GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

COMMITTEE AND WORKING GROUP QUESTIONNAIRE – RESEARCH PHASE 1

Instructions: As your committee or working group is in the Research Phase, it is important we work with other committees and working groups to get the information your team will need to be successful. Please answer the questions the best you can.

Provide your questions and answers to MosleyCLM@iot.in.gov.

Committee/Working Group Completing Questions: _____

Person Submitting Answers: _____

Email of Person Submitting: _____

Date Submitted: _____

1. What has your area done in the last five years to educate, train, and prepare for cybersecurity?
2. What (or who) are the most significant cyber vulnerabilities in your area?
3. What is your area's greatest cybersecurity need and/or gap?
4. What federal, state, or local cyber regulations is your area beholden to currently?
5. What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?
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.
7. What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?
8. What does success look like for your area in one year, three years, and five years?
9. What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?
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?
11. What do we need to do to attract cyber companies to Indiana?
12. What are your communication protocols in a cyber emergency?
13. What best practices should be used across the sectors in Indiana? Please collect and document.

GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

COMMITTEE AND WORKING GROUP: RESEARCH EXECUTIVE SUMMARY TEMPLATE
PHASE 1

Committee/Working Group: _____

Person Submitting Summary: _____

Email of Person Submitting: _____

Date Submitted: _____

Executive Summary

- **Research Conducted**

- **Research Findings**

- **Preliminary Deliverables**

- **Additional Notes**

- **References**

GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

COMMITTEE AND WORKING GROUP QUESTIONNAIRE – PLANNING PHASE 2

Instructions: As your committee or working group is in the Planning Phase, it is important we work with other committees and working groups to get the information your team will need to be successful. Below are all the committees and working groups' questions submitted by other teams. Please answer the questions the best you can. If it does not apply to your group, write in N/A. If the answer to a question is confidential/sensitive, please write the reason as to why it cannot be shared in this questionnaire. Do not leave questions with no answer.

Provide your questions and answers to MosleyCLM@iot.in.gov.

Committee/Working Group Completing Questions: _____

Person Submitting Answers: _____

Email of Person Submitting: _____

Date Submitted: _____

Government Service Committee

- Do you know of other state level cyber plans?
- How do state entities interface with existing national groups? The energy industry currently works with two national cyber coordinating councils (one for electric industry and one of the natural gas industry.) These groups include U.S. Department of Homeland Security personnel.
- What federal agencies have cybersecurity services/functions? What services do they provide?
- What communications following an incident would you like from energy utilities?
- How will state and federal agencies allocate scarce resources in an emergency? For example, fuel to allow back-up generators to operate.
- What do you expect to receive from the Committee/Working Groups?
- Which Committee/Working Groups do you expect to be most involved with during the implantation of your deliverables?
- What does your team expect from the (critical infrastructure) CI sectors during incident response?
- How does your sector currently coordinate and collaborate with each CI sector?
- Which electric or natural gas energy services does your sector utilize?
- Does your sector provide its own energy (e.g., solar, microgrid, hydro, etc.)

- Do you know of or participate in joint sector cyber exercises?
- How can we best institute joint-purchasing or sharing of government resources to protect infrastructure?
- How can local governments access the necessary infrastructure (i.e. to fiber optics) that are needed to provide adequate back-up systems and necessary redundancies?
- How can government use volunteers who are experts in the field versus paying for a vendor that provides the same service?
- What does Government Services uses for 3rd Party vendor assessment questions?
- What does Government Services follow Security Framework?
- Is there a Knowledge center to share information without recourse?
- Who/what are your audiences that need to be reached?
- What current means of communications with these audiences are available or in use in your industry?
- What key messages need to be shared?
- Which of those messages should only go to certain audiences?
- What training for your audiences needs to be provided?
- As we move forward working with you, who should serve as our liaison with your committee/working group for the Public Awareness and Training Group?
- How are cyber incident emergencies managed in your CI sector and who do you contact for incident response?
- What exercise planning and management support can US-CERT and ICS-CERT provide to local government, state government, and private sector?
- What existing state agency services are available for individual, small-business, and local government cyber-crime response?
- What processes are in place for information sharing between and within CI sectors?
- How often are cybersecurity plans exercised and evaluated?
- What cyber incident response capabilities does the state currently support for recovery from a cyber event?
- Do state agencies carry insurance for cybersecurity risks, such as data breaches, cyber extortion, and other privacy breaches? If so, provide details regarding the insurance policies that apply to such risks. For example, are they endorsement or customized stand-alone policies? Who is the insurer and does the policy offer the following coverages: network and information security liability, communications and media liability, regulatory defense expenses, crisis management event expenses, security breach remediation and notification expenses, computer fraud, funds transfer fraud, e-commerce extortion, business interruption. (Provide sample policy/endorsements.)
- Do state agencies have a standard cybersecurity agreement with outside vendors that have access to data? Or does the language of the agreement vary per agency? If so, do those agreements require such vendors to carry insurance for cybersecurity risks? (Provide sample cop(ies) of agreement(s).)
- Do state agencies carry insurance for cybersecurity risks, such as data breaches, cyber extortion, and other privacy breaches? If so, provide details regarding the insurance policies that apply to such risks. For example, are they endorsement or customized stand-alone policies? Who is the insurer and does the policy offer the following coverages: network and information security

