EMERGENCY SERVICES AND EXERCISE WORKING GROUP STRATEGIC PLAN

Chair: Executive Director Bryan Langley | Co-Chair: Carlos Garcia

September 2018
Indiana Executive Council on Cybersecurity

Emergency Services and Exercise Working Group Plan

Contents

Committee Members

Committee Members

Name	**Organization**	**Title**	**Committee/ Workgroup Position**	**IECC Membership Type**
Bryan Langley	IDHS	Executive Director	Chair	Voting
Carlos Garcia	IU - Emergency Management	University Director	Co-Chair	Advisory
Joe Romero	IU Health	Manager	Co-Chair Proxy	Advisory
Tom Vanderpool	Indiana Department of Transportation	Emergency Planning & Response Director	Full Time	Advisory
David Vice	Integrated Public Safety Commission	Executive Director	Full Time	Advisory
Kathy Dayhoff-Dwyer	Indiana Department of Homeland Security	Local Support Branch Director	Full Time	Advisory
Steve Berube	Citizens Energy Group	Manager of Water System Control and Planning	Full Time	Advisory
Doug Brock	American Water	Vice President of Operations	Full Time	Advisory
Cliff Campbell	Campbell Consulting	President	As Needed	Advisory
Ed Reuter	Indiana Statewide 911 Board	Executive Director	Full Time	Advisory
Debbie Fletcher	Indiana Department of Homeland Security	Exercise Training Officer	As Needed	Advisory
Erin Rowe	Indiana Department of Homeland Security	Director, Response and Recovery	As Needed	Advisory
Mike Alley	Resilient Strategies, LLC	President	Full Time	Advisory
Joe Meluch	Indiana Department of Homeland Security	Emergency Operations Center Shift Manager	Full Time	Advisory
Jonathon Barefoot	Ivy Tech Community College	Executive Director of Statewide Safety and Security	Full Time	Advisory

Introduction

Introduction

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

Executive Summary

Executive Summary

- **Research Conducted**
    - **National Incident Management System (NIMS)**: A comprehensive, national approach to incident management that is applicable at all jurisdictional levels and across functional disciplines.
    - **Emergency Management Accreditation Program (EMAP)**: A set of 64 professional emergency management standards designed as a tool for continuous improvement as part of a voluntary accreditation process for local, state, federal, higher education and tribal emergency management programs.
    - **National Fire Protection Association (NFPA) Standard 1600 - Disaster/Emergency Management and Business Continuity/Continuity of Operations Programs**: A common set of criteria for all hazards disaster/emergency management and business continuity programs.
    - **Centers for Medicare and Medicaid Services (CMS) Emergency Preparedness Rule:** Establishes national emergency preparedness requirements for healthcare entities to ensure adequate planning for both natural and man-made disasters, and coordination with federal, state, tribal, regional and local emergency preparedness systems.
    - **The Joint Commission Emergency Management Standard:** Healthcare accreditation standards outlining program requirements for preparedness, mitigation, response, and recovery phases of emergency management.
    - **Presidential Policy Directive (PPD) 41 – U.S. Cyber Incident Coordination:** This directive sets forth principles governing the Federal Government's response to any cyber incident, whether involving government or private sector entities**.**
    - **Health Insurance Portability and Accountability Act (HIPAA) Security Rule:** Federal information security requirements put in place to safeguard individuals' electronic protected health information.
    - **Homeland Security Exercise Evaluation Program (HSEEP):** Provides a set of guiding principles for exercise programs, as well as a common approach to exercise program management, design and development, conduct, evaluation, and improvement planning.
    - **United States Computer Emergency Readiness Team (US-CERT):** Organizations within the U.S. Department of Homeland Security tasked with providing cyber incident prevention, protection, preparedness, response, and recovery capabilities to federal, state, local, and tribal government agencies.

- **Research Findings**
    - Existing national standards and best practices for emergency preparedness and all-hazard incident management are applicable to cybersecurity initiatives.
    - The basic concepts for emergency planning, training, exercise, evaluation, and improvement can be implemented as the foundation for cybersecurity preparedness programs.
    - An abundance of cybersecurity information and services are available to individuals, government agencies, and private sector organizations.

  - There is, however, a lack of affordable, easily accessible tools and resources geared specifically for small business and small local government entities.
  - There no central point of coordination and information sharing for state-level cybersecurity planning, training, and exercise activity.

- **Working Group Deliverables**
  - Conduct review of the Cyber Annex to State of Indiana Comprehensive Emergency Management Plan.
  - Draft recommendations for revisions to the Cyber Annex and development of a coordinating entity within the Indiana State Emergency Operations Center.
  - Develop threat assessment, planning, training, and exercise toolkit for local government and small businesses.
  - Create guidance for coordination of local government, private sector, and state government cybersecurity drill and exercise activity.

- **Additional Notes**
  - No additional information at this time.

- **References**
  - **National Incident Management System (NIMS)**: https://www.fema.gov/national-incident-management-system
  - **Emergency Management Accreditation Program (EMAP)**: https://www.emap.org/
  - **National Fire Protection Association (NFPA) Standard 1600:** https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=1600
  - **Centers for Medicare and Medicaid Services (CMS) Emergency Preparedness Rule:** https://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/SurveyCertEmergPrep/Emergency-Prep-Rule.html
  - **The Joint Commission Emergency Management Standard:** https://www.jointcommission.org/emergency_management.aspx
  - **PPD 41 – U.S. Cyber Incident Coordination:** https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident
  - **Homeland Security Exercise Evaluation Program (HSEEP):** https://www.fema.gov/hseep
  - **Health Insurance Portability and Accountability Act (HIPAA) Security Rule:** https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html
  - **U.S. Computer Emergency Readiness Team (US-CERT):** https://www.us-cert.gov/

Research

Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
   - **COMPLETED ACTIONS**
     - 2015 State Cybersecurity Reference Guide – Drawing from the 2009 Cybersecurity Strategy, this document provides an overview of national best practices, professional standards, and provides case studies of cybersecurity programs in other states.
     - Supervisory Control and Data Acquisition (SCADA) Smartbook is completed, outlining Industrial Control System risks to critical infrastructure.
     - Management and oversight of joint public/private/military cybersecurity exercises have been transferred from the Indiana Chapter of Infragard to Indiana Department of Homeland Security (IDHS).
     - IDHS completes State Strategic Roadmap to Cybersecurity, outlining five essential pillars.
     - Crit-Ex 16.1 Cyber Disruption Tabletop Exercise is completed. Government, emergency management, water utilities, and power utilities discuss responding to a long-term regional power outage.
     - Crit-Ex 16.2 Functional Exercise is completed. Water utilities respond to a cyberattack on a water treatment facility's SCADA system at Muscatatuck Urban Training Center (MUTC).
     - Governor's Council on Cybersecurity is established via EO and launched.
     - Crit-Ex Cybersecurity Awareness Seminar is completed – first in a series of progressively sophisticated exercises for 2016-2017.
     - Significant Cyber Incident Response Annex to State CEMP Workshop is held.
     - IDHS Training & Exercise completes Cybersecurity Awareness Seminars for Emergency Management Administrators (EMAs) in districts 5, 6, and 7.
     - Continuity/Cybersecurity workshops are brought into local jurisdictions, designed by Federal Emergency Management Agency (FEMA) and US DHS.
   - **CURRENT ACTIONS**
     - Draft version of Significant Cyber Incident Response Annex is under review.
     - Identification and outreach with subject-matter experts, policymakers, and executive leadership for inclusion in the State's cybersecurity program governing and project management bodies.
     - Inventory and support cyber grant opportunities for local and CI partners.
   - There have been a number of exercises and trainings across the state that touch on cybersecurity and directly correspond public safety and emergency services. Examples of these include:
     - Indiana Office of Technology – Cyber Security Mentoring Program

        - State of Indiana Joint Full-Scale Exercises – CritEx – 2015 and 2016 (Electrical Grid response) at Muscatatuck Urban Training Center
        - Cyber Security-Based Tabletop Exercises – Private Sector, International Manufacturing, Higher Education
        - Hamilton County (Indiana) Threat and Hazard Identification and Risk Assessment Exercise focusing on Cyber Response – 2017
        - Ivy Tech has bi-annual training on Cyber Security for staff and adjunct faculty

2. **What (or who) are the most significant cyber vulnerabilities in your area?**
    - Critical infrastructures and emergency service sectors
    - In a conference call in December 2017 to discuss these questions, the Working Group proposed that the primary vulnerabilities in each of our areas fall generally in the following three (3) areas:
        - People – human error, lack of training, or actual intent to cause harm are all people-oriented vulnerabilities that can be mitigated or reduced.
        - Process – Key procedures, protocols, and policies related to the need to lessen or prevent cyber incidents has to be in place and directed toward all areas of vulnerabilities within a given agency, department, and/or sector.
        - Technology – new or emerging technologies to lessen or prevent vulnerabilities also seem to prompt hackers/criminals to test or challenge new systems, software, hardware, etc.

3. **What is your area's greatest cybersecurity need and/or gap?**
    - Resources to serve all those in need for the state is a significant need.
    - In a meeting and conference call conducted on December 2017 to discuss these questions, the Working Group all agreed the most significant cybersecurity need or gap continues to be the following:
        - Frequent and on-going training frontline system users and staff
        - Engaged and targeted outreach programs for all users and staff covering various areas of cyber incidents
        - Technical planning and process review
        - IT/Cyber Security cross training and engagement

4. **What federal, state, or local cyber regulations is your area beholden to currently?**
    - **National Incident Management System (NIMS)**: A comprehensive, national approach to incident management that is applicable at all jurisdictional levels and across functional disciplines.
    - **Emergency Management Accreditation Program (EMAP)**: A set of 64 professional emergency management standards designed as a tool for continuous improvement as part of a voluntary accreditation process for local, state, federal, higher education and tribal emergency management programs.
    - **National Fire Protection Association (NFPA) Standard 1600 - Disaster/Emergency Management and Business Continuity/Continuity of Operations Programs**: A common set of criteria for all hazards disaster/emergency management and business continuity programs.

- **Centers for Medicare and Medicaid Services (CMS) Emergency Preparedness Rule:** Establishes national emergency preparedness requirements for healthcare entities to ensure adequate planning for both natural and man-made disasters, and coordination with federal, state, tribal, regional and local emergency preparedness systems.
- **The Joint Commission Emergency Management Standard:** Healthcare accreditation standards outlining program requirements for preparedness, mitigation, response, and recovery phases of emergency management.
- **Presidential Policy Directive (PPD) 41 – U.S. Cyber Incident Coordination:** This directive sets forth principles governing the Federal Government's response to any cyber incident, whether involving government or private sector entities**.**
- **Health Insurance Portability and Accountability Act (HIPAA) Security Rule:** Federal information security requirements put in place to safeguard individuals' electronic protected health information.
- **Homeland Security Exercise Evaluation Program (HSEEP):** Provides a set of guiding principles for exercise programs, as well as a common approach to exercise program management, design and development, conduct, evaluation, and improvement planning.
- **United States Computer Emergency Readiness Team (US-CERT):** Organizations within the U.S. Department of Homeland Security tasked with providing cyber incident prevention, protection, preparedness, response, and recovery capabilities to federal, state, local, and tribal government agencies.
- **State Law Title 10**
- In a meeting and conference call conducted on December 12, 2017 to discuss these questions, the Work Group did not provide a list of federal, state or local cyber regulations, but instead, asked that the following authorities, as listed in the State of Indiana's Cyber Emergency Response Annex, be reviewed for accuracy and completeness:
    - **Federal**
        - The National Cyber Incident Response Plan (NCIRP)
        - National Response Framework (NRF)
        - The National Incident Management System (NIMS) Homeland Security Act of 2002
        - Homeland Security Presidential Directive
        - Robert T. Stafford Disaster Relief and Emergency Assistance Act, as amended. 42 United States Code 5121, et seq.
        - Code of Federal Regulations. Title 44, Part 205 and 205.16.
        - Buckle, Philip. (1999). "Re-defining Community and Vulnerability in the Context of Emergency Management." Australian Journal of Emergency Management (Summer): 21-26.
        - Guidance on the National Incident Management System (March 2008)
        - Guidance on the National Preparedness Goal (September 2007)
        - National Strategy to Secure Cyberspace, February 2003
        - National Cyber Incident Response Plan, Interim Version, September 2010

        - Cyber Incident Annex, National Response Plan, December 2004
        - Strengthening Regional Resilience through National, Regional, and Sector Partnerships, National Infrastructure Advisory Council (2013)
        - DoD Strategy for Operating in Cyberspace (DSOC), July 2011
        - Cyber Security Framework Strategy For the State of Indiana, 2009
    - **State**
        - Indiana Code 10-14-3, Emergency Management and Disaster Law
        - A Leader's Guide to Emergencies and Disasters, IDHS (September 2008)
        - Executive Order 13-09, January 2013
    - **Local**
        - County/Local Emergency Management Ordinances

5. **What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?**
    - 12 DHS CI Sector Specific Plans
    - Memo and report of benchmark research of other state response plans
    - 19 specific State Incident Response Plans/strategies
    - Indiana Crit-Ex reference documents and reports
    - Indiana Comprehensive Emergency Management Plan
    - Personnel present and those who called into the meeting were asked to provide information or previous cyber incidents or case studies to be included with this report.

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.**
    - Other State Incident Plans
    - National Governors Association State Studies
    - IDHS Advancing Cybersecurity Initiatives for the State of Indiana Roadmap
    - Preparedness Cycle Implementation Presentation – Indiana
    - IDHS Cyber SmartBook
    - Personnel present and those who called into the meeting were asked to provide information or previous incident to support the group's deliverables.

7. **What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?**
    - See references for other state cyber plans and incident plans.
    - See above – Item #1

8. **What does success look like for your area in one year, three years, and five years?**
    - Conduct review of the Cyber Annex to State of Indiana Comprehensive Emergency Management Plan.
    - Draft recommendations for revisions to the Cyber Annex and development of a coordinating entity within the Indiana State Emergency Operations Center.

