establishment of a statewide strategy for repositioning Indiana as a defense market thought and action leader.
      - The establishment and operation of a public-private partnership digital and physical defense industry ecosystem with the cybersecurity market being its first major vector.

- **Committee Deliverables**
  - Cyber Market System
  - Cyber Digital Platform
  - Cyber Statewide Testbed

- **Additional Notes / Way Ahead:**
  - The Defense Industry Committee has identified the following two tasks as being those that frame the way ahead:
    - Working closely with the Lieutenant Governor in integrating its efforts with those directed towards the larger state-level defense market development and capture system.
    - Identifying and advocating public-private partnership opportunities to advance the development and growth of the defense cybersecurity market within the State.

- **References**

  - Accenture, *Integrated Digital Platforms: Flexible Technology to Meet the Consumer* Challenge, (Accenture Interactive: 2012)
  - AcqNotes, *Acquisition Process*, http://acqnotes.com/acqnote/acquisitions/acquisitionprocess-overview

- AcqNotes, *Acquisition Category (ACAT),* http://acqnotes.com/acqnote/acquisitions/acquisition-category
- Aerospace Industries Association, *The Strength to Lift America: The State of the U.S. Aerospace and Defense Industry*, (AIA: 2016)
- American Legislative Exchange Council, *Rich States, Poor States – ALEC-Laffer State Economic Competitiveness Index*, (ALEC: 2017)
- APMP Center for Business Development Excellence, *Capability Maturity Model for Business Development, Version 2.0* (APMP: 2014)
- Arellano, Robert, *Analysis of Rapid Acquisition Processes to Fulfill Future Urgent Needs*, (Naval Postgraduate School: 2015)
- BD-CMM Development Team and Steering Committee, *Capability Maturity Model for Business Development, Version 1.0*, (Business Development Institute: 2007)
- Center for Strategic and International Studies, *Defense Acquisition Trends, 2016 – The End of the Contracting Drawdown*, (CSIS: 2017)
- Centers for Disease Control and Prevention, *Contracting Process*, https://www.cdc.gov/contracts/process/index.html
- Congressional Research Service, *Defense Primer: The National Defense Budget Function (050)*, (CRS: 2017)
- CNBC, *America's Top States for Business 2017*, https://www.cnbc.com/2017/07/11/americas-top-states-for-business-2017-overallranking.html
- DB4 Consulting, *Capture Management: Art, Science or Sorcery?* (Loudon County Chamber of Commerce GovCon Initiative Training Session: 2015)
- Defense Acquisition University, *Defense Acquisition Guidebook*, https://www.dau.mil/tools/dag
- Defense Science Board, *Fulfillment of Urgent Operational Needs*, (USD AT&L: 2009) Defense Systems Management College, *DoD Funds Management Platinum Card*, (Defense Acquisition University, Fort Belvoir, VA: 2016).
- Deloitte, *2017 Global Aerospace and Defense Sector Outlook – Growth Prospects Remain Upbeat*, (Deloitte: 2017)
- Deputy Assistant Secretary of Defense, Emerging Capability and Prototyping (EC&P), *Prototyping and Experimentation: Accelerating the Adoption of Transformative Capabilities*, (DASD EC&P: 2016)
- DeVol, Ross, Joe Lee and Minoli Ratnatunga, *2016 State Technology and Science Index*, (Milken Institute: 2016) 37
- Douglas, Brad, *Welcome to the New Normal: Winning Business in Today's Market Place*, (Deltek Insight 2015: 2015)
- Etherton, Jon, *Acquisition Policy: Current Acquisition Environment*, (NDIA: 2017)
- Evans, Peter, Annabelle Gawer, *The Rise of the Platform Enterprise: A Global Survey*, (The Center for Global Enterprise: 2016)
- Federal Procurement Data System-Next Generation, *Top 100 Contractors Report Fiscal Year 2016*, (GSA, https://www.fpds.gov/fpdsng_cms/index.php/en/reports/62-top-100-contractors-report)
- Gates, Doug, Tom Mayor, Erich Gampenrieder, *Global Aerospace and Defense Outlook: The Dawn of a New Day*, (KPMG: 2016)
- Goodly, Bernard, *Managing the Army's Research and Development Investments in a Time of Declining Resources*, (Defense Acquisition University: 2016)
- Governing for States and Localities, *Military Active-Duty Personnel, Civilians by State*, http://www.governing.com/gov-data/military-civilian-active-duty-employee-workforcenumbers-by-state.html