liability, communications and media liability, regulatory defense expenses, crisis management event expenses, security breach remediation and notification expenses, computer fraud, funds transfer fraud, e-commerce extortion, business interruption. (Provide sample policy/endorsements.)

- Do state agencies have a standard cybersecurity agreement with outside vendors that have access to data? Or does the language of the agreement vary per agency? If so, do those agreements require such vendors to carry insurance for cybersecurity risks? (Provide sample cop(ies) of agreement(s).)
- What laws or regulations (state or federal) impact your organization's cybersecurity initiatives?
- Please identify any positive effects of these laws/regulations on your organization (identifying which laws in particular).
- Please identity any negative effects of these laws/regulations on your organization (identifying which laws in particular).

Finance Committee

- What do you expect to receive from the Committee/Working Groups?
- What does your Sector expect from the Energy sector during incident response?
- How does your sector currently coordinate and collaborate with the energy sector?
- Which electric or natural gas energy services does your sector utilize?
- Does your sector provide its own energy (e.g., solar, microgrid, hydro, etc.)?
- Do you know of or participate in joint sector cyber exercises?
- Do you know of other state level cyber plans?
- What communications following an incident would you like from energy utilities?
- How can local governments fund cyber protection once it is determined what measures should be put in place?
- What are the minimum amounts that should be budgeted for cyber protection?
- Are there any collaborations that are possible to share the cost of funding?
- What does Finance sector use for 3rd Party vendor assessment questions?
- What does Finance sectors follow Security Framework?
- FFIEC - does anyone use FFIEC criteria and guidance to what extent?
- Any guidelines for Small Finance businesses or HealthCare sector?
- Who/what are your audiences that need to be reached?
- What current means of communications with these audiences are available or in use in your industry?
- What key messages need to be shared?
- Which of those messages should only go to certain audiences?
- What training for your audiences needs to be provided?
- As we move forward working with you, who should serve as our liaison with your committee/working group for the Public Awareness and Training Group?
- What are the funding options for state level departments to obtain cybersecurity insurance?
- Is there current funding, assistance, or pooling in place for local entities, including schools and county clerks, to obtain cybersecurity insurance? If not, does the state have other options to assist local entities to pay for cybersecurity insurance?
- What are the funding options for state level departments to obtain cybersecurity insurance?
- Is there current funding, assistance, or pooling in place for local entities, including schools and county clerks, to obtain cybersecurity insurance? If not, does the state have other options to assist local entities to pay for cybersecurity insurance?
- What laws or regulations (state or federal) impact your organization's cybersecurity initiatives?
- Please identify any positive effects of these laws/regulations on your organization (identifying which laws in particular).
- Please identity any negative effects of these laws/regulations on your organization (identifying which laws in particular).

Energy Committee

- What do you expect to receive from the Committee/Working Groups?
- What information about cybersecurity posture is collected or surveyed of the sector (required or voluntarily) and by whom?
- How is Protected Critical Infrastructure Information (PCII) maintained by the collecting agency when sharing compiled information?
- What does Energy sector use for 3rd Party vendor assessment questions?
- What does Energy sector follow Security Framework?
- Where does HealthCare fall in the order of delivering service after a disaster?
- Does the sector have a good contact list for local Healthcare officials?
- Any regulations preventing HealthCare standing up Solar or wind?
- Who/what are your audiences that need to be reached?
- What current means of communications with these audiences are available or in use in your industry?
- What key messages need to be shared?
- Which of those messages should only go to certain audiences?
- What training for your audiences needs to be provided?
- As we move forward working with you, who should serve as our liaison with your committee/working group for the Public Awareness and Training Group?
- What laws or regulations (state or federal) impact your organization's cybersecurity initiatives?
- Please identify any positive effects of these laws/regulations on your organization (identifying which laws in particular).
- Please identity any negative effects of these laws/regulations on your organization (identifying which laws in particular).