- Develop threat assessment, planning, training, and exercise document templates for local government and small businesses.
- Create guidance for coordination of local government, private sector, and state government cybersecurity drill and exercise activity.
- Develop “tabletop toolkits” with IDHS exercise support, including a cyber TTX, for local partners.
- Exercise Cyber Incident Response Annex to identify gaps.
- Develop the Statewide Cybersecurity Strategic Plan within the Cybersecurity Council.
- Determine future Crit-Ex direction.
- In a meeting and conference call conducted on December 2017 to discuss these questions, the Work Group described success over the short- and long-term as having the following factors:
    - Significant reduction or elimination of cyber incident in all critical sectors within the State of Indiana
    - The ability to effectively target and protect against new and emerging cyber threats
    - Make cyber response exercises a continual and frequent tool to validate and show improvement in the state’s overall capability to meet cyber threats head on

9. **What is the education, public awareness, and training needed to increase the State’s and your area’s cybersecurity?**
    - An abundance of cybersecurity information and services are available to individuals, government agencies, and private sector organizations.
    - There is no central point of coordination and information sharing for state-level cybersecurity planning, training, and exercise activity.
    - In a meeting and conference call conducted in December 2017 to discuss these questions, the Work Group provided the following as key in promoting public awareness and understanding of cyber incidents:
        - Having cybersecurity messaging and outreach directed toward the general public, similar to the US Department of Homeland Security’s “See Something, Say Something” program
        - General and frequent Public Service Announcements (PSAs) targeting specific sectors and portions of the populations, providing tips and considerations for lessening or eliminating cyber threats and incidents
        - Developing and targeting education and cybersecurity training for public safety warning points and dispatch centers as a means to meeting the needs of first responders

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?**
    - Workforce in this area is focused on training emergency managers, departments, etc.
    - No clear answers given for this question from the group – Each member was asked to provide their answers individually.

11. **What do we need to do to attract cyber companies to Indiana?**
    - In a meeting and conference call conducted on December 2017 to discuss these questions, the Work Group provided the following items to address how we can attract cyber companies to Indiana:
        - Involve Workforce Development in targeting and highlighting jobs in the field, while also offering training and job skill support
        - Working with private and public universities and colleges within the state to expand and enhance degree programs to target cyber processes, threat reduction, and innovation

12. **What are your communication protocols in a cyber emergency?**
    - Indiana is in the process of finalizing it state Cyber Annex.
    - Personnel present and those who called into the meeting were asked provide information on their organization's communications protocols for a cyber emergency.

13. **What best practices should be used across the sectors in Indiana? Please collect and document.**
    - Existing national standards and best practices for emergency preparedness and all-hazard incident management are applicable to cybersecurity initiatives.
    - The basic concepts for emergency planning, training, exercise, evaluation, and improvement can be implemented as the foundation for cybersecurity preparedness programs.
    - Personnel present and those who called into the meeting were asked to provide information on best practices for their specific sector to identify, lessen or eliminate cyber threats and incidents.

Deliverable: Annex

Deliverable: Annex

General information

1. **What is the deliverable?**
   a. Finalize IDHS Cyber Annex to CEMP

2. **What is the status of this deliverable**?
   a. In-progress; 75% 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. Complete the IDHS Cyber Annex

6. **What metric or measurement will be used to define success?**
   a. Annex to be completed and finalized with all the parties who are required to sign off on it per IDHS CEMP internal requirements.

7. **What year will the deliverable be completed?**
   a. 2018

8. **Who or what entities will benefit from the deliverable?**
    a. Emergency response agencies and partners

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. This is an annex to the State of Indiana's CEMP produced and executed by IDHS during declared emergencies.

Additional Questions

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

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. IDHS, Indiana State Police (ISP), Indiana National Guard (INNG), Indiana Office of Technology (IOT), 911 Board, and Governor's office.

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

13. **What are the expected challenges to completing this deliverable?**
    a. Ensuring that once finalized that the annex is exercised appropriately before an emergency occurs.

Implementation Plan

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

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Review Annex from IDHS – Preliminary review with key stakeholders	Cybersecurity Program Director/IDHS/IOT/ISP/INNG	100%	2017	
Rewrite Annex	Cybersecurity Program Director and Emergency Services and Exercise Working Group leads	100%	July 2018	
Working Group Review	Emergency Services and Exercise Working Group	100%	September 2018	
Committee Review	Government Services Committee	0	October 2018	
Finalize Annex	IDHS	0	November 2018	
Distribute/Communicate Annex to key stakeholders	IDHS	0	December 2018	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No

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

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

Benefits and Risks

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

a. Greatest benefit is to provide an operational framework that can guide response activity across multiple agencies, government, and private organizations.

18. **How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?**
    a. By a coordinated effort, the annex will allow private, public, and government organizations to respond to cyber emergencies efficiently and effect in a more coordinated fashion; therefore, reducing the potential for cybersecurity risk or possible impact.

19. **What is the risk or cost of not completing this deliverable?**
    a. The lack of coordination and possible mass confusion during a cyber emergency can increase the cybersecurity risk and negative impact on affected critical infrastructures and Indiana.

20. **What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?**
    a. Completion of annex and testing that it is an operational plan.

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. The National Governor's Association and FEMA identified several other states who have a cyber annex.

22. **Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?**
    a. Yes
    b. **If Yes, please list states/jurisdictions**
        i. The National Governor's Association and FEMA identified several other states who do not have a cyber annex.

Other Implementation Factors

23. **List factors that may negatively impact the resources, timeline, or budget of this deliverable?**
    a. Approval and consensus of all the functions of Indiana's CEMP Cyber Annex may be difficult among key stakeholders.

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. To review the Annex every 2-3 years and after a real-world incident.

26. **Who has the committee/working group contacted regarding implementing this deliverable?**
    a. N/A

27. Can this deliverable be used by other sectors?

a. Yes

b. **If Yes, please list sectors**

i. All critical infrastructure sectors

Communications

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

a. Appropriate contacts within the critical infrastructure sectors, key emergency management stakeholders, key state agencies executives, Governor's office, enforcement agencies.

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

a. No

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

a. The CEMP's Cyber Annex is meant to be an internal document and shared with those who are a "need to know" basis only.

Evaluation Methodology

Objective 1: IDHS will develop and distribute the IDHS CEMP Cyber Annex to appropriate parties by December 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: IDHS will exercise the IDHS CEMP Cyber Annex by December 2019.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group

☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☒ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: IDHS Exercise Engagement

Deliverable: IDHS Exercise Engagement

General information

1. **What is the deliverable?**
    a. IDHS Cyber Exercise Engagement Program

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

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

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

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. IDHS Cyber Exercise Engagement Program to be used by public, private, military, and government sectors so that state response can be realistically incorporated into cyber exercises being conducted throughout the State of Indiana.

6. **What metric or measurement will be used to define success?**
    a. Stakeholders are made aware of the completed program and use it.

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

8. **Who or what entities will benefit from the deliverable?**
    a. Public, private, military, and government sectors

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. None

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. None at this time.

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. None at this time.

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

13. **What are the expected challenges to completing this deliverable?**
    a. Completing with current IDHS resources and communicating the new program to stakeholders who would benefit. Once stakeholders begin using program there may be limitations on how much exercising IDHS can participate in.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing/sustained effort – it will need to continue to be updated and

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Review and Finalize Cyber Annex	Cybersecurity Program Director/IDHS/IOT/ISP/INNG	100%	2018	
Create internal Cyber Exercise Engagement Program Planning team	IDHS	0	March 2019	
Create Cyber Exercise Engagement Program	IDHS	0	July 2019	
Develop Cyber exercise based on annex and risk profile	IDHS	0	Fall 2019	
Conduct Cyber exercise based on annex and risk profile	IDHS	0	December 2019	

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
One FTE	One FTE	EM with cyber-focused planning background	EMPG/SHSP Grant funding		Already exists in IDHS budget. Other IDHS staff assist in creating the workshops, toolkit support, and sustainability

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
Printing cost	Cyber Workshops	$1000.00	TBD	EMPG		2019 Proposal needed
Travel Costs	Cyber Workshops		TBD	EMPG		

Benefits and Risks

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

a. The Exercise Engagement Group will allow government entities, businesses, and related nonprofits to partner together and exercise to a more unified and cost-effective response to a cyber incident, improving all preparedness capabilities.

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

a. Governments (state and local level), small businesses and other partners will be more prepared for a cyber incident response will reduce the cybersecurity risks to the State of Indiana and possible impacts during a cyber emergency.

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

a. No cost. Rather, not having a reviewed, trained, and exercised a cyber incident response plan can have a high impact not only on the effective response capability of the State of Indiana but can cause longer than expected disruption to the business or local government.

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

a. Completion of deliverable and meeting key milestones will be one measure of success. Timeline, scope of delivery, and quality of product are key measures.

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 – at varying levels. Requires more research and decision-making by working group.

b. **If Yes, please list states/jurisdictions**

   i. [No Response]

22. **Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?**
    a. No

Other Implementation Factors

23. **List factors that may negatively impact the resources, timeline, or budget of this deliverable?**
    a. The timeline and completion of the cyber annex drives the next steps in the planning, training, and exercise process. In addition, staff, monetary resources, or administrative priorities could change or slow the timeline of the project down.

24. **Does this deliverable require a change from a regulatory/policy standpoint?**
    a. No
    b. **If Yes, what is the change and what could be the fiscal impact if the change is made?**
        i. Perhaps a change in internal (IDHS) project/policy priorities but no regulation or statutory changes.

25. **What will it take to support this deliverable if it requires ongoing sustainability?**
    a. A review and update of the exercise based on feedback and emerging threats and technology will need to be considered regularly due to changes in the risk profile and ever-changing cyber culture. Additionally, workshops and training should be improved upon, further developed, and made available throughout the state to increase its use and effectiveness.

26. **Who has the committee/working group contacted regarding implementing this deliverable?**
    a. IDHS Executive Director Bryan Langley

27. **Can this deliverable be used by other sectors?**
    a. Yes
    b. **If Yes, please list sectors**
        i. Public (all levels, mostly local), private, nonprofit, other nongovernmental

Communications

28. **Once completed, which stakeholders need to be informed about the deliverable?**
    a. IECC members, local government, business associations, emergency management professionals, state and federal partners.

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. TBD at a later date.

Evaluation Methodology

Objective 1: IDHS will develop and launch Cyber Exercise Engagement Program by July 2019.

Type: ☒ Output ☐ Outcome

Evaluative Method:

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

Deliverable: Emergency Operations Center (EOC)

Deliverable: EOC

General information

1. **What is the deliverable?**
    a. Indiana State Emergency Operations Center Cyber Coordination procedures and implement the process of how the state responds to a cyber emergency, with guidance from the Cyber Emergency Response Annex to the Comprehensive Emergency Management Plan.

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

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**

    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☐ Strengthen best practices to protect information technology infrastructure.
    ☒ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**

    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☒ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Develop a coordinating entity within the Indiana State Emergency Operations Center

6. **What metric or measurement will be used to define success?**
    a. Complete the product

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

8. **Who or what entities will benefit from the deliverable?**
   a. Emergency management partners, sector partners, government partners

9. **Which state or federal resources or programs overlap with this deliverable?**
   a. N/A

Additional Questions

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

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. IDHS, ISP, IOT, INNG, IECC

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

13. **What are the expected challenges to completing this deliverable?**
    a. Ensuring that all those who would benefit from using this EOC coordinating procedure is aware of it and making sure it is exercised appropriately before an emergency occurs.

Implementation Plan

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

Tactic Timeline

Tactic	**Owner**	**% Complete**	**Deadline**	**Notes**
Create/Update Org Charts	State EOC		CERA completion + 30 days	
Create SOPs	State EOC		CERA completion + 30 days	
Create duty descriptions	State EOC		CERA completion + 30 days	
Identify Players	Chetrice Mosely/Director Langley		CERA Completion +30 days	
Conduct training	State EOC		CERA completion + 60 days	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No

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

Estimated Initial FTE	**Estimated Continued FTE**	**Skillset/Role**	**Primary Source of Funding**	**Alternate Source of Funding**	**Notes**
N/A – no additional IDHS staff; perhaps additional physical seat or workspace		EOC Training/ leverage existing skills			

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

a. None

Resource	**Justification/ Need for Resource**	**Estimated Initial Cost**	**Estimated Continued Cost, if Applicable**	**Primary Source of Funding**	**Alternate Source of Funding**	**Notes**
N/A						

Benefits and Risks

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

a. Formalized organization and training of personnel in anticipation of a cyber emergency.

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

a. Impact could be reduced by having a prepared, coordinated response. There will be mutual understanding between responders, which will increase efficiency.

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

a. Risking uncoordinated response, delayed acquisition of resources, general lack of understanding during an incident.

20. **What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?**
    a. Success will be defined by the effectiveness of a response. Because of the difficulty in quantifying success, qualitative data must be utilized, primarily through opinions derived by after action reports. These reports will indicate what portions of a response went well and what did not.

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. Michigan, Arizona, Maryland

22. **Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?**
    a. Yes
    b. **If Yes, please list states/jurisdictions**
        i. There are certainly some jurisdictions that lack a formal cyber incident response plan, but determining the consequence of no plan may prove difficult

Other Implementation Plan

23. **List factors that may negatively impact the resources, timeline, or budget of this deliverable?**
    a. The timeline and Completion of the cyber annex drives the next steps in the planning, training, and exercise process. In addition, staff, monetary resources, or administrative priorities could change or slow the timeline of the project down.
    b. Lack of support for the CERA may delay delivery.

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. A review and update of the exercise based on feedback and emerging threats and technology will need to be considered regularly due to changes in the risk profile and ever-changing cyber culture. Additionally, workshops and training should be improved upon, further developed, and made available throughout the state to increase its use and effectiveness.

26. **Who has the committee/working group contacted regarding implementing this deliverable?**
    a. IOT, ISP, and INNG have been partners in the development of the CERA.

27. Can this deliverable be used by other sectors?

a. Yes

b. **If Yes, please list sectors**

  i. Any sector; using the documents as templates and guidance for organizing a response to a cyber incident. This can guide other sectors as to who is responsible for what within state government, and each sector can adjust their plans accordingly.

Communications

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

a. Any stakeholder with responsibility outlined in the plan.

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

a. No

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

a. TBD at a later date.

Evaluation Methodology

Objective 1: IDHS will develop a Cyber Liaison position within Emergency Operations Center by May 2019.

Type: ☒ Output ☐ Outcome

Evaluative Method:

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

Objective 2: IDHS will complete training and exercise the Cyber Liaison position within the EOC by December 2019.

Type: ☐ Output ☒ Outcome

Evaluative Method:

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

Deliverable: Toolkit

Deliverable: Toolkit

General information

1. **What is the deliverable?**
   a. Develop a Cyber Incident Planning and Preparedness Toolkit for Emergency Managers that is compliant with FEMA, USDHS, and NIST. *See NGA Policy Academy Notes for further details.*

2. **What is the status of this deliverable?**
   a. In-progress; 50% 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. Emergency Managers treat each cyber incident like any other hazard. Assist stakeholders with developing, planning, and preparing for a cyber incident.

6. **What metric or measurement will be used to define success?**
   a. Completion of the toolkit and providing it to stakeholders

7. **What year will the deliverable be completed?**
   a. Version 1 – 2018
   b. Version 2 – 2019

8. **Who or what entities will benefit from the deliverable?**
    a. Stakeholders include local government, small businesses, and state agencies

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. State preparedness report, federal grant programs, and Hazard Identification and Risk Assessment (HIRA). More information about the HIRA can be found at https://www.in.gov/dhs/3879.htm.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Not currently.