- Government Accountability Office, *Contracting Data Analysis – Assessment of Government-wide Trends*, (GAO: 2017)
- Government Accountability Office, *Defense Science and Technology- Adopting Best Practices Can Improve Innovation Investments and Management*, (GAO: 2017)
- Government Accountability Office, *DoD Rapid Innovation Program – Some Technologies Have Transitioned to Military Users, but Steps Can Be Taken to Improve Program Metrics and Outcomes*, (GAO: 2016)
- GovernmentContractsWon.com, *Indiana Defense Contractor Lists by City*, https://www.governmentcontractswon.com/department/defense/indiana_cities.asp
- GovWin, *Top 20 Unrestricted Federal Business Opportunities for FY2018*, (Deltek Federal Information Solutions: 2017)
- Hahn, Heather, Maeve Gearing, Michael Katz, Ria Amin, *Observations of Leaders Driving Changes in State Government*, (Urban Institute: 2015)
- Indiana University *I-Light Network Map*, http://ilight.net/map
- Industrial Research Institute, *2017 Global R&D Funding Forecast*, (R&D Magazine: 2017)
- LeHong, Hung, Chris Howard, Dennis Gaughan, Debra Logan, *Building a Digital Business Technology Platform*, (Gartner: 2016)
- Levinson, Robert, Sopen Shah, Paige Connor, *Impact of Defense Spending: A State-by-State Analysis*, (Bloomberg Government: 2011)
- Linsscott, Warren, *2015 Deltek Clarity GovCon Industry Study Results*, (Deltek: 2015)
- Martin, Greg, *Lunch & Learn: Congressional Enactment*, (DAU: 2017)
- Milken Institute, *2016 State Technology and Science Index – Sustaining America's Innovation Economy*, (Milken Institute: 2016)
- Morgan, Steve. Cybersecurity Market Report, Q1 2017. http://cybersecurityventures.com/cybersecurity-market-report/
- Morgan, Steve. Cybersecurity Market Report, Q1 2017. http://cybersecurityventures.com/cybersecurity-market-report/
- Newman, Larry, *Shipley Proposal Guide for Business Development and Sales Professionals*, (Shipley Associates: 2009)
- Office of the Assistant Secretary of Defense for Research and Engineering, *DoD Laboratories and Centers*, https://www.acq.osd.mil/rd/laboratories/
- Office of the Secretary of Defense (Acquisition, Technology and Logistics), *Department of Defense Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) List*, (DoD: 2016) http://www.acq.osd.mil/ara/documents/mdap_mais_program_list_dated_01Nov16.pdf
- Office of the Secretary of Defense Test Resource Management Center, Test & Evaluation/Science & Technology Opportunities, June 8, 2015, http://slideplayer.com/slide/6052297/
- Office of the Undersecretary of Defense (Comptroller)/Chief Financial Officer, *Program Acquisition Cost by Weapon System United States Department of Defense*, (DoD: 2017)
- PricewaterhouseCoopers, *Aerospace and Defense 2016 in Review and 2017 Forecast*, (PwC: 2017)
- PricewaterhouseCoopers, *Aerospace Manufacturing Attractiveness Rankings*, (PwC: 2017)
- Project Management Institute, *PMBOK Guide, 6th Edition*, (Project Management Institute: 2017)
- Purdy, Ellen and Ted Bujewski, *Rapid Innovation Fund (RIF) 101*, (OSD Research and Engineering: 2017)