Water and Wastewater Committee

- What do you expect to receive from the Committee/Working Groups?
- What does your Sector expect from the Energy sector during incident response?
- How does your sector currently coordinate and collaborate with the energy sector?
- Which electric or natural gas energy services does your sector utilize?
- Does your sector provide its own energy (e.g., solar, microgrid, hydro, etc.)?
- Do you know of or participate in joint sector cyber exercises?
- Do you know of other state level cyber plans?
- What communications following an incident would you like from energy utilities?
- How do we design water and waste water cyber security protections for treatment plants with varying levels of connectivity?
- What does Water/Wastewater sector use for 3rd Party vendor assessment questions?
- What does Water/Wastewater sector follow Security Framework?
- Where does HealthCare fall in the order of delivering service after a disaster?
- Does the sector have a good contact list for Local Healthcare officials?
- Are there regulations on using Groundwater?
- Who/what are your audiences that need to be reached?
- What current means of communications with these audiences are available or in use in your industry?
- What key messages need to be shared?
- Which of those messages should only go to certain audiences?
- What training for your audiences needs to be provided?
- As we move forward working with you, who should serve as our liaison with your committee/working group for the Public Awareness and Training Group?
- How are cyber incident emergencies managed in your CIKR sector and who do you contact for incident response?
- What laws or regulations (state or federal) impact your organization's cybersecurity initiatives?
- Please identify any positive effects of these laws/regulations on your organization (identifying which laws in particular).
- Please identity any negative effects of these laws/regulations on your organization (identifying which laws in particular).

Communications Committee

- What do you expect to receive from the Committee/Working Groups?
- What does your Sector expect from the Energy sector during incident response?
- How does your sector currently coordinate and collaborate with the energy sector?
- Which electric or natural gas energy services does your sector utilize?
- Does your sector provide its own energy (e.g., solar, microgrid, hydro, etc.)
- Do you know of or participate in joint sector cyber exercises?
- Do you know of other state level cyber plans?
- What communications following an incident would you like from energy utilities?
- If the telecommunications network is interrupted, what back-up or alternatives are available to assist energy companies in maintaining safe operations?
- How can local government best protect our emergency response communication systems?
- What does Communications sector use for 3rd Party vendor assessment questions?
- What does Communications sector follow Security Framework?
- Where does HEALTHCARE fall in the order of delivering service after a disaster?
- Does the sector have a good contact list for Local Healthcare officials?
- Are there Communication channels for disasters
- Who/what are your audiences that need to be reached?
- What current means of communications with these audiences are available or in use in your industry?
- What key messages need to be shared?
- Which of those messages should only go to certain audiences?
- What training for your audiences needs to be provided?
- As we move forward working with you, who should serve as our liaison with your committee/working group for the Public Awareness and Training Group?
- What laws or regulations (state or federal) impact your organization's cybersecurity initiatives?
- Please identify any positive effects of these laws/regulations on your organization (identifying which laws in particular).
- Please identity any negative effects of these laws/regulations on your organization (identifying which laws in particular).

Healthcare Committee

- What do you expect to receive from the Committee/Working Groups?
- What does your Sector expect from the Energy sector during incident response?
- How does your sector currently coordinate and collaborate with the energy sector?
- Which electric or natural gas energy services does your sector utilize?
- Does your sector provide its own energy (e.g., solar, microgrid, hydro, etc.)
- Do you know of or participate in joint sector cyber exercises?
- Do you know of other state level cyber plans?
- What communications following an incident would you like from energy utilities?
- What information about cybersecurity posture is collected or surveyed of the sector (required or voluntarily) and by whom?
- How is Protected Critical Infrastructure Information (PCII) maintained by the collecting agency when sharing compiled information?
- Does anyone have the ability or support Wells?
- What types of Cyber Tabletop formats have you performed?
- Who/what are your audiences that need to be reached?
- What current means of communications with these audiences are available or in use in your industry?
- What key messages need to be shared?
- Which of those messages should only go to certain audiences?
- What training for your audiences needs to be provided?
- As we move forward working with you, who should serve as our liaison with your committee/working group for the Public Awareness and Training Group?
- What laws or regulations (state or federal) impact your organization's cybersecurity initiatives?
- Please identify any positive effects of these laws/regulations on your organization (identifying which laws in particular).
- Please identity any negative effects of these laws/regulations on your organization (identifying which laws in particular).

Defense Industrial Committee

- What do you expect to receive from the Committee/Working Groups?
- What does your Sector expect from the Energy sector during incident response?
- How does your sector currently coordinate and collaborate with the energy sector?
- Which electric or natural gas energy services does your sector utilize?
- Does your sector provide its own energy (e.g., solar, microgrid, hydro, etc.)?
- Do you know of or participate in joint sector cyber exercises?
- Do you know of other state level cyber plans?
- What communications following an incident would you like from energy utilities?
- What does Defense sector use for 3rd Party vendor assessment questions?
- What does Defense sector follow Security Framework?
- Who/what are your audiences that need to be reached?
- What current means of communications with these audiences are available or in use in your industry?
- What key messages need to be shared?
- Which of those messages should only go to certain audiences?
- What training for your audiences needs to be provided?
- As we move forward working with you, who should serve as our liaison with your committee/working group for the Public Awareness and Training Group?
- What laws or regulations (state or federal) impact your organization's cybersecurity initiatives?
- Please identify any positive effects of these laws/regulations on your organization (identifying which laws in particular).
- Please identity any negative effects of these laws/regulations on your organization (identifying which laws in particular).
- Are there uniform security standards and/or cyber insurance requirements for each election district?