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. IECC working groups and partners

12. **Who should be main lead of this deliverable?**
    a. IECC Emergency Services and Training Working Group to develop
    b. State of Indiana to promote
    c. IDHS to provide support and subject matter expertise in assisting with training and exercising among local government/EMAs

13. **What are the expected challenges to completing this deliverable?**
    a. Ensuring that those who want to use the toolkit can receive assistance, guidance, and training in using the toolkit.

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
Gather current resources and templates for incident response toolkit	Joe Romero	100%	June 2018	
Create toolkit – version 1	Joe Romero and Carlos Garcia	75%	October 2018	
Develop cyber workshops	IDHS	0	January - August 2019	
Conduct cyber workshops	IDHS	0	October 2019	
Develop cyber risk profile tool and toolkit 2.0	Joe Romero, Carlos Garcia, Cybersecurity Program Director	15%	August 2019	National Governors Association Project (see supporting documentation)
Develop cyber incident workshops plan	IDHS	0	August – December 2019	
Conduct Cyber incident workshops	IDHS	0	March 2020	
Make improvements to toolkit	IDHS	0	August 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
0.5 FTE	0.5 FTE	Emergency Management	State of Indiana	N/A	IDHS to assist in creating the workshops, toolkit support, and sustainability

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
N/A						

Benefits and Risks

17. **What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)**
    a. The toolkit will provide a user template planning documents geared towards small businesses and local government entities that may not have the financial resources or personnel to develop complex response plans and training programs.

18. **How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?**
    a. Small businesses and local governments being more prepared for a cyber incident response will reduce the cybersecurity risks to the State of Indiana and possible impacts during a cyber emergency.

19. **What is the risk or cost of not completing this deliverable?**
    a. Not having a cyber incident response plan due to lack of financial resources or personnel can have a high impact not only on the effective response capability of the State of Indiana but can cause longer than expected disruption to the business or local government.

20. **What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?**
    a. Completion of deliverable and meeting key milestones will be one measure of success. End-user success in effectively using the toolkit will be an additional measure of success.

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. Small Business Administration, Federal Communications Commission (FCC), and FEMA have templates to use in incident response planning.

22. **Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?**
    a. Yes
    b. **If Yes, please list states/jurisdictions**
        i. While there are planning resources from ISACs and FEMA, there are not any comprehensive planning toolkits created by other states to this degree that could be found geared to small businesses and local government that does not have a high knowledge in information technology and emergency management.

Other Implementation Factors

23. **List factors that may negatively impact the resources, timeline, or budget of this deliverable?**
    a. The risk profile tool may not be complete due to resources by the first year, but can certainly be completed in year two of the IECC.

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. A review of the toolkit based on feedback and emerging threats and technology will need to be considered annually. Additionally, workshops and training should be made available throughout the state to increase its use and effectiveness.

26. **Who has the committee/working group contacted regarding implementing this deliverable?**
    a. Have contacted Purdue regarding risk assessments and IU Health Chief Information Security Officer (CISO) regarding specific cyber risks.

27. **Can this deliverable be used by other sectors?**
    a. Yes
    b. **If Yes, please list sectors**
        i. All

Communications

28. **Once completed, which stakeholders need to be informed about the deliverable?**
    a. IECC members, local government, business associations, emergency management professionals, state and federal partners

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

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

a. None as of now.

Evaluation Methodology

Objective 1: IECC Emergency Services and Exercise Working Group will develop a Cyber Response Toolkit 1.0 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: IDHS will launch four workshops throughout Indiana using the Cyber Response Toolkit by December 2019.

Type: ☐ Output ☒ Outcome

Evaluative Method:

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

Objective 3: Partnering with the National Governors Association, the IECC Emergency Services and Exercise Working Group will develop a Cyber Response Toolkit 2.0 with a cyber risk tool for emergency personnel by August 2019.

Type: ☒ Output ☐ Outcome

Evaluative Method:

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

Objective 4: IDHS will develop and launch four workshops throughout Indiana using the Cyber Response Toolkit 2.0 by March 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

Supporting Documentation

Supporting Documentation

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

- 2015 Advancing Cybersecurity Initiatives for the State of Indiana: A Strategic Roadmap
- Crit-Ex 16.1
- Crit-Ex 16.2
- National Governors Association – Workshop Cyber Toolkit Materials – August 2018

Indiana Department of Homeland Security (IDHS)

Advancing Cybersecurity Initiatives for the State of Indiana: A Strategic Roadmap

April 2018

INDIANA DEPARTMENT OF HOMELAND SECURITY

Advancing Cybersecurity Initiatives for the State of Indiana: A Strategic Roadmap

PURPOSE

This document establishes a common operating picture of previous and current public and private sector cybersecurity activity and serves as a roadmap for establishing a comprehensive cybersecurity strategy for the State of Indiana.

MISSION

Desired Cybersecurity Outcomes as Established by the Office of the Governor:

1. Develop and implement a state cybersecurity strategy.
2. Maintain a preparedness-based protective posture.
3. Pursue and enhance statewide cyber incident response capabilities.

BACKGROUND

Numerous, high-profile incidents involving security breaches and data theft from government agencies and large corporations illustrate the vulnerability that exists. Data breaches are, and will continue to be, a significant issue for both the public and private sector. While the theft of data and the resulting financial consequences affect government agencies, large corporations, and private citizens, a disturbing trend has begun to emerge in recent years. Industrial control systems, complex computer networks used to operate industrial production equipment and public utility infrastructure, have also come under attack in recent years.

Unlike intrusion into information technology systems, which results in the loss of data, the compromise of industrial control systems can allow attackers to take control of physical infrastructure and mechanical systems. This evolving threat puts complex manufacturing, energy infrastructure, water utilities, and petrochemical production systems at risk for attack. In 2012 alone, The U.S. Department of Homeland Security reported nearly 200 attacks on industrial control systems, 40% of which were against energy production and distribution systems.

The idea that the United States is facing a “Cyber 9/11” is at the forefront of homeland security discussion nationwide. Like the rest of the country, the State of Indiana has a short window of opportunity to prepare for a major cybersecurity incident that, if successful, could be as devastating as a major earthquake or tornado. At this time, however, the State lacks a comprehensive strategy for preventing, protecting, mitigating, responding to and recovering from cyber incidents affecting critical infrastructure, key resources, and essential services statewide.

Securing Indiana’s information technology infrastructure and industrial control systems is beyond the reach of any single entity. The diverse authorities, roles, and responsibilities of critical infrastructure stakeholders require a collaborative partnership that encourages unity of effort. The Indiana Department of Homeland Security (IDHS), Indiana Office of Technology (IOT), and the Indiana National Guard (INNG) are leading a statewide, collaborative effort involving government, private-sector, military, research, and academic stakeholders to enhance Indiana’s cybersecurity posture. It will be through this unique partnership that the State of Indiana will develop a strategic vision, consolidate and coordinate its efforts, and turn good ideas and policy into effective action.

SITUATION

Numerous local, state, and federal agencies, military and private-sector entities, universities, and research groups within the State of Indiana are actively pursuing cybersecurity initiatives. Though these individual efforts do enhance the level of cybersecurity, these improvements are often sector-specific and narrow in scope. The current threat environment requires a state-driven effort to synchronize independent cybersecurity programs into a coordinated and unified effort.

COMPLETED ACTIONS

- 2015 State Cybersecurity Reference Guide – Drawing from the 2009 Cybersecurity Strategy, this document provides an overview of national best practices, professional standards, and provides case studies of cybersecurity programs in other states.
- Comprehensive review of ISO 27000 Series standards, the National Institute of Standards and Technology (NIST) Cybersecurity Framework, applicable Presidential Policy and Homeland Security Presidential Directives, US DHS Cybersecurity Strategy for the Homeland Security Enterprise, and the National Infrastructure Protection Plan.
- Draft Indiana National Guard Cyber Incident Response Plan completed.
- “Cyber Shield” exercises successfully conducted by the Indiana National Guard.
- State Level Exercise 2017 scheduled at the Muscatatuck Urban Training Center (MUTC). Exercise scenario will be a coordinated cyber attack on public power and water utilities.
- IOT incident response protocols for state information networks are in place, as are IT disaster recovery procedures and secure off-site data centers.
- Management and oversight of joint public/private/military cybersecurity exercises has been transferred from the Indiana Chapter of Infragard to IDHS.
- Manager hired for the Security Operations Center, the first operational element of the Indiana Information Sharing and Analysis Center (IN-ISAC).

CURRENT ACTIONS

- Comprehensive Strategy for State Cybersecurity – Initial draft under development.
- Review and migration of IOT security protocols from ISO to NIST standards.
- Restructuring and re-purposing existing executive steering committee and core project team under IDHS leadership.
- Re-branding and re-launching of “CritX” cybersecurity exercise program.
- Identification and coordination of current State agency and private-sector stakeholder cybersecurity activity.
- Identification and outreach with subject-matter experts, policy makers, and executive leadership for inclusion in the State’s cybersecurity program governing and project management bodies.

FUTURE ACTIONS

-Short-Term Target Dates (3 to 6 months)

- Strategic roadmap document completed – August 1st, 2015
- Initial Draft - Preparedness framework completed – August 7th, 2015
- Initial Draft - Response protocol framework completed – August 14th, 2015
- Convene Cybersecurity Executive Steering Committee – August 2015
- Convene Cybersecurity Core Project Team – August 2015
- Initial Draft - Comprehensive Strategy for State Cybersecurity completed – September 1st, 2015
- Final Draft - Comprehensive Strategy for State Cybersecurity completed – October 1st, 2015
- Cybersecurity Awareness Month – October 2015
- IN-ISAC Promotional Launch – October 2015
- Cybersecurity Exercise Series Launch – October 2015
- Initial Draft – Cybersecurity and Information Assurance ESF Annex – December 2015

PROPOSED STRATEGIC INITIATIVES

1.0 GOVERNANCE - Establish an effective cybersecurity governance structure and strategic direction

- 1.1 State Cybersecurity Council
- 1.2 Cybersecurity Core Team
- 1.3 Project Working Groups

Maintaining an evolved cybersecurity posture requires a multi-level governance structure. A Core Team comprised of representatives from government, military and private-sector organizations will keep apprised of changes in the cyber ecosystem, ensure the continued viability of the State strategy, and designed forward-thinking programs and initiatives. It will operate at the direction of the executive-level Cybersecurity Council, which will also act as the implementing arm of policy proposed by the Core Team. Supporting working groups will manifest on an as-needed basis to supply subject-matter expertise on specific issues, such as Private-Sector Engagement, Risk Analysis, and Industrial Control Systems.

2.0 INTEGRATION – Formalize strategic cybersecurity partnerships

- 2.1. Define State, FBI, INNG, DHS, ISP, and private-sector roles and responsibilities
- 2.2. Assess & integrate capabilities
- 2.3. Align goals and objectives

Convene sector-specific representation to define individual roles for cyber emergency management and solicit ongoing input. Cybersecurity Council and Core Team membership will reflect a commitment to integration across agencies, sectors, jurisdictions, and levels of government. This approach relies on the expertise of state, local and federal government agencies; the Indiana National Guard; academic and research; critical infrastructure stakeholders; and the private sector.

3.0 PREPAREDNESS - Strengthen best practices through effective prevention, protection & mitigation

- 3.1. Establish state agency cybersecurity policies, standards, and key performance indicators
- 3.2. Establish and communicate best practices to external public and private sector stakeholders
- 3.3. Effectively coordinate and conduct planning, training, and exercise activity

A key strength of the State's cybersecurity strategy will be the best practices and tools it offers to stakeholders in order to yield a more robust preparedness posture. IOT has defined key performance indicators for departments in the State Executive branch using NIST and ISO27000. IDHS will use these metrics to draft a formal Preparedness Doctrine for to determine key performance indicators for State agencies. Information hygiene practices, network and system assessments, and decision-making will comprise areas of special scrutiny.

Concurrent preparedness and possible legislative activities which will focus on gaining private sector support may also require the State to develop market incentives. The purpose of these incentives would be to motivate companies to adopt additional security practices, request technical support from external sources, and join information-sharing groups.

4.0 RESPONSE – Build and maintain robust statewide cyber incident response capabilities

- 4.1. Refine and enhance internal response protocols for incidents involving state government systems and networks.
- 4.2. Develop and maintain effective multi-agency cyber incident response plans that outline how the State will respond to major attacks on public and private sector information technology networks and industrial control systems.
- 4.3. Coordinate the development and deployment of cyber incident response teams and other deployable resources.

The State of Indiana must be able effectively respond to cybersecurity incidents, regardless of the size, scope, complexity, and the target of attack. Building upon existing IOT response protocols, an expanded response plan for significant cyber incidents will be developed to address breaches of state government networks. The formal development of a cybersecurity Emergency Support Function will detail the roles of lead, coordinating, and supporting agencies active during the response to a major incident.

5.0 INFRASTRUCTURE – Bridge the gaps between people, technology, and resources

- 5.1. Develop, maintain, and enhance the capabilities and functionality of the IN-ISAC.
- 5.2. Establish a public-facing cybersecurity website that serves as a clearinghouse for information.
- 5.3. Engage in statewide cyber infrastructure mapping.

The priority of the State is to build and expand systems and network solutions that support the five mission areas of prevention, protection, mitigation, response, and recovery. As well as the corresponding NIST Function Areas. Technology is only part of the solution. Human factors are key components of any cybersecurity effort. Education and public outreach programs focused on improving individual behavior and information security practices are essential to any successful strategy implemented by the State.

6.0 ECONOMIC OPPORTUNITIES – Leverage business and economic opportunities related to information, critical infrastructure, and network security

- 6.1. Launch an aggressive public information campaign to promote State cybersecurity initiatives.
- 6.2. Promote the use of the Muscatatuck Urban Training Center and Camp Atterbury as a cyber training ranges to regional, national, and international stakeholders.
- 6.3. Leverage the considerable technological resources of state universities and Indiana-based corporations to develop next-generation cybersecurity initiatives and attract investment.

Public and private organizations within the State should be as optimistic about the continued growth of cybersecurity efforts as they are concerned about attacks. Indiana's cybersecurity workforce can look forward exponential growth and opportunity – *if* the State cultivates conditions that train and retain skilled workers, attracts investment, and secures a competitive advantage for cybersecurity companies. Promotion of Indiana's cybersecurity initiatives will produce a synergy to ensure the growth of information security businesses and facilities. These initiatives can also support a wide variety of skilled jobs for Hoosiers, and strengthen a culture of preparedness that is critical for the State.

The Muscatatuck Urban Training Center's potential as a "cyber range" is also drawing interest from US DHS, which is considering MUTC as a federal training facility for cybersecurity. Today, the State has an unprecedented opportunity to leverage the "cyber problem" and emerge as a leader in innovative approaches to cybersecurity policy and practice — thereby serving the State's public safety interests while also attracting investment and promoting economic growth.