- Ross, Alec, “Want Job Security? Try online security”. Wired, April 25, 2016
- Salesforce, *Federal Government Contractor Study 2016*, (Market Connections: 2016)
- Salesforce, *Government Contractor Best Practices*, (Market Connections, 2016).
- Sego, Patricia, *Capture Management*, (Glendale Technical Sales Consulting, Inc.: 2012)
- Shipley and Associates, *Business Development Lifecycle*, http://sbdl.shipleywins.com
- Shipley and Associates, *Business Development Lifecycle*, http://advancedpm.es/wpcontent/uploads/2015/04/Shipley-Business-Development-Process.jpg
- U.S. Department of Defense, *Department of Defense Directive 5000.01 Operation of the Defense Acquisition System*, (DoD: 2017)
- U.S. Department of Defense, *Department of Defense Instruction 5000.74, Defense Acquisition of Services*, (DoD: 2017)
- U.S. Department of Defense, *Manual for the Operation of the Joint Capabilities Integration and Development System (JCIDS)*, (DoD: 2015)
- U.S. Department of Defense, *Performance of the Defense Acquisition System – 2016 Annual Report*, (DoD: 2016)
- U.S. Department of Defense, *Rapid Innovation Fund (RIF) Program: Use of Technology Transition Best Practices*, (DoD: 2016)
- U.S. Department of Defense, *Report to Congress- Restructuring the Department of Defense Acquisition, Technology and Logistics Organization and Chief Management Officer Organization*, (DoD: 2017)
- U.S. Department of Defense Office of Economic Adjustment, *Defense Spending by State Fiscal Year 2014*, (DoD OEA: 2016)
- U.S. Department of Defense Office of Economic Adjustment, *Defense Spending by State Fiscal Year 2015*, (DoD OEA: 2017)
- U.S. Department of Defense Office of Small Business Programs, *2017 Small Business Training Week – Rapid Innovation Fund*, (DoD OSBP: 2017)
- U.S. Department of Defense Rapid Reaction Technology Office, *Rapid Reaction Technology Office Overview*, (DoD RRTO: 2016)
- U.S. Department of Defense, *2016 Report to Congress: Sustainable Ranges*, (USD P&R: 2016)
- USASpending.gov, *Indiana Spending Map*, https://www.usaspending.gov/transparency/Pages/SpendingMap.aspx?statecode=IN
- Warley, David, *The Project Manager’s Survival Guide to Bids, Tenders and Proposals*, (Association for Project Management: 2016)
- Whaley, Eileen and Dana Stewart, *Path from Urgent Operational Need to Program of Record*, (Defense Acquisition University Alumni Association: 2014)
- Wyatt, Earl, *Rapid Fielding: A Path for Emerging Concept and Capability Prototyping*, (DASD RF: 2013)

Research

Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
    a. Continued Defense Federal Acquisition Regulation (DFARS) training / software
    b. User training / programs to catch vulnerabilities

2. **What (or who) are the most significant cyber vulnerabilities in your area?**
    a. The everyday user
    b. Information Sharing Channels

3. **What is your area's greatest cybersecurity need and/or gap?**
    a. Studies have indicated that 60% of small business fail within 6 months of a significant cyber incident such as a breach or ransomware – Need affordable solutions to comply with current regulations and solution sets for the above statistics
    b. Technology Expertise
    c. Education and Training

4. **What federal, state, or local cyber regulations is your area beholden to currently?**
    a. DFARS compliance
    b. European Union's General Data Protection Regulation (GDPR)
    c. National Institute of Standards and Technology (NIST)

5. **What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?**
    a. Kentucky completed a full evaluation of Cyber in the State through Defense Office of Economic Adjustment (OEA) grant
    b. Cyber document – Indiana Economic Development Corporation (IEDC) 2017
    c. State of Illinois Cybersecurity Strategy

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. Defense Industry State Document – Sagamore Institute Produced
    b. Other State Research

7. **What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?**
    a. Private, Public, Partnership Investment in cybersecurity
    b. Innovation / Entrepreneur programs (California model)
    c. Defining the lane they want to dominate (Marketing plan and strategic plan attached)
    d. MiC3: Serving Michigan. The Michigan Cyber Civilian Corps (MiC3) is a group of trained cybersecurity experts who volunteer to provide expert assistance to enhance the State's ability to rapidly resolve cyber incidents when activated under a Governor declared State of Emergency. The group includes volunteers from government, education, and business sectors.

8. **What does success look like for your area in one year, three years, and five years?**
    a. Cyber Defense Capture Market system by 2019
    b. Working Digital platform by 2019
    c. Industry Lead Cyber Conference 2019

d. Defense Industry Legislative Recommendations Summer 2019
e. 2% Market Share gain by 2022

9. What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?

a. Need to define exactly what you want to be in cyber, can't be the expert of all.