Elections Committee

- What do you expect to receive from the Committee/Working Groups?
- What does your Sector expect from the Energy sector during incident response?
- How does your sector currently coordinate and collaborate with the energy sector?
- Which electric or natural gas energy services does your sector utilize?
- Does your sector provide its own energy (e.g., solar, microgrid, hydro, etc.)?
- Do you know of or participate in joint sector cyber exercises?
- Do you know of other state level cyber plans?
- What communications following an incident would you like from energy utilities?
- What does Elections use for 3rd Party vendor assessment questions?
- What does Elections follow Security Framework?
- Who/what are your audiences that need to be reached?
- What current means of communications with these audiences are available or in use in your industry?
- What key messages need to be shared?
- Which of those messages should only go to certain audiences?
- What training for your audiences needs to be provided?
- As we move forward working with you, who should serve as our liaison with your committee/working group for the Public Awareness and Training Group?
- Are there uniform security standards and/or cyber insurance requirements for each election district?
- What laws or regulations (state or federal) impact your organization's cybersecurity initiatives?
- Please identify any positive effects of these laws/regulations on your organization (identifying which laws in particular).
- Please identity any negative effects of these laws/regulations on your organization (identifying which laws in particular).

Economic Development Committee

- What do you expect to receive from the Committee/Working Groups?
- What does your Sector expect from the Energy sector during incident response?
- How does your sector currently coordinate and collaborate with the energy sector?
- Which electric or natural gas energy services does your sector utilize?
- Does your sector provide its own energy (e.g., solar, microgrid, hydro, etc.)?
- Do you know of or participate in joint sector cyber exercises?
- Do you know of other state level cyber plans?
- What communications following an incident would you like from energy utilities?
- Is there software to electronically "sort" the vast amount of data to help identify and prioritize risks?
- Has anyone created a centralized clearinghouse which assesses vendors with differing levels of cybersecurity exposure and risk mitigation?
- Is there a centralized way to understand the risks in a particular component right "out of the box" when a utility procures that component? This should include things like chain of custody for the component or who built a subcomponent.
- What other policy changes could encourage sector growth?
- What would impact be of eliminating non-competes? What if non-compete exclusion only applied if individual left to start new business (competing, but not leveraging IP)?
- Should there be a cyber investment credit for businesses? If they use Indiana-based companies? How to offset investment by Small/Medium Businesses?
- How do we ensure infrastructure is in place?
- Once a sector can quantify moving their Cybersecurity how can we use that to bring more development
- Who/what are your audiences that need to be reached?
- What current means of communications with these audiences are available or in use in your industry?
- What key messages need to be shared?
- Which of those messages should only go to certain audiences?
- What training for your audiences needs to be provided?
- As we move forward working with you, who should serve as our liaison with your committee/working group for the Public Awareness and Training Group?
- What laws or regulations (state or federal) impact your organization's cybersecurity initiatives?
- Please identify any positive effects of these laws/regulations on your organization (identifying which laws in particular).
- Please identity any negative effects of these laws/regulations on your organization (identifying which laws in particular).

Workforce Development Committee

- What do you expect to receive from the Committee/Working Groups?
- What does your Sector expect from the Energy sector during incident response?
- How does your sector currently coordinate and collaborate with the energy sector?
- Which electric or natural gas energy services does your sector utilize?
- Does your sector provide its own energy (e.g., solar, microgrid, hydro, etc.)?
- Do you know of or participate in joint sector cyber exercises?
- Do you know of other state level cyber plans?
- What communications following an incident would you like from energy utilities?
- Training of skilled cybersecurity professionals, including those with less that a four-year degree. The NIST National Initiative for Cybersecurity Education (NICE) cybersecurity workforce framework, developed in August 2017, provides the foundational skills necessary in various roles within the cybersecurity protection departments of Indiana's energy companies. Is this the model every sector should be following?
- Once a sector can quantify moving their Cybersecurity how can we use that to bring more development?
- Who/what are your audiences that need to be reached?
- What current means of communications with these audiences are available or in use in your industry?
- What key messages need to be shared?
- Which of those messages should only go to certain audiences?
- What training for your audiences needs to be provided?
- As we move forward working with you, who should serve as our liaison
- with your committee/working group for the Public Awareness and Training Group?
- What laws or regulations (state or federal) impact your organization's cybersecurity initiatives?
- Please identify any positive effects of these laws/regulations on your organization (identifying which laws in particular).
- Please identity any negative effects of these laws/regulations on your organization (identifying which laws in particular).
- What are the current STEM education and outreach initiatives within the state?
- Are there cyber tax credits/Tuition reimbursement programs?
- Are there Federal grants?