Indiana Department of Homeland Security (IDHS)

Crit-Ex 16.1

March 2016

Crit-Ex 2016

Cyber-Power Disruption Tabletop Exercise

Situation Manual

March 2016

This Situation Manual (SitMan) provides exercise participants with all the necessary tools for their roles in the exercise. Some exercise material is intended for the exclusive use of exercise planners, facilitators, and evaluators, but players may view other materials that are necessary to their performance. All exercise participants may view the SitMan.

Preface

The Crit-Ex 2016 Series 1 Tabletop Exercise (TTX) is sponsored by the Indiana Department of Homeland Security (IDHS), Indiana Office of Technology, and the Indiana National Guard. This Situation Manual (SitMan) was produced with input, advice, and assistance from the Crit-Ex 2016 Series 1 TTX Planning Team, which followed guidance set forth by the U.S. Department of Homeland Security (DHS) Homeland Security Exercise and Evaluation Program (HSEEP).

This SitMan provides exercise participants with all the necessary tools for their roles in the exercise. It is tangible evidence of Indiana's commitment to ensure public safety through collaborative partnerships that will prepare it to respond to any emergency.

The Crit-Ex 2016 Series 1 TTX is an unclassified exercise. Control of exercise information is based on public sensitivity regarding the nature of the exercise rather than actual exercise content. Some exercise material is intended for the exclusive use of exercise planners, facilitators, and evaluators, but players may view other materials that are necessary to their performance. All exercise participants may view the SitMan.

All exercise participants should use appropriate guidelines to ensure proper control of information within their areas of expertise and protect this material in accordance with current jurisdictional directives. Public release of exercise materials to third parties is at the discretion of IDHS and the Crit-Ex 2016 Core Team and Steering Committee.

Handling Instructions

1. The title of this document is Crit-Ex 2016 *Series 1 Tabletop Exercise (TTX) Situation Manual (SitMan).*

2. Information gathered in this SitMan is designated as For Official Use Only (FOUO) and should be handled as sensitive information that is not to be disclosed. This document should be safeguarded, handled, transmitted, and stored in accordance with appropriate security directives. Reproduction of this document, in whole or in part, without prior approval from IDHS is prohibited.

3. Given the scenario, topics and personnel involved in the Crit-Ex Tabletop Exercise, some of the discussion topics may necessitate restrictions. While this exercise is engineered to elicit productive dialogue on capabilities, not vulnerabilities, conversation may touch on issues with implications for local, state, or national security. This may include unclassified information about an organization's operations, the unauthorized disclosure of which could adversely impact a public safety or welfare, the effectiveness of the organization's critical operations programs, or other operations essential to state or national interest.

4. At a minimum, the attached materials will be disseminated strictly on a need-to-know basis and, when unattended, will be stored in a locked container or area that offers sufficient protection against theft, compromise, inadvertent access, and unauthorized disclosure.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Exercise Overview

Exercise Name	Crit-Ex Cyber-Power Disruption Tabletop Exercise
Exercise Date, Time, and Location	March 3, 2016 10AM – 4PM Camp Atterbury, Indiana
Scope	This exercise is a facilitated tabletop exercise, planned for 6 hours. The exercise is intended to facilitate discussion surrounding cyberattack response, energy disruption response, and other issues related to the mitigation of a wide-scale power outage.
Mission Area(s)	Mitigation, Response & Recovery
Core Capabilities	Operational Coordination; Operational Communications; Information Sharing
Objectives	1. Discuss the ability to establish and maintain a unified and coordinated operational structure and process that integrates all critical stakeholders during a power outage. 2. Discuss the ability to communicate information in support of security, situational awareness, and operations by all means available, within the area of operations and among all response forces during a power outage. 3. Discuss the ability develop and maintain a common operating picture throughout the duration of a power outage by providing timely, accurate, and actionable information, intelligence, data, or knowledge among government and private-sector entities, as appropriate.
Threat or Hazard	Cyberattack Vector: Control Systems Malware
Scenario	A state-sponsored terrorist group executes a coordinated cyberattack on several power facilities throughout Indiana, resulting in a widespread and prolonged power outage.
Sponsor	Indiana Department of Homeland Security
Participating Organizations	Approximately 25 participating organizations and 35 players from the Indiana Department of Homeland Security; Indiana Office of Technology; Indiana National Guard; Indiana Utility Regulatory Commission; Indiana State Police; local Emergency Management Agencies; Water/Wastewater Utilities; Power Utilities. For a full list of participating organizations, see Appendix B.

Points of Contact

David Kane
Executive Director
Indiana Department of Homeland Security
302 W. Washington St., E208
Indianapolis, IN 46254
dkane@dhs.in.gov

Jennifer de Medeiros
Emergency Services Program Manager
Indiana Department of Homeland Security
302 W. Washington St., W246
Indianapolis, IN 46254
(317) 452-0380
jdemedeiros@dhs.in.gov

James McHugh
Infrastructure Protection Program Manager
302 West Washington Street, Room W246
Indianapolis, IN 46204
317-473-0353
jmchugh@dhs.in.gov

MAJ Stacy Kennedy Barker
Deputy J7 Exercise and Training
2002 S. Holt Road
Indianapolis, IN 46241
Office: 317-247-3300 X73206

Additional Information

Crit-Ex planners have designed this exercise to focus on the coordination between critical infrastructure owners and operators and their local and state emergency management. The suggested audience includes jurisdictional emergency management partners and critical infrastructure owners and operators.

Contents

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

SECTION 1: GENERAL INFORMATION

Background

The idea that the United States is facing a "Cyber 9/11" is at the forefront of homeland security discourse. Like the rest of the country, Indiana has a short window of opportunity to prepare for a major cybersecurity incident that, if successful, could be as devastating as a major earthquake or tornado. The year 2015 has been groundbreaking for developing cross-sector partnerships, governance structure, and strategic programs necessary for preventing, protecting, mitigating, responding to and recovering from cyber incidents. The Indiana Department of Homeland Security (IDHS) has been working in close conjunction with the Indiana Office of Technology (IOT) and the Indiana National Guard (INNG) to lead a collaborative effort between government, private-sector, military, and academic stakeholders, as well as incorporating cyber research to enhance Indiana's cybersecurity posture.

Crit-Ex 2016 is the first of these cross-sector initiatives, designed for both the public and private sectors in order to improve understanding of cybersecurity posture and identify capability gaps. It will function as a series of tabletop and functional exercises that explore the intersection of cybersecurity and critical infrastructure, using scenarios in which a cyberattack on a critical asset leads to physical-world consequences. The project is designed to recur annually, allowing partners from different critical infrastructure sectors across Indiana to participate and improve their cyber defenses. This year's scenario will focus on power disruption response within the water/wastewater and power sectors, allowing participants to exercise their cybersecurity processes across all five phases of emergency management. As such, Crit-Ex 2016 will be a "first-of-its kind" project that catalyzes information sharing, training opportunities, partnerships, and response planning across the state.

Purpose

The purpose of this exercise is to:

- Increase the operational readiness of the local, state and federal partners to respond to a prolonged, wide-spread power outage caused by a cyberattack.
- Evaluate the ability of local, state and federal partners to identify and respond to cascading events in accordance with current policies, plans, and procedures if traditional communications are down.
- Identify successes, shortfalls, and areas for improvement in current policies, plans, and procedures.

Scope

This exercise emphasizes the role of local, state and federal agencies, water/wastewater utilities, and power utilities in response to a coordinated cyberattack that affects the entire State of Indiana.

Exercise Objectives & Core Capabilities

The following exercise objectives in Table 1 describe the expected outcomes for the exercise. The objectives are linked to core capabilities, which are distinct critical elements necessary to achieve the specific mission area(s). The objectives and aligned core capabilities are guided by elected and appointed officials and selected by the Exercise Planning Team.

Exercise Objective	Core Capability
1. Discuss the ability to establish and maintain a unified and coordinated operational structure and process that integrates all critical stakeholders during a power outage.	Operational Coordination
2. Discuss the ability to identify and maintain partnership structures among response elements to support situational awareness, mobilize critical resources, and establish coordination structures at the local, state, and national level.	Operational Coordination
3. Discuss the ability to communicate information in support of security, situational awareness, and operations by all means available, within the area of operations and among all response forces during a power outage.	Operational Communications
4. Discuss the ability to re-establish sufficient communications infrastructure within the affected areas to support critical services and transition to recovery.	Operational Communications
5. Discuss the ability to develop and maintain a common operating picture throughout the duration of a power outage by providing timely, accurate, and actionable information, intelligence, data, or knowledge among government and private-sector entities, as appropriate.	Information Sharing

Table 1. Exercise Objectives and Associated Core Capabilities

Participants

The term *participant* encompasses many groups of people, not just those playing in the exercise. Groups of participants involved in the exercise, and their respective roles and responsibilities, are as follows:

- **Players:** Players respond to the situation presented, based on expert knowledge of response procedures, current plans and procedures, and insights derived from training.

- **Observers:** Observers support the group in developing responses to the situation during the discussion; they are not participants in the moderated discussion period, however.

- **Facilitators:** Facilitators provide situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key Exercise Planning Team members also may assist with facilitation as subject matter experts during the TTX.

- **Evaluators:** Evaluators are assigned to observe and evaluate certain objectives during the exercise. Their primary role is to document player discussions, including how and if those discussions conform to written and established procedures.

- **Scribes:** Scribes are assigned to observe, listen, and record the participant discussions during the table group facilitated sessions.

Exercise Structure

This will be a multimedia, facilitated TTX. Players will participate in the following modules:

- **Module 1:** Incident Onset & Notification
- **Module 2:** Response
- **Module 3:** Recovery

Each module will begin with a multimedia update that summarizes key events occurring within that time period. After the updates, participants will review the situation and engage in functional group discussions of appropriate response issues. For this TTX, the functional groups are:

- Emergency Management
- Water/Wastewater Utilities
- Energy Utilities

After these functional group discussions, participants will engage in a facilitated caucus discussion in which a spokesperson from each group will present a synopsis of the group's actions based on the scenario.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Exercise Evaluation

Evaluation of the TTX is based on a set of objectives and Exercise Evaluation Guides (EEGs). Evaluators will be provided with EEGs for each of their assigned areas, and players will be asked to complete exercise evaluation forms. These documents, coupled with facilitator observations and notes, will be used to evaluate the exercise and compile the After Action Report (AAR).

Exercise Guidelines

- This TTX will be held in an open, low-stress, no-fault environment. Varying viewpoints, even disagreements, are expected.
- Respond on the basis of your knowledge of current plans and capabilities (i.e., you may use only existing assets) and insights derived from your training.
- Decisions are not precedent setting and may not reflect your organization's final position on a given issue. This exercise is an opportunity to discuss and present multiple options and possible solutions.
- Issue identification is not as valuable as suggestions and recommended actions that could improve response and preparedness efforts. Problem-solving efforts should be the focus.

Assumptions & Artificialities

In any exercise, assumptions and artificialities may be necessary to complete play in the time allotted. During this exercise, the following apply:

- The scenario as designed may not be catastrophic or coordinated enough to cause a power outage that affects all the organizations involved. However, it is the intent of the Exercise Planning Team to utilize a catastrophic scenario according to Homeland Security Exercise and Evaluation Program (HSEEP) standards to drive exercise discussion.
- Incident attribution may take longer than the scenario describes. However, productive discussion will hinge on knowing the attack source and vector.
- There is no hidden agenda, and there are no trick questions.
- All players receive information at the same time.

SECTION 2: EXERCISE SUMMARY & SCENARIO

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Module 1: Incident Onset & Notification

Date: Friday, January 15 – 5:00AM
Weather: Frigid winter weather. 15°F, 11 MPH winds NE

Over the course of several years, a hostile Nation State has sponsored individuals to work in electric generation facilities and control centers, where they had access to SCADA systems controlling both transmission and generation. These individuals have overcome the "air gap" (see Appendix) defense mechanisms by bridging the SCADA network and the business network. USB drives were used to install Remote Access Trojans (RATs) on all of the SCADA systems. The bridging laptops would then be used to connect to the RATs. The individuals now have remote control of both the generation SCADA system and the transmission SCADA system. Additional software was loaded that would erase evidence of the RATs.

At 5:00AM on January 15th, timed, coordinated cyberattacks are executed against these power facilities' generation control systems and transmission SCADA systems. These individuals begin opening breakers and changing generator setpoints to cause the generators to go into an overspeed condition and trip offline. The result is immediate power disruption across approximately 70% of the state, with outages extending outside state lines.

Within 30 minutes, cascading effects visibly impact the interdependencies of the facilities. Traditional communication lines are disrupted, including telecommunications and cell towers. Most of the state is blind to the coordinated nature of the incident and the extent of the outages.

Key Issues

- Indiana is experiencing a power loss that covers nearly 70% of the state and surrounding region.
- Throughout the powerless region, telecommunications circuits fail and/or are jammed.
- Power outage alarms alert water/wastewater facilities of the power outage.
- Not every jurisdiction is aware that a cyber-attack has caused this power outage and most are going through normal power outage recovery operations.

Questions

The following questions are provided as suggested general subjects. These questions are not meant to constitute a definitive list of concerns to be addressed, nor is there a requirement to address every question.

- What actions would your organization take initially? What are your organization's first priorities?
- Who is your first call? How do you identify your critical partners for a power outage?

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

- How would you contact partners outside the organization without traditional communications? Within the organization? What is the primary and alternate (backup) method to notify personnel about the status of your organization and its needs?
- How will the information presented in the scenario be shared? Who is contacted as part of the alert/notification process—are pre-identified key personnel notified, and are other State agencies notified?
  - Local Government, Police, Fire, Emergency Services, and trusted third parties?
  - State partners and/or agencies?
  - Federal partners and/or agencies?
- Based on your contact and alert procedures after an incident, do those match your mandated reporting requirements? Internal? Local, state, and federal levels of government? What specifically are your reporting requirements?
- How do you determine when and with whom to share sensitive and/or classified information about the event, including information about proprietary systems? What concerns or considerations do you have in coordinating with or discussing your situation with external entities?
- What are the backup power requirements for your agency? How long could you sustain operations from your primary facility on generators/backup power?
  - When was the last time these backup systems were checked and/or tested? (e.g., fuel, maintenance, etc.)
- What resources and capabilities are available to analyze or deal with the disruption? Do you have pre-defined cyber incident response teams? What external resources would you use?
- Based on the scenarios identified and from where you sit now, do you see any voids or vacuums in either the private and/or public sectors that should be better managed, enhanced, or filled? (e.g. "*I believe the state can do a better job of X, Y, and Z*" or "*I believe a sector does a poor job of prior planning regarding X, Y, and Z.*")

Related Objectives

- Assess the effectiveness of the organization's incident reporting and notification process.
- Determine how and how quickly utilities communicate with interdependent facilities, emergency management and government following an attack.
- Identify when intelligence and information is shared, and with whom.
- Identify available resources and resource request channels for a power outage.
- Explore the timelines and communication channels for power disruption incident management.
- Explore what polices and/or procedures are in place to identify a cyber-incident.
- Explore what policies and/or procedures are in place to react and mitigate a cyberattack

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Module 2: Response & Continuity of Operations

Date: Friday, January 15 – 9:00AM through Tuesday, January 19 – 5:00PM
Weather: Between 13°F and 25°F, depending on location

While conducting normal procedural recovery operations, IT personnel discover that malware has infected all forms of back up, preventing any restoration capabilities on those systems at this moment in time. By noon, a state-sponsored terrorist group claims responsibility for the cyberattack. State officials are now aware of the complexity surrounding the attack causing widespread outages over the region. State officials are now aware of the complexity surrounding this attack causing widespread outages over the region.