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. Indiana Based Cyber Focus companies
    i. Cimtrak (software)
    ii. Pondurance (services)
    iii. Rook Security (software and services)
    iv. RADcube (consulting and implementation)
    v. Gravicom, LLC
b. Cyber Focused companies with office in Indiana
    i. Optiv (reseller and services)
    ii. Proofpoint (software)
    iii. Mako Group
    iv. Rofori
c. Companies that do cyber but not as primary focus:
    i. EY
    ii. PwC
    iii. KSM
    iv. Crowe
    v. Raytheon
    vi. Vespa Group
d. Major Primes – All will have cyber experts inside protecting assets
e. Cybersecurity workforce – Needs to be defined and studied at a higher level

11. What do we need to do to attract cyber companies to Indiana?

a. Develop a market capture system that can truly identify opportunity in this sector
b. Land a large program of record / Department of Defense (DOD) Contract with cyber component (US Govt 19B in 2017)
c. Define focus in cyber
d. Invest money into the current assets (Georgia, Michigan, Rhode Island model)
e. Full inventory of all current assets (Kentucky model with OEA grant)
f. Consider models of Maryland's Cybersecurity Investment Incentive Tax Credit
g. Host conference or workshop on cyber insurance, funding risk assessments for critical infrastructure assets, piloting new technologies for critical infrastructure protection; and investing in processes to help critical infrastructure operators mitigate cyber risk. (already been offered by STLogics company in Indiana to host)

12. What are your communication protocols in a cyber emergency?

a. Internal Company protocols – Individually defined by each company

13. What best practices should be used across the sectors in Indiana? Please collect and document.

a. Partner with Industry. State governments can leverage partnerships with the private sector by utilizing industry expertise through the acquisition of products and services with high levels of security and reasonable terms and conditions.

b. Adopt Industry-Recognized Security Standards. State governments should adopt international standards recognized by industry to better align security across all agencies and departments.
c. Standardize Cloud Security. If state governments plan on standardizing their approach to cloud security, they should leverage existing federal certification programs at the state level.
d. Establish an Outcome Focused Governance Structure. A state's governance structure should cover all aspects of the enterprise and encourage cross-organizational collaboration and transparency.
e. Actively Share Information. There are a wide variety of different models for the sharing of cyber threat information, and integration centers have emerged in recent years to provide a vital link between all levels of government, the private sector, and academia.
f. Create a Culture of Awareness. State governments should invest in training and education for their workforces to enhance overall cybersecurity awareness

Deliverable: Cyber Market Systems

Deliverable: Cyber Market System

General Information

1. **What is the deliverable?**
    a. Indiana defense industry cybersecurity market pursuit collaboration plan and system.
    b. Define programs that are worthy of a collective Statewide program and complete asset mapping for what capabilities we have in the State.

2. **What is the status of this deliverable?**
    a. In-progress 80%

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. Reposition Indiana as a thought and action leader nationally and internationally in the defense cybersecurity market space. This platform will enable us to pull statewide and regional resources to compete in the national cyber market.

6. **What metric or measurement will be used to define success?**
    a. Two percent, about $300 million of DOD cybersecurity market share, around $15 billion plus, by Fiscal Year (FY) 2022 as identified in contracts and grants awarded captured in usaspending.gov

7. **What year will the deliverable be completed?**
    a. 2018
    b. Formalized Group 2018 – Defense Industry Cyber Committee
    c. Fully operationalized 2020

8. **Who or what entities will benefit from the deliverable?**
    a. Indiana entrepreneurs, businesses, colleges, universities and agencies involved in the defense cybersecurity market space

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. State and federal defense cybersecurity-related programs.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Economic Development
    b. Policy

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. Indiana Economic Development Corporation, Crane, Indiana National Guard, National Center for Complex Operations, Inc., Sagamore Institute, Prime / Mid / Small Cybersecurity Industry, Indiana Office of Technology & Other State Resources.

12. **Who should be main lead of this deliverable?**
    a. Indiana Office of Defense Development (Danielle Chrysler) & Indiana Economic Development Corporation (Dave Roberts)

13. **What are the expected challenges to completing this deliverable?**
    a. None at this time

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
Build Cyber Defense Team	IODD / IEDC	100%	January 1, 2018	Defense Industry Cyber Group will be Cyber lead for State Defense Effort with IEDC
Asset Mapping	IODD / IEDC	50%	January 1, 2019	Digital Platform will help us complete this process
Research National Cyber Opportunities	Defense Industry Committee / IEDC	50%	Ongoing	Working on group proposals for current opportunities
National & International Cybersecurity Market Development & Capture Support	IODD/IEDC/ NCCO	20%	Ongoing	Viable pursuit of opportunities requires sustained development & capture support.