Personal Identifiable Information Working Group

- What do you expect to receive from the Committee/Working Groups?
- What does your Sector expect from the Energy sector during incident response?
- How does your sector currently coordinate and collaborate with the energy sector?
- Which electric or natural gas energy services does your sector utilize?
- Does your sector provide its own energy (e.g., solar, microgrid, hydro, etc.)?
- Do you know of or participate in joint sector cyber exercises?
- Do you know of other state level cyber plans?
- What communications following an incident would you like from energy utilities?
- Local governments house sensitive personal identification information from citizens (i.e. social security numbers, child protection records, etc.) – how can we best protect it?
- Local governments house data that is public information (such as property records, arrest records, election information, and historical financial information). Although accessible to the public, a loss of these records would be devastating to the operation of government. How do we best protect it?
- How will information about Critical Infrastructure companies, and key employees be managed?
- What Risk and process assessments should local government use to protect their data?
- What laws or regulations (state or federal) impact your organization's cybersecurity initiatives?
- Please identify any positive effects of these laws/regulations on your organization (identifying which laws in particular).
- Please identity any negative effects of these laws/regulations on your organization (identifying which laws in particular).
- Has anyone considered expanding the definition to include biometric information, unencrypted login and password combinations, html5 "digital fingerprint," unencrypted knowledge-based authentication questions, unique policy numbers, unique account numbers, debit card numbers where the card may be used as a credit card?
- Who/what are your audiences that need to be reached?
- What current means of communications with these audiences are available or in use in your industry?
- What key messages need to be shared?
- Which of those messages should only go to certain audiences?
- What training for your audiences needs to be provided?
- As we move forward working with you, who should serve as our liaison with your committee/working group for the Public Awareness and Training Group?
- How are cyber incident emergencies managed in your CIKR sector and who do you contact for incident response?

Public Awareness and Training Working Group

- What do you expect to receive from the Committee/Working Groups?
- What does your Sector expect from the Energy sector during incident response?
- How does your sector currently coordinate and collaborate with the energy sector?
- Which electric or natural gas energy services does your sector utilize?
- Does your sector provide its own energy (e.g., solar, microgrid, hydro, etc.)?
- Do you know of or participate in joint sector cyber exercises?
- Do you know of other state level cyber plans?
- What communications following an incident would you like from energy utilities?
- How do we train local government employees to institute cyber security protections?
- What should the training curriculum be?
- Are there way to collaborate to standardize training and share training costs between governmental entities?
- What training support will be available to each of the verticals?
- What has worked in the past for driving public education and messages?
- How can we align to help drive public awareness for the sectors?
- What mechanisms are you planning on using to distribute any training materials created by the Council?
- Are you concentrating on both the public and private sectors?
- Who/what are your audiences that need to be reached?
- What current means of communications with these audiences are available or in use in your industry?
- What key messages need to be shared?
- Which of those messages should only go to certain audiences?
- What training for your audiences needs to be provided?
- As we move forward working with you, who should serve as a liaison with other committee/working groups?
- How can we all identify, differentiate, and clarify cyber terminology: cyber, cybersecurity, cyber incident, cyber emergency, etc.?
- What laws or regulations (state or federal) impact your organization's cybersecurity initiatives?
- Please identify any positive effects of these laws/regulations on your organization (identifying which laws in particular).
- Please identity any negative effects of these laws/regulations on your organization (identifying which laws in particular).
- What programs, if any, currently focus on public awareness and training for any state function?

Emergency Services and Exercise Working Group

- What do you expect to receive from the Committee/Working Groups?
- What does your Sector expect from the Energy sector during incident response?
- How does your sector currently coordinate and collaborate with the energy sector?
- Which electric or natural gas energy services does your sector utilize?
- Does your sector provide its own energy (e.g., solar, microgrid, hydro, etc.)?
- Do you know of or participate in joint sector cyber exercises?
- Do you know of other state level cyber plans?
- What communications following an incident would you like from energy utilities?
- How can local government best protect our emergency response communication systems?
- How does HEALTHCARE notify Emergency Service for issues / diverting patients?
- Planned for Cyber-attacks for the sector? If done, what were the results of the exercise?
- What are Cyber Tabletop formats and strategies used?
- Are there knowledge center to share information without recourse?
- Do you have sample table top exercises?
- Who/what are your audiences that need to be reached?
- What current means of communications with these audiences are available or in use in your industry?
- What key messages need to be shared?
- Which of those messages should only go to certain audiences?
- What training for your audiences needs to be provided?
- As we move forward working with you, who should serve as our liaison with your committee/working group for the Public Awareness and Training Group?
- What laws or regulations (state or federal) impact your organization's cybersecurity initiatives?
- Please identify any positive effects of these laws/regulations on your organization (identifying which laws in particular).
- Please identity any negative effects of these laws/regulations on your organization (identifying which laws in particular).
- What programs, if any, currently focus on public awareness and training for any state function?