Some rural locations outside immediate downtown have power, but the certainty of that power maintaining is unknown. Many employees are stranded at home, unaware of the catastrophe caused by this cyberattack. Local counties conducting response operations are beginning to request government assistance, with heated shelters at the top of their list. Given the frigid winter temperatures, heat will become a life-dependent commodity along with food and water.

Water utilities are starting to feel the strain of the attack affecting their ability to provide service to its customers. The weather could have cascading effects on the water supply if the lack of power disrupts the ability of the utility companies to keep water from freezing. Within 24 hours, local fuel supplies will begin to dry up because of increased use for power generators. There are also signs of looting in the powerless regions, with the general public still unware of how serious the power outage is.

The private-sector operations dependent upon information technology and/or power have shut down or transitioned to alternate methods. Utility companies without proper continuity of operations plans are moving very slow in their transition to manual operations in an attempt to get the power back on.

Key Issues

- Power is still out in the downtown area and significant islanding around the state and region. Systems cannot be restored from backup.
- Terrorists have claimed responsibility for the cyberattack.
- Freezing temperatures pose a public safety issue and affect pipes.
- Communication issues plague the utility sector.
- Fuel availability for transportation and generators will become an issue in the immediate future.

Questions

The following questions are provided as suggested general subjects. These questions are not meant to constitute a definitive list of concerns to be addressed, nor is there a requirement to address every question.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

- How and with whom will this information be communicated?
- Does this information change your priorities? How? How will it affect your response operations? How would a law enforcement investigation impact your current operations?
- How does the attribution of a terrorist cyberattack change your priorities and courses of action?
- What types of sensitive information/intelligence need to be communicated outside your organization, and how will that be delivered?
- Does your organization have the resources it needs to respond to this cyberattack? How will you request more resources?
- What protective actions would you take across non-impacted systems or agencies?
  - Who is responsible for protective action decision-making?
  - How are actions coordinated across departments/agencies?
- What external resources would be needed to support the response and continue your mission-essential functions (MEFs) and primary mission-essential functions (PMEFs)?
- What mutual aid agreements does your organization partake in? Are processes in place to request government or third party resources? Do current mutual aid agreements or assistance request processes address power-disruption resources and staff?
- What if key personnel are unavailable due to lack of notification or inability to reach the facility? What is each entities alternate approach to staffing? Would this degrade your ability to perform MEFs?
- Does your entity have backup power-generation capabilities for an extended blackout period? If not, how will you address the issue? What other contingency plans are required to address an extended blackout period?
- How will you address public safety issues? With what agencies/entities will you coordinate?
- What plans, procedures, and/or agreements do you have in place to control resource distribution within and outside your jurisdiction?

Related Objectives

- Assess the effectiveness of the organization’s secondary communications capabilities.
- Examine the effectiveness of the organizations intelligence information-sharing protocols.
- Analyze the organization’s ability to coordinate with external organization to access resources to respond to the attack and power outage.
- Determine primary and alternate sources for response capabilities.
- Identify the second and third-order effects of a prolonged power outage both at the organization and its partners.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Module 3: Recovery

Date: January 20, 11:00AM ongoing
Weather: Between 17°F and 30°F, depending on location

ICS-CERT, SCADA incident response teams, and other private-sector cybersecurity experts have started to eradicate the malware from the control systems so that normal operations can continue. Private-sector critical infrastructure providers begin to restore service as quickly as possible, starting with the Indy Metro area. Providers with advanced planning efforts are able to restore service quicker than others, but some of the critical infrastructure requiring replacement is in limited supply. This depleted supply chain will have continuing affects resulting in limited power supply in certain regions of Indiana until the entire infrastructure is revived.

The local population is now aware of the cyberattack affecting power to their regions. Local law enforcement and emergency teams have been placed throughout the region, providing continual support to those who are still lacking power. Many people have been displaced during the power outage and will now need to be transported back to their dwellings. The terrorist group has continued to boast of their accomplishment on social media, warning that any region in the United States with similar industrial control networks will become a target in the future.

Key Issues

- Power and essential services are beginning to be restored.
- The governor has directed all agencies to return to normal operations
- Limited supply on critical infrastructure replacement parts and/or systems
- Many of the populace is still without power and/or been removed from their homes for safety reasons.
- Public opinion could swing negatively given the terrorist social media presence.

Questions

- Describe your role in post-incident recovery.
- At what point does your organization decide that it is in recovery mode? How would your organization support the transition back to a normal operating state?
  - How would you work with critical infrastructure providers to determine the incident is over?
- What processes or protocols are in place when contacting and/or working with law enforcement?
- How do you prioritize the allocation of critical infrastructure parts and/or systems? How are they distributed?
- Who are the essential personnel in a recovery mode? What are your organization’s key coordination points at this time?
- How do you prioritize where to allocate resources?
- What external resources would be needed to support the recovery? When do mutual aid compacts end?

- What external resources would be needed to support continuous recovery? Are processes in place to request government and/or third party resources? How would these resources be distributed?
- Describe the process for how your agency would capture mission-critical findings; lessons learned; shortfalls; and gaps in plans, policies, and procedures to improve COOP.
- How would you address any misinformation in the media?

SECTION 3: EXERCISE APPENDICES

Appendix A: Exercise Schedule

March 3, 2016 Time	Activity
9:15	Registration
10:00	Welcome & Opening Remarks
10:30	TTX Overview
10:45	Module One & Questions
10:55	Break-Out Sessions
11:45	Working Lunch & Module One Discussion
12:45	Module Two & Questions
12:55	Breakout Sessions
1:40	Module Two Discussion
2:00	Break
2:10	Module Three & Questions
2:20	Breakout Sessions
3:05	Module Three Discussion & Hotwash
3:50	Closing Remarks

Appendix B: Exercise Participants

Participating Organizations
Indiana Department of Homeland Security
Infragard Indiana
FEMA Region V
Indiana Office of Technology
Indiana Army National Guard
Indiana Utility Regulatory Commission
Indiana State Police
Allen County EMA
Bartholomew County EMA
Crawford County EMA
Montgomery County EMA
Vanderburgh County EMA
US Department of Homeland Security
Federal Bureau of Investigation
Michigan City Water
Evansville Water & Sewage
Fort Wayne Utilities
Citizens Energy Group
Vectren
Duke Energy
AES/Indianapolis Power & Light
NiSource/NIPSCO
Indiana Michigan Power Company
Rook Security
MISO
Pondurance

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

SECTION 4: INFORMATIONAL APPENDICES

The following section includes background and example information related to cybersecurity threats and attacks on the power grid.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Appendix C: Background Information

Air Gap

An air-gapped computer is one that is neither connected to the Internet nor connected to other systems that are connected to the Internet. Air gaps generally are implemented where the system or network requires extra security, such as classified military networks or industrial control systems (ICS) that operate critical infrastructure. To maintain security, ICS should only be on internal networks that are not connected to the company's business network, thus preventing intruders from entering the corporate network through the Internet and working their way to sensitive systems. A true air gap means the machine or network is physically isolated from the Internet, and data can only pass to it via a USB flash drive, other removable media, or a firewire connecting two computers directly.

Many companies insist that a network or system is sufficiently air-gapped even if it is only separated from other computers or networks by a software firewall. However, these firewalls can be breached if the code has security holes or if the firewalls are configured insecurely. Although air-gapped systems were believed to be more secure in the past, recent attacks involving malware that spread via infected USB flash drives have showcased vulerabilities. More recently, evidence has shown that air-gapped systems can also be attacked through radio waves.

BlackEnergy Malware

BlackEnergy was first identified several years ago as a type of malware used to launch distributed denial of service attacks (DDoS) and steal information. The majority of BlackEnergy's computer coding appears designed to conduct highly sophisticated monitoring and recording of data – a tactic known as "sniffing." However, more recent versions of BlackEnergy, such as BlackEnergy3, have evolved into an advanced persistent threat (APT) tool used in significant geopolitical operations, including Russia, Poland and most recently Ukraine.

Experts worry that versions of BlackEnergy could be programmed to damage pieces of critical infrastructure by hacking into its control system, since its complexity hints at a highly skilled team of hackers with a broad technical background. This latest version of BlackEnergy is "modular," making it much easier for hackers to quickly change how the malware works, and significantly harder for security analysts to find and root it out.

Also worrisome is the proliferation of BlackEnergy malware. The US Department of Homeland Security has already identified BlackEnergy malware deep within the industrial control systems that operate critical infrastructure, and evidence is mounting that the bug has already been deployed around Europe and is "sleeping" until activated. Cybersecurity analysts say they are sure the bug will continue to spread, and that will lead to many more blackouts and "mysterious" malfunctions in national power grids, transportation, and other industrial infrastructure.

Remote Access Trojans

Remote Access Trojans (RATs) provide cybercriminals with unlimited access to infected endpoints. Using the victim's access privileges, they can access and steal sensitive business and personal data – including intellectual property and personally identifiable information. While automated cyberattacks allow cybercriminals to attack browser-based access to sensitive applications, RATs are used to steal information through manual operation of the endpoint on behalf of the victim. Most Advanced Persistent Threat (APT) attacks take advantage of RAT technology for reconnaissance, bypassing strong authentication, spreading the infection, and accessing sensitive applications to exfiltrate data. RATs are commercially available (e.g. Poison Ivy, Dark Comet) and can be maliciously installed on endpoints using drive-by-download and spearphishing tactics.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

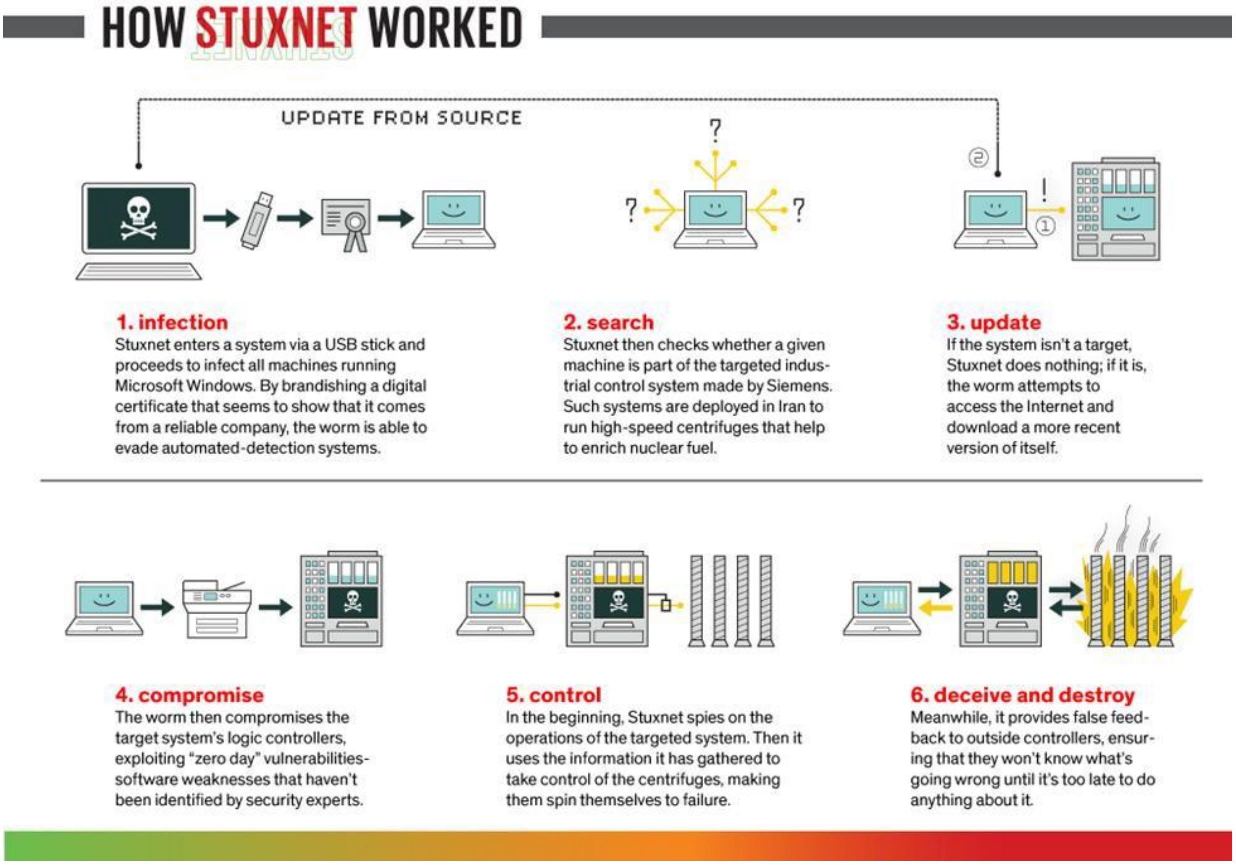
Appendix D: Case Studies

Stuxnet

One of the most famous cases involving the infection of an air-gapped system is Stuxnet, the virus/worm designed to sabotage centrifuges used at a uranium enrichment plant in Iran.

Although a computer virus relies on an unwitting victim to install it, a worm spreads on its own, often over a computer network. First, it targeted Microsoft Windows machines and networks, repeatedly replicating itself. Then it sought out Siemens Step7 software, which is also Windows-based and used to program industrial control systems that operate equipment, such as centrifuges. Finally, it compromised the programmable logic controllers – the heart of a SCADA system. The worm's authors could thus spy on the industrial systems and even cause the fast-spinning centrifuges to tear themselves apart, unbeknownst to the human operators at the plant.

.



1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

Shamoon

The most destructive post-Stuxnet discovery of advanced threats is a malicious malware known as Shamoon. Like Stuxnet, Duqu and Flame, it targeted energy companies in the Middle East, this time Saudi Aramco, Qatar’s RasGas and other oil and gas concerns in the region.