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No
   i. We will use current staff of IOT, IEDC, IODD and other entities to complete this process.

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

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
N/A					

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
Digital Platform - Pilot	Establishes Base Line Cybersecurity Market Development & Capture Capability	$800K	N/A	OEA Grant	N/A	
Digital Platform – Phase 2	Digital Platform Marketing Capability	$10K	$10K / month	State	N/A	
Defense Cybersecurity Market Development & Capture Support	Viable market development & capture system requires persistent research & market analysis	$35K	$35K / month	State	N/A	

Benefits and Risks

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

a. Provides state with capability to develop and capture national and international cybersecurity market share.

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

a. Indiana collectively has the resources to lead the national security dialogue in the cybersecurity space. No estimated cost at this time.

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

a. Indiana currently has lost 60% of the market share in the DOD contracting space and the risk is to continue this losing trend when we have all the resources / companies to do business in the cybersecurity and DOD space.

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

a. Two percent increase in the Defense Market by 2022 / National recognition of Cyber capabilities in Indiana.

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. State of Georgia – $40M to new cybersecurity building / assets – leaning in on future cyber solutions.

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

Other Implementation Factors

23. **List factors that may negatively impact the resources, timeline, or budget of this deliverable?**
    a. None

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. See chart under question number 16.
26. **Who has the committee/working group contacted regarding implementing this deliverable?**
    a. Sagamore Institute – Outside think tank
27. **Can this deliverable be used by other sectors?**
    a. Yes
    b. **If Yes, please list sectors**
        i. Cybersecurity marketing can be leveraged for adjacent markets and opportunities.

Communications

28. **Once completed, which stakeholders need to be informed about the deliverable?**
    a. Indiana Office of Defense Development – Danielle Chrysler; Indiana Office of Economic Development (Defense Sector) – Danielle Chrysler (Innovation) – Dave Roberts

29. **Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?**
    a. Yes, but will require more discussion

30. **What are other public relations and/or marketing considerations to be noted?**
    a. None

Evaluation Methodology

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

Deliverable: Cyber Digital Platform

General Information

1. **What is the deliverable?**
    a. Indiana defense cybersecurity market development and capture plan and system (Digital Platform)

2. **What is the status of this deliverable?**
    a. Phase 1 - Pilot Phase 100% 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. Reposition Indiana as a thought and action leader nationally and internationally in the defense cybersecurity market space. This platform will enable us to pull statewide and regional resources to compete in the national cyber market.

i. This platform will allow Indiana business and academia to qualify and register as defense contractors. Once qualified and registered, the software platform will facilitate a streamlined and automated proposal and contract process, matching Government acquisition opportunities (e.g., Request for Information (RFI), Request for Proposal (RFP), Small Business Innovative Research and Small Business Technology Transfer (SBIR/STTR), and grants) to Indiana defense contractors.
ii. This platform will also allow Government and business users to perform Market Research, collect defense contract-related metrics, serve as a historical document, and "lessons-learned" repository and to allow post-contract award debriefs.

6. **What metric or measurement will be used to define success?**
    a. Two percent, about $300 million of DOD cybersecurity market share, around $15 billion plus, by Fiscal Year (FY) 2022 as identified in contracts and grants awarded captured in usaspending.gov.
    b. Percentage increase in defense spending executed through the digital platform.

7. What year will the deliverable be completed?
    a. 2018
    b. Pilot July 1, 2018
    c. Fully operationalized if funded by 2020

8. **Who or what entities will benefit from the deliverable?**
    a. Indiana entrepreneurs, businesses, colleges, universities and agencies involved in the defense cybersecurity market space.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. State and federal defense cybersecurity-related programs.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Economic Development
    b. Policy

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. Indiana Economic Development Corporation, Crane, Indiana National Guard, National Center for Complex Operations, Inc., Sagamore Institute, Prime / Mid / Small Cybersecurity Industry, PTAC, Westgate/ARI, Indiana Universities, Atterbury-Muscatatuck.