Cyber Sharing Working Group

- What do you expect to receive from the Committee/Working Groups?
- What does your Sector expect from the Energy sector during incident response?
- How does your sector currently coordinate and collaborate with the energy sector?
- Which electric or natural gas energy services does your sector utilize?
- Does your sector provide its own energy (e.g., solar, microgrid, hydro, etc.)?
- Do you know of or participate in joint sector cyber exercises?
- Do you know of other state level cyber plans?
- What communications following an incident would you like from energy utilities?
- What legitimate cyber protection tools are already available to local government to guard against cyber threats?
- Is IN-ISAC used as an information sharing method?
- Is there a place for Knowledge center to share information without recourse?
- How are we going to promote a culture of cyber sharing within the state in such a way to provide no recourse/retribution for those People/Entities who share cyber-related information?
- How do you intend to share threat intelligence to organizations that don't have the ability to process stix feeds, etc?
- Do you have information about the best way to receive and respond to cyber threat information?
- Training materials for this?
- Who/what are your audiences that need to be reached?
- What current means of communications with these audiences are available or in use in your industry?
- What key messages need to be shared?
- Which of those messages should only go to certain audiences?
- What training for your audiences needs to be provided?
- As we move forward working with you, who should serve as our liaison with your committee/working group for the Public Awareness and Training Group?
- What laws or regulations (state or federal) impact your organization's cybersecurity initiatives?
- Please identify any positive effects of these laws/regulations on your organization (identifying which laws in particular).
- Please identity any negative effects of these laws/regulations on your organization (identifying which laws in particular).

Policy Working Group

- What do you expect to receive from the Energy Committee?
- What does your Sector expect from the Energy sector during incident response?
- How does your sector currently coordinate and collaborate with the energy sector?
- Which electric or natural gas energy services does your sector utilize?
- Does your sector provide its own energy (e.g., solar, microgrid, hydro, etc.)?
- Do you know of or participate in joint sector cyber exercises?
- Do you know of other state level cyber plans?
- What communications following an incident would you like from energy utilities?
- There is a need to strengthen communications between the sectors. For example it is not unprecedented that an issue in the financial sector appears in the Energy sector later. How can this be accomplished?
- Any regulations preventing HEALTHCARE standing up Solar or wind?
- Any Regulations preventing HEALTHCARE from sanding up direct wells?
- Sample policies for physical security of systems?
- What laws or regulations (state or federal) impact your organization's cybersecurity initiatives?
- Please identify any positive effects of these laws/regulations on your organization (identifying which laws in particular).
- Please identity any negative effects of these laws/regulations on your organization (identifying which laws in particular).
- Who/what are your audiences that need to be reached?
- What current means of communications with these audiences are available or in use in your industry?
- What key messages need to be shared?
- Which of those messages should only go to certain audiences?
- What training for your audiences needs to be provided?
- As we move forward working with you, who should serve as our liaison with your committee/working group for the Public Awareness and Training Group?

Pre thru Post Incident Working Group

- What do you expect to receive from the Committee/Working Groups?
- What does your Sector expect from the Energy sector during incident response?
- How does your sector currently coordinate and collaborate with the energy sector?
- Which electric or natural gas energy services does your sector utilize?
- Does your sector provide its own energy (e.g., solar, microgrid, hydro, etc.)?
- Do you know of or participate in joint sector cyber exercises?
- Do you know of other state level cyber plans?
- What communications following an incident would you like from energy utilities?
- What should local governments be doing pre-incident to make sure that internal controls are in place?
- What is the best approach for local governments to institute penetration testing?
- What is the best approach for local governments to use for cyber security planning, response and recovery?
- Contact info to obtain services as needed?
- When or how to use 'jump team'?
- Sample Incident response plans?
- Who/what are your audiences that need to be reached?
- What current means of communications with these audiences are available or in use in your industry?
- What key messages need to be shared?
- Which of those messages should only go to certain audiences?
- What training for your audiences needs to be provided?
- As we move forward working with you, who should serve as our liaison with your committee/working group?
- What laws or regulations (state or federal) impact your organization’s cybersecurity initiatives?
- Please identify any positive effects of these laws/regulations on your organization (identifying which laws in particular).
- Please identity any negative effects of these laws/regulations on your organization (identifying which laws in particular).