Shamoon was introduced into Saudi Aramco by a disgruntled insider who had full access to the system. It took control of an Internet connected computer and used that computer to communicate back to an external Command-and-Control server. It also infected other computers that were not Internet connected. This type of malware is called a “botnet,” which is a collection of compromised computers under the control of a single individual or group. While it did not disrupt an industrial process or stealthily steal business information as previous types of malware did, Shamoon removed and overwrote the information on the hard drives of 30,000 to 55,000 workstations of Saudi Aramco, wiping the computers' hard drives clean.

Saudi Aramco says damage was limited to office computers and did not affect systems software that might hurt technical operations. However, the destruction of 30,000 workstations undoubtedly caused a vast amount of damage without directly hitting oil production or harming the flow of oil out of the ground.

Ukrainian Cyberattack

On December 23, 2015, Western Ukrainian power company Prykarpattyaoblenergo reported an outage on December 23rd that affected an area including the regional capital Ivano-Frankivsk. A subsequent investigation revealed that a variant of the BlackEnergy malware had caused “interference” in the working of the company’s systems, which led to the power interruption. The investigation also found that the malware had been injected into the networks of two other utilities, though neither had reported any service problems. This event is a milestone because, while destructive events have been targeted at energy before – oil firms, for instance – this is the first event that has caused the widely feared blackout.

BlackEnergy used Microsoft Office documents containing malicious macros in these particular attacks. The attack scenario is simple: the target receives a spearphishing email that contains an attachment with a malicious document. The document itself contains text trying to convince the victim to run the macro in the document. This is an example where social engineering is used instead of exploiting software vulnerabilities. If victims are successfully tricked, they end up infected with BlackEnergy Lite.

German Steel Mill Cyberattack

In December 2014, the German government’s Federal Office for Information Security released an annual findings report in which they noted that a malicious actor had infiltrated a steel facility. The adversary used a spearphishing email to gain access to the corporate network and then moved into the plant network. According to the report, the adversary showed extensive knowledge in industrial control systems (ICS) and was able to cause multiple components of the system to fail. This specifically caused critical process components to become unregulated, which resulted in massive physical damage. To date, the only other public example of a cyberattack causing physical damage to control systems was Stuxnet.

Appendix F: Cybersecurity Glossary

Access control: The process of granting or denying specific requests for or attempts to: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities.

Advanced Persistent Threat: An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception).

Alert: A notification that a specific attack has been detected or directed at an organization’s information systems.

Antivirus software: A program that monitors a computer or network to detect or identify major types of malicious code and to prevent or contain malware incidents – sometimes by removing or neutralizing the malicious code.

Blue Team: A group that defends an enterprise's information systems when mock attackers (i.e., the Red Team) attack, typically as part of an operational exercise conducted according to rules established and monitored by a neutral group (i.e., the White Team).

Bot: A computer connected to the Internet that has been surreptitiously / secretly compromised with malicious logic to perform activities under the command and control of a remote administrator.

Bot master: The controller of a botnet that, from a remote location, provides direction to the compromised computers in the botnet**.**

Computer network defense: The actions taken to defend against unauthorized activity within computer networks.

Continuity of Operations Plan: A document that sets forth procedures for the continued performance of core capabilities and critical operations during any disruption or potential disruption.

Cyber ecosystem: The interconnected information infrastructure of interactions among persons, processes, data, and information and communications technologies, along with the environment and conditions that influence those interactions.

Cyber infrastructure: An electronic information and communications systems and services and the information contained therein.

Cybersecurity: The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.

Denial of Service: An attack that prevents or impairs the authorized use of information system resources or services.

Distributed Denial of Service (DDoS): A denial of service technique that uses numerous systems to perform the attack simultaneously.

Encryption: The process of transforming plaintext into ciphertext.

Firewall: A capability to limit network traffic between networks and/or information systems.

Hacker: An unauthorized user who attempts to or gains access to an information system.

Industrial Control System: An information system used to control industrial processes such as manufacturing, product handling, production, and distribution or to control infrastructure assets.

Inside(r) threat: A person or group of persons within an organization who pose a potential risk through violating security policies.

Keylogger: Software or hardware that tracks keystrokes and keyboard events, usually surreptitiously / secretly, to monitor actions by the user of an information system.

Malicious code: Program code intended to perform an unauthorized function or process that will have adverse impact on the confidentiality, integrity, or availability of an information system.

Passive attack: An actual assault perpetrated by an intentional threat source that attempts to learn or make use of information from a system, but does not attempt to alter the system, its resources, its data, or its operations.

Penetration testing: An evaluation methodology whereby assessors search for vulnerabilities and attempt to circumvent the security features of a network and/or information system.

Phishing: A digital form of social engineering to deceive individuals into providing sensitive information.

Remote-Access Trojan: A malware program that includes a back door for administrative control over the target computer. RATs are usually downloaded invisibly with a user-requested program or sent as an email attachment.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Red Team: A group authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's cybersecurity posture.

Spyware: Software that is secretly or surreptitiously installed into an information system without the knowledge of the system user or owner.

Supervisory Control and Data Acquisition: A generic name for a computerized system that is capable of gathering and processing data and applying operational controls to geographically dispersed assets over long distances.

Threat: A circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact (create adverse consequences for) organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society.

Trojan horse: A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

Virus: A computer program that can replicate itself, infect a computer without permission or knowledge of the user, and then spread or propagate to another computer.

White Team: A group responsible for refereeing an engagement between a Red Team of mock attackers and a Blue Team of actual defenders of information systems.

Worm: A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.

Appendix G: Acronyms

AAR: After action report

APT: Advanced persistent threat

DDoS: Distributed denial of service

DHS: Department of Homeland Security

EEG: Exercise evaluation guide

EMA: Emergency management agency

FOUO: For Official Use Only

HSEEP: Homeland Security Exercise & Evaluation Program

ICS: Industrial control system

IDHS: Indiana Department of Homeland Security

INNG: Indiana National Guard

IOT: Indiana Office of Technology

MEF: Mission essential function

PMEF: Primary mission essential function

POC: Point of contact

RAT: Remote-Access Trojan

SCADA: Supervisory Control & Data Acquisition

SitMan: Situation manual

TTX: Tabletop exercise

USB: Universal Serial Bus

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Indiana Department of Homeland Security (IDHS)

Crit-Ex 16.2

May 2016

Crit-Ex 16.2

Water Utility Disruption Facilitated Cyber Exercise

Exercise Plan

May 18-19, 2016

This Exercise Plan (EXPLAN) provides participants with all the necessary tools for their roles in the exercise. Use of the EXPLAN by all exercise participants is unrestricted.

Preface

The Crit-Ex 2016 Series 2 (Crit-Ex 16.2) Facilitated Cyber Exercise is sponsored by the Indiana Department of Homeland Security (IDHS), Indiana Office of Technology, and the Indiana National Guard. This Exercise Plan (EXPLAN) was produced with input, advice, and assistance from the Crit-Ex 16.2 Planning Team, which followed guidance set forth by the U.S. Department of Homeland Security (DHS) Homeland Security Exercise and Evaluation Program (HSEEP).

This EXPLAN provides exercise participants with all the necessary tools for their roles in the exercise. It is tangible evidence of Indiana's commitment to ensure public safety through collaborative partnerships that will prepare it to respond to any emergency.

The Crit-Ex 16.2 Facilitated Cyber Exercise is an unclassified exercise. Control of exercise information is based on public sensitivity regarding the nature of the exercise rather than actual exercise content. Some exercise material is intended for the exclusive use of exercise planners, facilitators, and evaluators, but players may view other materials that are necessary to their performance. All exercise participants may view the EXPLAN.

Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Handling Instructions

1. The title of this document is Crit-Ex 16.2 *Cyber Exercise Plan (EXPLAN).*

2. Information gathered in this EXPLAN is designated as For Official Use Only (FOUO) and should be handled as sensitive information that is not to be disclosed. This document should be safeguarded, handled, transmitted, and stored in accordance with appropriate security directives. Reproduction of this document, in whole or in part, without prior approval from the exercise sponsors is prohibited.

3. Given the scenario, topics, and personnel involved in the exercise, some of the discussion topics may necessitate restrictions. While this exercise is engineered to elicit productive dialogue on capabilities, not vulnerabilities, conversation may touch on issues with implications for local, state, or national security. This may include unclassified information about an organization's operations, the unauthorized disclosure of which could adversely impact public safety or welfare, the effectiveness of the organization's critical operations programs, or other operations essential to state or national interest.

4. At a minimum, the attached materials will be disseminated strictly on a need-to-know basis and, when unattended, will be stored in a locked container or area that offers sufficient protection against theft, compromise, inadvertent access, and unauthorized disclosure.

Exercise Overview

Exercise Name	Crit-Ex 16.2 Water Utility Disruption Facilitated Cyber Exercise
Exercise Date, Time, and Location	May 18 and 19, 2016 8AM – 7PM Muscatatuck Urban Training Center, Indiana
Scope	This exercise is a controlled, operations-based, facilitated cyber exercise, planned for two 10 hour days of execution. The exercise is intended to bring awareness and discuss potential responses to a cyberattack on water utility Supervisory Control and Data Acquisition (SCADA) systems, and improve the overall security and responsiveness in the event that an advanced cyber event disrupts essential utility services and presents debilitating effects across a range of critical functions.
Mission Areas	Mitigation, Response, and Recovery
Core Capabilities	Operational Coordination, Operational Communications, Intelligence and Information Sharing, and Cybersecurity
Objectives	1. Protect and restore the SCADA system information and services from damage, unauthorized use, and exploitation caused by malicious activity. 2. Stabilize water infrastructure functions, minimize health and safety threats, and efficiently restore and revitalize systems and services to support a viable, resilient community. 3. Bring awareness to the current readiness of water utilities to respond to a cyberattack and draw out best practices for improving system security and incident response. 4. Provide water utility observers with the training that empowers them for a real-world emergency, identifying key decision points, and decision making.
Threat or Hazard	Cyberattack Vector: Control Systems Malware
Scenario	A state-sponsored terrorist group (Red Team) remotely conducts a cyberattack on a SCADA system at various water utility treatment facilities in Indiana with the identified utility representatives (Blue Team) serving as active observers.
Sponsors	Indiana Department of Homeland Security, Indiana Office of Technology, Indiana Army National Guard

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Participating Organizations	Approximately 16 participating organizations and 18 players from the Indiana Department of Homeland Security; Indiana Office of Technology; Indiana National Guard; Indiana water/wastewater utilities, the Indiana Chapter of the AWWA, Indiana Energy Association, and cybersecurity organizations. For a full list of participating organizations, see Appendix D.
Points of Contact	Jennifer de Medeiros Emergency Services Program Manager Indiana Department of Homeland Security 302 W. Washington St., W246 Indianapolis, IN 46254 (317) 452-0380 jdemedeiros@dhs.in.gov James McHugh Critical Infrastructure Program Manger 302 West Washington Street, Room W246 Indianapolis, IN 46204 317-473-0353 jmchugh@dhs.in.gov Doug Rapp President, Cyber Leadership Alliance 85 East Cedar Street Zionsville, IN 46077 doug@cyberleaders.org Philip N. Barker Contractor, Patriot Strategies Program Manager Atterbury-Muscatatuck Center for Complex Operations Office: (317) 247-3300 ext.: 62063 Cell: (812) 345-4343 philip.n.barker.ctr@mail.mil
Additional Information	Crit-Ex 16.2 planners have designed this exercise to focus on water utility cyberattack management. The suggested audience should be limited to water utilities, cyber-incident response entities, and government.

Contents

SECTION 1: GENERAL INFORMATION

Background

The idea that the United States is facing a “Cyber 9/11” is at the forefront of homeland security discourse. Like the rest of the country, Indiana has a short window of opportunity to prepare for a major cybersecurity incident that, if successful, could be as devastating as a major earthquake or tornado. The year 2016 has been groundbreaking for developing cross-sector partnerships, governance structure, and strategic programs necessary for preventing, protecting, mitigating, responding to and recovering from cyber incidents. IDHS has been working in close conjunction with the Indiana Office of Technology (IOT) and the Indiana National Guard (INNG) to lead a collaborative effort between government, private-sector, military, and academic stakeholders, as well as incorporating cyber research to enhance Indiana’s cybersecurity posture.

Crit-Ex 2016 is the first of these cross-sector initiatives, designed for both the public and private sectors in order to improve understanding of cybersecurity posture and identify capability gaps. It will function as a series of tabletop, demonstration, and functional exercises that explore the intersection of cybersecurity and critical infrastructure, using scenarios in which a cyberattack on a critical asset leads to physical-world consequences. The project is designed to recur annually, allowing partners from different critical infrastructure sectors across Indiana to participate and improve their cyber defenses. This year’s scenarios are focusing on cyberattacks disrupting SCADA systems at a water and power utility, allowing participants to exercise their cybersecurity response processes. As such, Crit-Ex 2016 will be a “first-of-its kind” exercise that catalyzes information sharing, training opportunities, partnerships, and response planning across the state.

Purpose

The purpose of the Crit-Ex 16.2 Cyber Exercise is to improve the overall security and responsiveness of Indiana’s critical infrastructure in the event that an advanced cyber event disrupts essential services, and presents debilitating effects across a range of critical functions. Crit-Ex 16.2 will also:

- Increase key stakeholder awareness to a cyberattack on a water utility SCADA system;
- Improve the overall security and responsiveness in the event that an advance cyber event disrupts essential utility services and presents debilitating effects across a range of critical functions;
- Offer a real-world simulation of a small rural water company and provide a learning opportunity to improve SCADA security and operations;
- Develop security technologies and best practices for the field devices based upon actual and expected Industrial Control Systems (ICS) cyber incidents; and
- Establish, promote, and support an open demonstration facility at Muscatatuck Urban Training Center (MUTC), and additional areas around the State that are dedicated to, and promote best practices for ICS systems.

.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Scope

This exercise focuses on how water/wastewater utilities will respond to a coordinated cyberattack, and also draws the role of federal, state, and local agencies into the conversation. This exercise will be a controlled, operations-based facilitated cyber exercise, planned for two, 10 hour days of execution. The exercise will bring awareness of and discuss potential responses to a cyberattack.

Core Capabilities and Exercise Objectives

The National Preparedness Goal of September 2011 has steered the focus of homeland security toward a capabilities-based planning approach using 32 identified Core Capabilities. Capabilities-based planning focuses on planning under uncertainty because the next disaster can never be forecast with complete accuracy. Therefore, capabilities-based planning takes an all-hazards approach to planning and preparation that builds capabilities, which can be applied to a wide variety of incidents. States and urban areas use capabilities-based planning to identify a baseline assessment of their homeland security efforts by comparing their current capabilities against the Core Capabilities. This approach identifies gaps in current capabilities.

The Core Capabilities are essential for the execution of each of the five mission areas: Prevention, Protection, Mitigation, Response, and Recovery. These capabilities provide the foundation for development of the exercise design objectives and scenario.

Mitigation Mission Area: Mitigation comprises “the capabilities necessary to reduce the loss of life and property by lessening the impact of disasters.”