12. Who should be main lead of this deliverable?

a. Indiana Office of Defense Development through the Office of Economic Adjustment Grant

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

a. State budget programmed funding for maintenance / upkeep of the platform

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
Minimum Viable Product Phase 1	NCCO	100%	Jul 31, 2018	This is a pilot.
Marketing Plan	NCCO	0%	Aug 31, 2018	Unfunded
Training	NCCO	0%	Sep 31, 2018	Unfunded
Support	NCCO	0%	Jul 31, 2018	Unfunded
Scalable KCC Platform Phase 2	NCCO	0%	TBD	Unfunded

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
2 hours / week	1 hour / week	Product Sponsor (Business)	Office of Economic Adjustment (OEA) Grant	x	Product Owner-Decision Maker for product
2 hours / week	1 hour / week	Product Owner (Business)	OEA grant	x	Product Owner-Decision Maker for product
2 hours / week	1 hour / week	Product Technical Subject Matter Expert (Business)	OEA grant	x	Need at least one representative able to serve as a technical representative
2 hours / week	1 hour / week	Product Process Subject Matter Expert (Business)	OEA grant	x	Need one representative for each process owner if process has multiple owners

25 hours / week	25 hours / week	Product Build – Account Manager	OEA grant	x	
80 hours / week	80 hours / week	Business Analyst (Project Lead)	OEA grant	x	
40 hours / week	40 hours / week	Project Manager	OEA grant	x	
80 hours / week	80 hours / week	Front-End Developers	OEA grant	x	Need two or more
40 hours / week	40 hours / week	Lead System Architect	OEA grant	x	
80 hours / week	80 hours / week	Back-End Developers	OEA grant	x	Need two or more
0 hours / week	80 hours / week	Support Personnel (Business)	OEA grant	x	
0 hours / week	80 hours / week	Support Personnel (Technical)	OEA grant	x	
30 hours / week	30 hours / week	Training Personnel (Business)	OEA grant	x	Need three trainers
30 hours / week	30 hours / week	Training Personnel (Business)	OEA grant	x	Need three trainers

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**
Subscription Access to External and Government Databases	Data from External and Government Databases are required in order to supply the new product with needed information assets	$5,000	$500/month	OEA grant	x	Access to all databases
Cloud Infrastructure	This is required to host the application. Web Servers and Database Servers will be required.	$200,000	$15,000/month			

Benefits and Risks

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

a. To increase the share of defense contracts in Indiana and ensuring that all the work is performed by companies, organizations and research institutions based in Indiana – analytics attached to the digital platform.
b. The major focus and benefit is job creation, more economic and business growth opportunities in Indiana and beyond.

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

a. Cybersecurity is the primary service category that the platform will capture and would enable organizations, academia and research institutions to provide risk reduction at the overall State level by developing capabilities and attracting and retaining talent.
b. Minimum viable product (MVP) cost is around $500 thousand and while the final costs are still being finalized it is generally in the range of 6-10 times the cost of MVP.

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

a. Continue losing market share in the overall defense expenditure in State of Indiana.
b. Continue losing market share in the overall cybersecurity-related defense projects expenditure.
c. The limited capability of the tool will limit the amount of potential jobs created; as well as a limiting the contribution to economic prosperity and business potential in the State of Indiana.

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

a. Increased dollars from DoD funded contracts awarded to Indiana vendors.
b. Number of cybersecurity and defense contracts executed through the platform in automated fashion and in alignment with Defense Federal Acquisition Regulation (DFAR).
c. Increased number of Indiana jobs created by DoD funded contracts.
d. Baselines to be provided by DoD.

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
b. **If Yes, please list states/jurisdictions**
    i. N/A
    ii. From what we understand, the product being generated is the first of its kind for states / jurisdictions. The product will only generate more jobs, economic prosperity and business potential regardless of the current economic status of a given state/jurisdiction.

Other Implementation Factors

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

a. Availability and accessibility of key stakeholders / resources for critical information and support.

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. Strategic Guidance
b. Financial Support
c. Business Support
d. Technical Support

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

a. National Center for Complex Operations (NCCO)

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
    i. Deliverable has unlimited use potential and can be used by any other federal agency

Communications

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

a. Potential companies and users of the system.
b. IEDC, Indiana Procurement Technical Assistance Center (PTAC)
c. Academia and Research Institutions
d. NCCO and IODD internal users
e. Investors, Entrepreneurs, Donors

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

a. Yes
    i. A safe, secure platform for connecting, vetting, and qualifying local vendors, national vendors, and government agencies.

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

a. The site will be available via the web to the public and will be advertised on other websites / social media channels.

Evaluation Methodology

Objective 1: Indiana Office of Defense Development and partners will develop a pilot of the Indiana defense cybersecurity market development and capture plan and system (Digital Platform) by August 2018.