Legal and Cyber Insurance Working Group

- What do you expect to receive from the Committee/Working Groups?
- What does your Sector expect from the Energy sector during incident response?
- How does your sector currently coordinate and collaborate with the energy sector?
- Which electric or natural gas energy services does your sector utilize?
- Does your sector provide its own energy (e.g., solar, microgrid, hydro, etc.)?
- Do you know of or participate in joint sector cyber exercises?
- Do you know of other state level cyber plans?
- What communications following an incident would you like from energy utilities?
- Can the state offer a statewide insurance policy that is available to local governments in order to provide a cost-savings?
- Who/what are your audiences that need to be reached?
- What current means of communications with these audiences are available or in use in your industry?
- What key messages need to be shared?
- Which of those messages should only go to certain audiences?
- What training for your audiences needs to be provided?
- As we move forward working with you, who should serve as our liaison with your committee/working group for the Public Awareness and Training Group?
- What laws or regulations (state or federal) impact your organization's cybersecurity initiatives?
- Please identify any positive effects of these laws/regulations on your organization (identifying which laws in particular).
- Please identity any negative effects of these laws/regulations on your organization (identifying which laws in particular).

Local Government Working Group

- What do you expect to receive from the Committee/Working Groups?
- What does your Sector expect from the Energy sector during incident response?
- How does your sector currently coordinate and collaborate with the energy sector?
- Which electric or natural gas energy services does your sector utilize?
- Does your sector provide its own energy (e.g., solar, microgrid, hydro, etc.)?
- Do you know of or participate in joint sector cyber exercises?
- Do you know of other state level cyber plans?
- What communications following an incident would you like from energy utilities?
- How is cybersecurity for water/wastewater managed?
- How does the local government work with the local HealthCare system?
- Is there current funding, assistance, or pooling in place for local entities, including schools and county clerks, to obtain cybersecurity insurance? If not, does the state have other options to assist local entities to pay for cybersecurity insurance?
- Are there current guidelines for local entities and school systems regarding cybersecurity insurance for the local entities and for outside vendors that handle private electronic data?
- Do we know how many local governments carry insurance for cybersecurity risks, such as data breaches, cyber extortion, and other privacy breaches? If so, provide details regarding the insurance policies that apply to such risks. For example, are they endorsements or stand-alone customized policies? Who is the insurer and does the policy offer the following coverages: network and information security liability, communications and media liability, regulatory defense expenses, crisis management event expenses, security breach remediation and notification expenses, computer fraud, funds transfer fraud, e-commerce extortion, business interruption. (Provide sample policy/endorsements.)
- Is there current funding, assistance, or pooling in place for local entities, including schools and county clerks, to obtain cybersecurity insurance? If not, does the state have other options to assist local entities to pay for cybersecurity insurance?
- Are there current guidelines for local entities and school systems regarding cybersecurity insurance for the local entities and for outside vendors that handle private electronic data?
- Do we know how many local governments carry insurance for cybersecurity risks, such as data breaches, cyber extortion, and other privacy breaches? If so, provide details regarding the insurance policies that apply to such risks. For example, are they endorsements or stand-alone customized policies? Who is the insurer and does the policy offer the following coverages: network and information security liability, communications and media liability, regulatory defense expenses, crisis management event expenses, security breach remediation and notification expenses, computer fraud, funds transfer fraud, e-commerce extortion, business interruption. (Provide sample policy/endorsements.)
- What laws or regulations (state or federal) impact your organization's cybersecurity initiatives?
- Please identify any positive effects of these laws/regulations on your organization (identifying which laws in particular).
- Please identity any negative effects of these laws/regulations on your organization (identifying which laws in particular).
- Who/what are your audiences that need to be reached?

- What current means of communications with these audiences are available or in use in your industry?
- What key messages need to be shared?
- Which of those messages should only go to certain audiences?
- What training for your audiences needs to be provided?
- As we move forward working with you, who should serve as our liaison with your committee/working group for the Public Awareness and Training Group?

Strategic Resource Working Group

- What do you expect to receive from the Committee/Working Groups?
- What does your Sector expect from the Energy sector during incident response?
- How does your sector currently coordinate and collaborate with the energy sector?
- Which electric or natural gas energy services does your sector utilize?
- Does your sector provide its own energy (e.g., solar, microgrid, hydro, etc.)?
- Do you know of or participate in joint sector cyber exercises?
- Do you know of other state level cyber plans?
- What communications following an incident would you like from energy utilities?
- How do local governments choose a legitimate/reputable provider of cyber security services?
- How do local governments differentiate between vendors that are vying for business?
- Who/what are your audiences that need to be reached?
- What current means of communications with these audiences are available or in use in your industry?
- What key messages need to be shared?
- Which of those messages should only go to certain audiences?
- What training for your audiences needs to be provided?
- As we move forward working with you, who should serve as our liaison with your committee/working group for the Public Awareness and Training Group?
- How can cybersecurity information collected for surveys, assessments, and evaluations of water/wastewater entities be shared with the state?
- Who can help at the state level make a more formal request?
- How can we identify, differentiate, and clarify terminology: cyber, cybersecurity, cyber incident, cyber emergency, etc.?
- What laws or regulations (state or federal) impact your organization's cybersecurity initiatives?
- Please identify any positive effects of these laws/regulations on your organization (identifying which laws in particular).
- Please identity any negative effects of these laws/regulations on your organization (identifying which laws in particular).