Response Mission Area: Response comprises “the capabilities necessary to save lives, protect property and the environment, and meet basic human needs after an incident has occurred.”

Recovery Mission Area: Recovery comprises "the core capabilities necessary to assist communities affected by an incident to recover effectively.”

The following exercise objectives in Table 1 describe the expected outcomes for the exercise. The objectives are linked to both the identified Core Capabilities and the American Water Works Association’s (AWWA) standards. The Core Capabilities are identified as distinct critical elements necessary to achieve the specific mission area(s) and the AWWA Practice Categories are recommended cybersecurity practices for the Water Sector. The objectives, aligned Core Capabilities and AWWA Practice Categories were selected by the Exercise Planning Team. Appendix B of this EXPLAN provides a more detailed breakdown of the crosswalk between Core Capabilities and AWWA Practice Standards.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Exercise Objective	Core Capability	AWWA Practice Standards
1. Protect and restore the SCADA system information and services from damage, unauthorized use, and exploitation caused by malicious activity.	• Cybersecurity (CS), • Intelligence & Information Sharing (I/IS) • Operational Coordination (OC)	• Access Control (CS) • Application Security (CS) • Business Continuity & Disaster Recovery (OC, OS) • Education (CS) • Encryption (CS) • Government and Risk Management (OC, CS) • Operations Security (CS) • Personnel Security (CS) • Physical Security of PCS Equipment (CS) • Server and Workstation Hardening (CS) • Service Level Agreements (CS) • Telecom, Network Security, and Architecture (CS)
2. Stabilize water infrastructure functions, minimize health and safety threats, and efficiently restore and revitalize systems and services to support a viable, resilient community.	• Operational Coordination (OC) • Operational Communications (OCOM)	• Access Control (OC) • Business Continuity & Disaster Recovery (OC) • Encryption (OCOM)) • Governance and Risk Management (OC) • Service Level Agreements (OC, OCOM) • Telecommunications, Network Security, and Architecture (OCOM))

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

3. Bring awareness to the current readiness of water utilities to respond to a cyberattack and draw out best practices for improving system security and incident response.	• Cybersecurity (CS) • Operational Coordination (OC) • Operational Communications (OCOM)	• Access Control (CS) • Application Security (CS) • Business Continuity and Disaster Recovery (CS, OC, OCOM) • Education (CS, OCOM) • Encryption (CS, OCOM) • Governance and Risk Management (CS, OC) • Operations Security (CS) • Personnel Security (CS) • Physical Security of PCS Equipment (CS) • Service Level Agreements (CS, OCOM) • Service and Workstation Hardening (CS) • Telecommunications, Network Security, and Architecture (CS)
4. Provide water utility observers with the training that empowers them for a real world emergency, identifying key decision points and decision making.	• Cybersecurity (CS), • Intelligence & Information Sharing (I/IS)	• Access Control (CS) • Application Security (CS) • Business Continuity and Disaster Recovery (CS) • Encryption (CS) • Governance and Risk Management (CS) • Operations Security (CS) • Personnel Security (CS) • Physical Security of PCS Equipment (CS) • Server and Workstation Hardening (CS, IS) • Service Level Agreements (CS) • Telecommunications, Network Security, and Architecture (CS, IS) • Education (CS, IS)

Table 1. Exercise Objectives and Associated Core Capabilities/AWWA Standards

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Participants

The term *participant* encompasses many groups of people, not just those playing in the exercise. Groups of participants involved in the exercise, and their respective roles and responsibilities, are as follows:

- **Players:** Players respond to the situation presented, based on expert knowledge of response procedures, current plans and procedures, and insights derived from training.

- **Controllers:** The exercise control representative is trained on the specifics of the exercise, to include the MSEL and evaluation criteria. This individual will help to guide the exercise as needed to ensure that it meets the training intent, and records data that will be evaluated against exercise/industry best practices.

- **Observers:** Observers support the group in developing responses to the situation during the discussion; however, they are not participants in the moderated discussion period. For this exercise the planning team has additionally identified the role of utility observer, with specific roles to include the following:
    - **Utility Observer:** This participant is a member of the utility team and is generally familiar with utility response plans and the expectations of the utility leadership. The Utility Observer will be situated in the Control Room and observer operations during exercise execution.

- **Facilitators:** Facilitators provide situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key Exercise Planning Team members also may assist with facilitation as subject matter experts during the Exercise. For this exercise representatives from Purdue and Indiana University are scheduled to serve in this role.

- **Exercise Operator:** The exercise operator is a non-participating member of the team who is familiar with the environment/controls that are being used in the exercise. Individuals in this role will be utilized to be an interpreter for the environment, and an extension of the controls for a utility operator who may not be comfortable at the controls in an unfamiliar operating environment.

- **Utility Operator/Supervisor:** The utility operator is the individual who physically sits at the controls of the plant and has intimate knowledge of water treatment operations. The supervisor intimately understands water treatment operations and is most familiar with incident management procedures for the utility and will potentially go into the field during exercise execution. Depending on the size and structure of the specific utility, the utility operator and utility supervisor might be the same individual.

- **Evaluators:** Evaluators are assigned to observe and evaluate certain objectives during the exercise. Their primary role is to document player discussions, including how and if those discussions conform to written and established procedures.

- **VIPs:** VIPs are individuals who have been invited to the exercise event, but will be in attendance briefly and do not serve any official role in exercise conduct.

Exercise Structure

This will be a multimedia, facilitated Exercise. Wastewater utility observers (“players”) will participate in the following exercise events/phases:

- **Phase 1:** “Business as Usual”
- **Phase 2:** “Fool Me Twice”
- **Facilitated After Action Review**

Each phase of the cyber exercise will begin with a multimedia update that summarizes key events occurring. After the updates, active observers will review the situation and engage in facilitated discussions of appropriate response issues. For Crit-Ex 16.2, the functional groups are:

- Operators
- Supervisors

After these functional group discussions, participants will engage in a facilitated After Action Review discussion in which representatives from each utility will present a synopsis of the group’s actions based on the scenario presented.

Exercise Evaluation

Evaluation of the exercise is based on a set of objectives developed by the Exercise Planning Team. Evaluators will be provided with the identified objectives, and players will be asked to complete exercise evaluation forms. These documents, coupled with facilitator observations and notes compiled during the After Action Review process will be used to evaluate the exercise and compile the After Action Report (AAR).

Exercise Guidelines

- This Exercise will be held in an open, low-stress, no-fault environment. Varying viewpoints, even disagreements, are expected.
- Respond on the basis of your knowledge of current plans and capabilities (i.e., you may use only existing assets) and insights derived from your training.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

- Decisions are not precedent setting and may not reflect your organization's final position on a given issue. This exercise is an opportunity to discuss and present multiple options and possible solutions.
- Issue identification is not as valuable as suggestions and recommended actions that could improve response and preparedness efforts. Problem-solving efforts should be the focus.

Assumptions & Artificialities

In any exercise, assumptions and artificialities may be necessary to complete play in the time allotted. During this exercise, the following apply:

- The scenario as designed may not be catastrophic or coordinated enough to affect all the organizations involved. However, it is the intent of the Exercise Planning Team to utilize a catastrophic scenario according to Homeland Security Exercise and Evaluation Program (HSEEP) standards to drive exercise discussion.
- Incident attribution may take longer than the scenario describes. However, productive discussion will hinge on knowing the attack source and vector.
- There is no hidden agenda, and there are no trick questions.
- All players receive information at the same time.

SECTION 2: SYSTEMS/NETWORK OVERVIEW & EXERCISE SCENARIO BACKGROUND

Systems/Network Overview

For Crit-Ex 16.2 the exercise will utilize a system specifically designed to mirror a small municipal water treatment plant. The water plant has two Allen Bradley MicroLogix Programmable Logic Controllers (PLC). One monitors turbidity of the filtered water, and the other controls the High Service pumps based on flow and/or pressure. These PLCs are connected through a Cisco process network to Human-Machine Interface (HMI) and data servers located in building 5016 using Rockwell Automation FactoryTalk View software. The plant operator uses an operator workstation (client) to monitor and control the water plant. Also located in the control room is a business personal computer (PC) connected to the Internet through an Integrated Threat Management appliance (SonicWALL). The third PC in play is a historian/engineering server. It is used to collect trended information and as a programming terminal with RSLogix software installed to modify the PLC code as required**.**

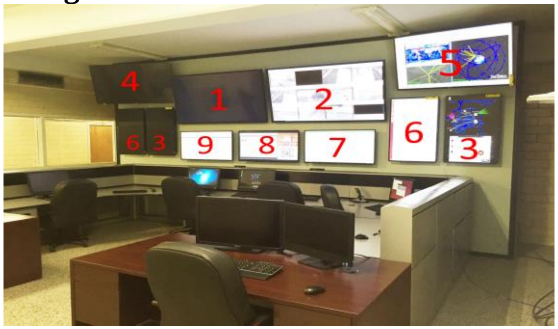
The operator control room will be equipped with several monitors including:

- Operator Workstation – What the operator sees on his HMI
- Business Workstation – Used for Internet access and email
- Engineering Workstation – PLC programming/engineering

A "mirrored server" is also connected to the PLCs. It will allow for the monitoring of actual plant control activities and feed information to the observation room during the breach. Screens will also be in-place to show the changes that occur within the PLC and the associated network traffic and event log changes that occur as result of the attack. To do this, the observation room will be equipped with monitors that include: (See Figure 2.1 for additional information)

1. Operator Workstation – What the operator sees on his HMI
2. Observer Workstation – Actual (reality) HMI values from the water plant's PLC
3. Wireshark – real-time view of local network traffic
4. Attacker Workstation – What the adversary is doing
5. Video Screen – Camera feed of plant discharge at lagoon to indicate plant activity
6. Event Log – Shows activity on water plant PLC
7. RSLogix – shows actual programming in water plant PLC
8. Event Sentry – Consolidates event logs from multiple devices
9. Threat Map – Internet threat tracking application

Figure 2.1: Observer Room Screens



Attack Vectors and Desired Effects

A public-facing Internet Protocol (IP) address connected to the Internet is defended by a firewall that connects the Internet Service Provider (ISP) to the business network. A single physical switch (Cisco) is VLANd off from the process network. For Crit-Ex 16.2, the attack will be of two varieties:

- Brute Force – Designed to start attacking a public-facing IP.
    - The end result will be the attacker pushing through the Sonicwall (Demilitarized Zone [DMZ]), bridging the two Virtual Local Area Networks (VLAN) and then enabling a Remote-Access Trojan (RAT) of the PLC programming software, allowing the hacker to modify code without the operator seeing a change on his screens.
- Watering Hole – Operator visits an approved website that has been compromised causing a malicious payload to be delivered.
    - Following the start-up of the malicious payload, an outbound connected HTTPS connection is made on tcp/443 through the firewall.
    - At that point the attacker can initiate commands with the infected host, and a series of commands can then be run to allow full control of the machine and other interconnected systems.
    - Each of the commands below will be executed on the compromised machine (agent) making an outbound connection to the listener.

Desired effects of attacks include the following:

- By reprogramming high-service (HS) pump controls, the bad actor will be able to:
    - Stop water flow through the distribution network, causing a boil-water order to be issued, or;
    - Cycle HS pumps, causing water hammer and burst pipes.
- By reprogramming filter controls and turbidity reports, the bad actor will be able to:
    - Generate non-potable water and distribute it to the population, requiring flush and boil orders.

Exercise Scenario Background

Phase 1: “Business as Usual”

A state-sponsored terrorist group has begun a targeting campaign aimed at small utility companies, attempting to find vulnerabilities in their public-facing websites that will result in access to critical industrial control systems. The group has targeted smaller companies because of their lack of resources and ability to protect their growing IT networks. With the resources backing this particular terrorist group, it is only a matter of time before access is granted, likely without the utility companies having any notification of malicious intrusion into their network.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

During this campaign, the state-sponsored group has successfully accessed a rural water utility company's critical infrastructure network via a brute force attack passing through the DMZ. Once inside the network, the group is able to pivot laterally without detection from operational and technical controls. With such ease of movement, the group has successfully changed the code to a PLC, giving it the ability to control the water-related functions of this PLC anytime it chooses. The advantage for the terrorist group changing the code is two-fold in nature because the operator at the water company does not see any change on their HMI display. Once the process is triggered, the only way an operator would become aware of the change is after something drastic has already occurred in the distribution network.

Key Issues

- Indiana is experiencing potential water disruption that affects various water utility companies around the state.
- Utilities are not aware that a cyberattack has caused this disruption, and most are going through normal recovery operations.

Questions

The following questions are provided as suggested general subjects. These questions are not meant to constitute a definitive list of concerns to be addressed, nor is there a requirement to address every question.

- What initial actions would your organization take? What are your organization's first priorities?
- Who is your first call? How do you identify your critical partners for a disruption?
- Would information presented in this phase (or this stage of the attack) be shared? Who is contacted as part of the alert/notification process?
  - Local government, police, fire, emergency services, and trusted third parties?
  - State partners and/or agencies?
  - Federal partners and/or agencies?
- Are manual overrides available to allow operation of key processes?
- What are your reporting requirements? Based on your contact and alert procedures after an incident, do those match your mandated reporting requirements? Internal? Local, state, and federal levels of government?
- How do you determine when and with whom to share sensitive and/or classified information about the event, including information about proprietary systems? What concerns or considerations do you have in coordinating with or discussing your situation with external entities?
- Have you identified available resources and their specific requests channels for a water disruption?

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

After Action Review Discussion Topics for Consideration

- Assess the effectiveness of the organization's incident reporting and notification process.
- Determine how and how quickly utilities communicate with interdependent facilities, emergency management and government following an attack.
- Identify when intelligence and information is shared, and with whom.
- Identify available resources and resource request channels for a water disruption.

Phase 2: "Fool Me Twice"

As the state-sponsored terrorist group campaign persists against small utility companies, it continues to find vulnerabilities that add to its overall attack package. It has already successfully changed the normal operating functions of many utility companies in the past few weeks, causing them to revert to manual operation while IT-related issues were resolved. Most of the companies are unaware that the change in functions could be attributed to a cyberattack, and those that have suspicions have failed to share their findings with other utilities. Some attack vectors previously exploited by the group have been revoked because of normal IT procedures. That may have fixed the initial intrusion, as a persistent threat always looks for another way in.

Normal processes and procedures in the daily life of utility operators can seem menial, but to an attacker they present opportunities to exploit vulnerabilities of daily operations. A website used by many utility operators in the area has been compromised by the group, and when users think they are checking local weather reports a malicious payload is dropped onto their system. From there, the group is able to capture a multitude of data, helping them develop secondary attack vectors in the chance that their initial vector is closed off. The result is the same; it gives the group complete access to pivot inside the utility network without being detected. Having that ability allows the attackers to change whatever they want without operator knowledge and repeat and/or initiate new attacks against compromised utility companies.