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 increases to two percent (about $300M) of the Department of Defense (DOD) cybersecurity market share ($15B plus) by FY 2022.
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: Cyber Statewide Testbed

Deliverable: Cyber Statewide Testbed

General Information

1. **What is the deliverable?**
    a. Indiana defense cybersecurity product test, training and demonstration plan and capability. (Cyber Statewide Testbed)

2. What is the status of this deliverable?
    a. In-progress 50%

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. Reposition Indiana as a thought and action leader nationally and internationally in the defense cybersecurity market space. This testbed will allow for companies, universities, local entities and military assets to test, train and demonstrate cyber capabilities.

6. **What metric or measurement will be used to define success?**
    a. Two percent, about $300 million of DOD cybersecurity market share, around $15 billion plus, by Fiscal Year (FY) 2022 as identified in contracts and grants awarded captured in usaspending.gov.

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

8. **Who or what entities will benefit from the deliverable?**
    a. Indiana entrepreneurs, businesses, colleges, universities and agencies involved in the defense cybersecurity market space.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. State and federal defense cybersecurity related programs.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Economic Development
    b. Policy

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. Indiana Economic Development Corporation, Crane, Indiana National Guard, National Center for Complex Operations, Inc., Sagamore Institute, Prime / Mid / Small Cybersecurity Industry.

12. **Who should be main lead of this deliverable?**
    a. Indiana Office of Defense Development & Indiana Economic Development Corporation with technical expertise of Primes, Crane and Indiana National Guard assets and Indiana Office of Technology

13. **What are the expected challenges to completing this deliverable?**
    a. State budget programmed funding – (Georgia has put $40M towards Cybersecurity)

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
Multi-Threat Energy Grid (M-TEG)	IEDC/NCCO	10%	January 2020	
Muscatatuck Cybertropolis (MUTC-C)	Indiana Guard	10%	January 2020	
Indiana Cyber Ecosystem (ICE)	IEDC/NCCO	0%	January 2020	

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
5	5	Project Management	DOE Grant	X	

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
M-TEG Design/Construct	Self-Explanatory	$22M	$1M / year	DOE Grant	X	
M-TEG Technical Project Lead & Analysis	Self-Explanatory	$1.2M	$1.2M / year	DOE Grant	X	
M-TEG Construction Project Manager & Required Studies	Self-Explanatory	$2.2M	$200K / year	DOE Grant	X	
M-TEG Program Management & Business Operations	Self-Explanatory	$1M	$1M / year	DOE Grant	X	
M-TEG Contingency	Self-Explanatory	$3.2M	N/A	DOE Grant	X	
M-TEG Phase II	Self-Explanatory	$20M	$20M	Private/State (80%/20%)	X	
M-TEG Phase III	Self-Explanatory	$20M	$20M	Private/State (80%/20%)	X	
Cybertropolis Project Management & Required Studies	Self-Explanatory	$1.5M	$1.5M	State	X	
Cybertropolis Design/Construct	Self-Explanatory	$10M	$10M	Private/State (80%/20%)	X	
Indiana Cyber Ecosystem	Self-Explanatory	$2M	$2M	State	X	

Benefits and Risks

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

a. This deliverable establishes Indiana as a thought and action leader in the national and international cybersecurity market.

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

a. This deliverable provides to the state, nation and world a capability to rapidly identify and respond to cyber threats against critical infrastructure.

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

a. Indiana surrenders cybersecurity market dominance to other states.

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

a. Success equals capture of five percent of international cybersecurity market share by end of calendar year 2023.

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 do 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. Award of DoE M-TEG Phase I grant.

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. This deliverable will be self-sustaining through public-private business model no later than (NLT) end of calendar year 2022.

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

a. IODD, NCCO, IEDC, state and national stakeholders.

27. Can this deliverable be used by other sectors?

a. Yes.
b. **If Yes, please list sectors**
    i. Any sector involved in critical infrastructure and product protection training or testing will benefit from this deliverable.

Communications

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

a. Indiana Office of Defense Development and Indiana Economic Development Corporation.

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 deliverable will have an embedded public relations and marketing component.

Evaluation Methodology

Objective 1: Establish a nationally recognized cybersecurity test bed in Indiana by January 2020.

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 captures five percent of international cybersecurity market share of cybersecurity test, training, and demonstration plan and capability by December 2023.

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

No Supporting Documentation Provided At This Time