Cyber Summit Working Group

- What other cyber conferences/summits are held in the USA and internationally?
- What do you expect to receive from the Committee/Working Groups?
- What does your Sector expect from the Energy sector during incident response?
- How does your sector currently coordinate and collaborate with the energy sector?
- Which electric or natural gas energy services does your sector utilize?
- Does your sector provide its own energy (e.g., solar, microgrid, hydro, etc.)?
- Do you know of or participate in joint sector cyber exercises?
- Do you know of other state level cyber plans?
- What communications following an incident would you like from energy utilities?
- How do local governments choose a legitimate/reputable provider of cyber security services?
- How do local governments differentiate between vendors that are vying for business?
- Who/what are your audiences that need to be reached?
- What current means of communications with these audiences are available or in use in your industry?
- What key messages need to be shared?
- Which of those messages should only go to certain audiences?
- What training for your audiences needs to be provided?
- As we move forward working with you, who should serve as our liaison with your committee/working group for the Public Awareness and Training Group?
- How can cybersecurity information collected for surveys, assessments, and evaluations of w/ww entities be shared with the state? Who can help at the state level make a more formal request?
- Can this summit be used to identify, differentiate, and clarify terminology: cyber, cybersecurity, cyber incident, cyber emergency, etc.?
- What laws or regulations (state or federal) impact your organization's cybersecurity initiatives?
- Please identify any positive effects of these laws/regulations on your organization (identifying which laws in particular).
- Please identity any negative effects of these laws/regulations on your organization (identifying which laws in particular).

GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

DELIVERABLE FORM
PHASE 2

IECC Committee/Working Group: _____
Person Submitting Form: _____
Date: _____

PHASE 2 – PLANNING

1. What is the deliverable?

2. What is the status of this deliverable?
   ☐ Completed ☐ In-progress 25% ☐ In-progress 50% ☐ In-progress 75% ☐ 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?

6. What metric or measurement will be used to define success?

7. What year will the deliverable be completed?
   ☐ 2018 ☐ 2019 ☐ 2020 ☐ 2021 ☐ 2022 ☐ 2023+

8. Who or what entities will benefit from the deliverable?

9. Which state or federal resources or programs overlap with this deliverable?

Additional Questions:

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

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

12. Who should be main lead of this deliverable?

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

PHASE 3 – IMPLEMENTATION

As your team works through completing the Deliverable Form for Phase 2, please begin making note and thinking through the specific tasks, owners, and deadlines to complete this deliverable. In addition, start discussing the estimated budget to start the deliverable, budget to sustain the deliverable (if applicable), resources (staff, structure, stuff), etc. Further direction will be provided in the coming weeks for Phase 3.

GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

IMPLEMENTATION PLANNING FORM
PHASE 3

IECC Committee/Working Group:
Person Submitting Form:
Date:

PHASE 3 – IMPLEMENTATION PLANNING

1. What is the deliverable?

2. Is this a one-time deliverable or one that will require sustainability?
   ☐ One-time deliverable
   ☐ Ongoing/sustained effort

Tactic Timeline (Please add rows as needed.)

Tactic	Owner	% Complete	Deadline	Notes

Resources and Budget

3. Will staff be required to complete this deliverable? ☐No ☐ Yes
   a. If Yes, please complete the following:

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

4. 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

Benefits and Risks

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

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

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

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

9. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics? ☐No ☐ Yes
   a. If Yes, please list states/jurisdictions: Click or tap here to enter text.

10. 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? ☐No ☐ Yes
    a. If Yes, please list states/jurisdictions: Click or tap here to enter text.

Other

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

12. Does this deliverable require a change from a regulatory/policy standpoint? ☐No ☐ Yes
    a. If Yes, what is the change and what could be the fiscal impact if the change is made?

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

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

15. Can this deliverable be used by other sectors? ☐No ☐ Yes,
    a. If Yes, please list sectors:

Communications

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

17. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)? ☐No ☐ Yes

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

GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

EVALUATION FORM
PHASE 4

IECC Committee/Working Group:
Date:

PHASE 4 – EVALUATION PHASE

Deliverable:

Objective 1:

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:

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

Evaluative Methods Details for all methods except "Completion"

#	Who	How	Owner	Staff #	Costs	Funding Source	Schedule / Frequency	Notes
1								
2								
3								
4								
5								

Questions

Notes