Key Issues

Utilities are now aware that a cyber-attack has caused this disruption.

Questions

The following questions are provided as suggested general subjects. These questions are not meant to constitute a definitive list of concerns to be addressed, nor is there a requirement to address every question.

- How and with whom will this information be communicated?
- Does this information change your priorities? How? How will it affect your response operations? How would a law enforcement investigation impact your current operations?
- How does the attribution of a terrorist cyberattack change your priorities and courses of action?
- What types of sensitive information/intelligence need to be communicated outside your organization, and how will that be delivered?

- Does your organization have the resources it needs to respond to this cyberattack? How will you request more resources?
- What protective actions would you take across non-impacted systems or agencies?
  - Who is responsible for protective action decision-making?
  - How are actions coordinated across departments/agencies?
- How will you address public safety issues? With what agencies/entities will you coordinate?
- What plans, procedures, and/or agreements do you have in place to control resource distribution within and outside your jurisdiction?
- Is a Crisis Management Team identified with at least one representative from executive management? Does the team have the authority to declare the disaster and coordinate necessary recovery activities?
- Is there an Incident Response Plan and does it include a contact list and procedures for contacting necessary personnel? Is there a back-up plan if essential personnel cannot be reached?
- Does the organization have consistent contact with intelligence organizations to stay abreast of current threat Tactics, Techniques, and Procedures (TTPs)? Are changes made to security procedures based on available intelligence?
- Are written Service Level Agreements (SLA) established for all identified external dependencies? Are expectations for response times/restoration included? Are they exercised to ensure external organizations can realistically meet demands?
- Are SLAs with staff and contracted employees established to respond in emergency conditions?
- Have you identified available resources and their specific requests channels for a water disruption?

After Action Review Discussion Topics for Consideration

- Examine the effectiveness of the organizations intelligence information-sharing protocols.
- Explore what polices and/or procedures are in place to identify a cyber incident.
- Explore what policies and/or procedures are in place to mitigate and react to a cyberattack.
- Identify available resources and resource request channels for a water disruption.

Phase 3: After Action Review Discussion

After these functional group discussions, participants will engage in a facilitated After Action Review discussion in which representatives from each utility will present a synopsis of the group's actions based on the scenario presented. This discussion, which will be led and facilitated by identified representatives from Camp Atterbury-Muscatatuck, will also examine various strengths and lessons learned from the exercise, as well as future areas for improvement.

Evaluation of the exercise is based on a set of objectives developed by the Exercise Planning Team. Evaluators will be provided with the identified objectives, and players will be asked to complete exercise evaluation forms. These documents, coupled with facilitator observations and notes compiled during the After Action Review process will be used to evaluate the exercise and compile the AAR.

SECTION 3: EXERCISE APPENDICES

Appendix A: Exercise Schedule – Day 1 (Groups 1, 2, and 3)

May 18, 2016

May 18, 2016 – Indiana American Water	
Time	**Activity**
0800-0820	Welcome Briefing
0820-0830	Move to Building 16
0830-1000	Phase 1 - Attack 1
1000-1130	Phase 2 – Attack 2
1130+20	Reboot exercise control system for next group
1130-1200	Wrap-up and Debrief (After Action Review)
1230-1300	FBI Command Tour
1300-1400	Tour of MUTC

May 18, 2016 – Michigan City water Department	
Time	**Activity**
1120-1140	Welcome Briefing
1140-1150	Move to Building 16
1150-1320	Phase 1 - Attack 1
1320-1450	Phase 2 – Attack 2
1450+20	Reboot exercise control system for next group
1450-1520	Wrap-up and Debrief (After Action Review)
1530-1600	FBI Command Tour
1600-1700	Tour of MUTC

May 18, 2016 – Carmel Utilities	
Time	**Activity**
1300-1320	Welcome Briefing
1320-1330	Move to FBI Command Center
1330-1400	FBI Command Tour
1400-1500	Tour of MUTC
1510-1640	Phase 1 – Attack 1
1640-1810	Phase 2 – Attack 2
1810	Reboot exercise control system (for day 2)
1810-1840	Wrap-up and Debrief (After Action Review)

Exercise Schedule – Day 2 (Groups 4, 5, and 6)

May 19, 2016

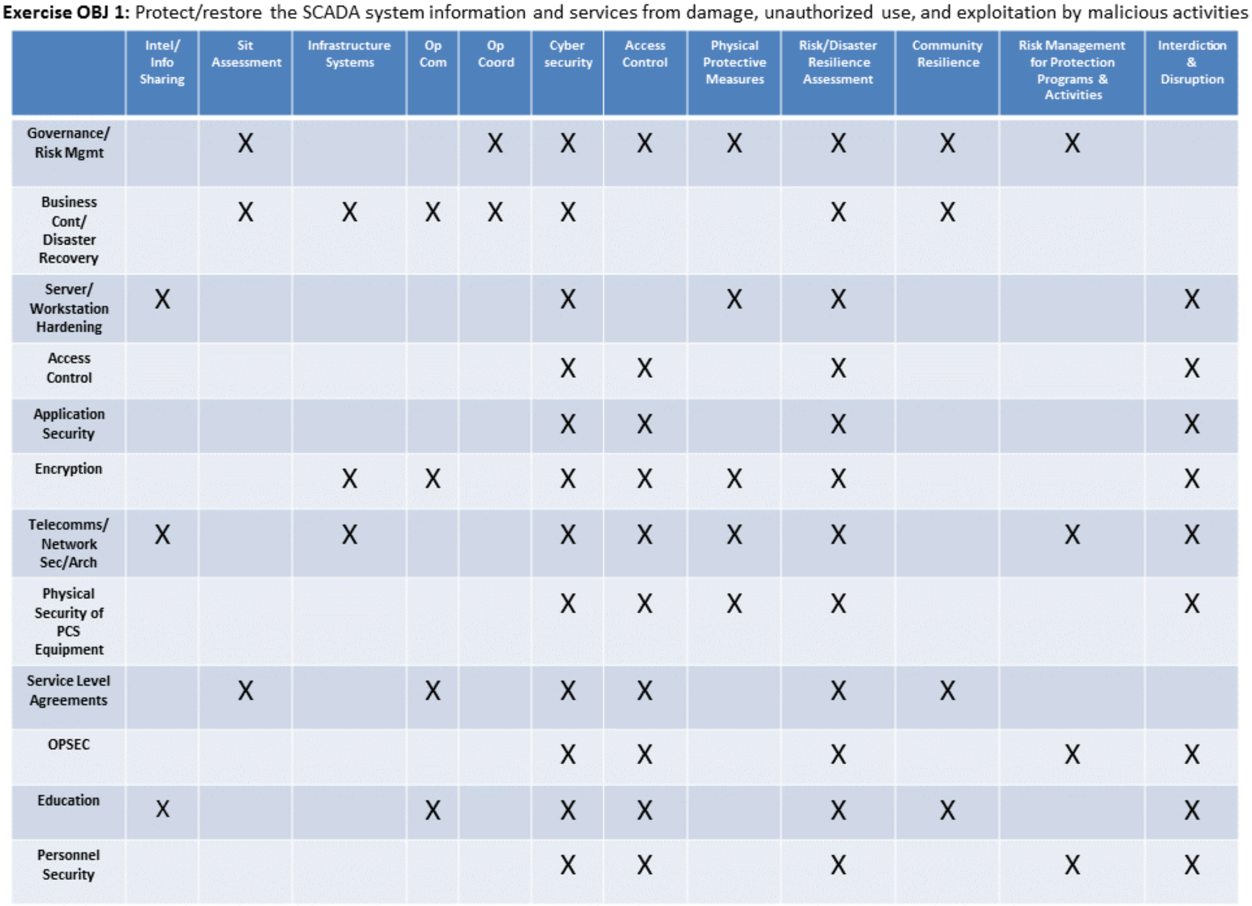
May 19, 2016 – Evansville Water & Sewage	
Time	**Activity**
0800-0820	Welcome Briefing
0820-0830	Move to Building 16
0830-1000	Phase 1 - Attack 1
1000-1130	Phase 2 – Attack 2
1130+20	Reboot exercise control system for next group
1130-1230	Wrap-up and Debrief (After Action Review)
1230-1300	FBI Command Tour
1300-1400	Tour of MUTC

May 19, 2016 – Citizens Water	
Time	**Activity**
1120-1140	Welcome Briefing
1140-1150	Move to Building 16
1150-1320	Phase 1 - Attack 1
1320-1450	Phase 2 – Attack 2
1450+20	Reboot exercise control system for next group
1450-1520	Wrap-up and Debrief (After Action Review)
1530-1600	FBI Command Tour
1600-1700	Tour of MUTC

May 19, 2016 – Fort Wayne Utilities	
Time	**Activity**
1300-1320	Welcome Briefing
1320-1330	Move to FBI Command Center
1330-1400	FBI Command Tour
1400-1500	Tour of MUTC
1510-1640	Phase 1 – Attack 1
1640-1810	Phase 2 – Attack 2
1810-1840	Wrap-up and Debrief (After Acton Review)

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Appendix B: Core Capability/AWWA Practice Standards Crosswalk



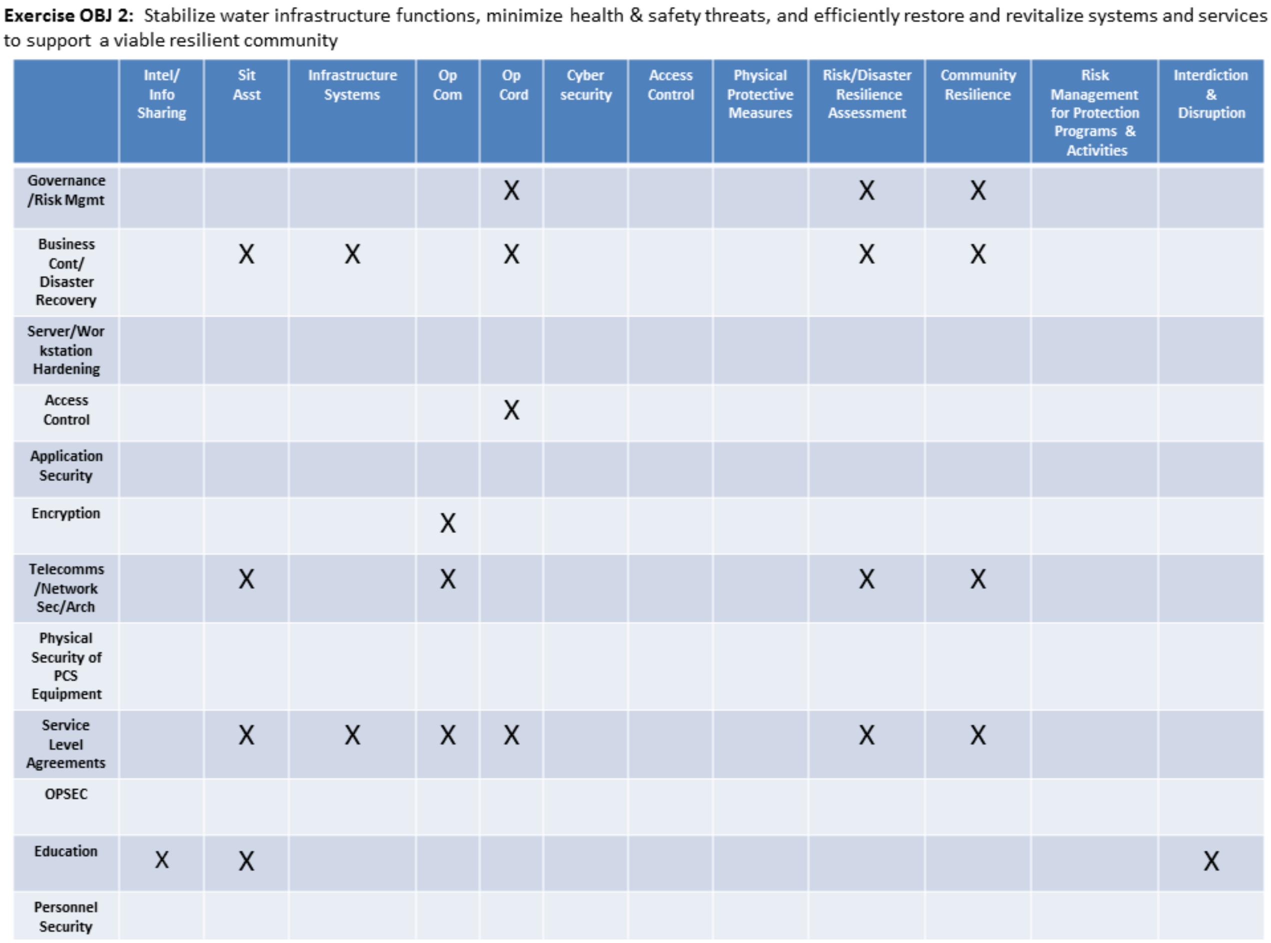
Exercise OBJ 1: Protect/restore the SCADA system information and services from damage, unauthorized use, and exploitation by malicious activities

	Intel/ Info Sharing	Sit Assessment	Infrastructure Systems	Op Com	Op Coord	Cyber security	Access Control	Physical Protective Measures	Risk/Disaster Resilience Assessment	Community Resilience	Risk Management for Protection Programs & Activities	Interdiction & Disruption
Governance/ Risk Mgmt		X			X	X	X	X	X	X	X	
Business Cont/ Disaster Recovery		X	X	X	X	X			X	X		
Server/ Workstation Hardening	X					X		X	X			X
Access Control						X	X		X			X
Application Security						X	X		X			X
Encryption			X	X		X	X	X	X			X
Telecomms/ Network Sec/Arch	X		X			X	X	X	X		X	X
Physical Security of PCS Equipment						X	X	X	X			X
Service Level Agreements		X		X		X	X		X	X		
OPSEC						X	X		X		X	X
Education	X			X		X	X		X	X		X
Personnel Security						X	X		X		X	X

Most Relevant Questions:

- Does the organization implement a cyber-security awareness program that cross trains Process Control System (PCS) & IT staff on best practices for PCS cybersecurity and trains personnel on risky behaviors /threats (including social engineering)?
- Is there a formal, written Cybersecurity policy that addresses the specific operational needs of PCs, contains priorities for mission/objectives/activities, established cybersecurity roles & responsibilities for the entire workforce/3rd party stakeholders, legal requirements, and includes an information security policy?
- Does the organization have consistent contact with intelligence organizations to stay abreast of current threat Tactics, Techniques, and Procedures (TTPs)? Are changes made to security procedures based on available intelligence?
- Does the organization conduct vulnerability assessments on a regular basis?
- Does the organization maintain a PCS asset inventory?
- Are PCS Cybersecurity standards articulated/required in all procurement packages?
- Is storage encryption implemented for devices that could be stolen?

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.



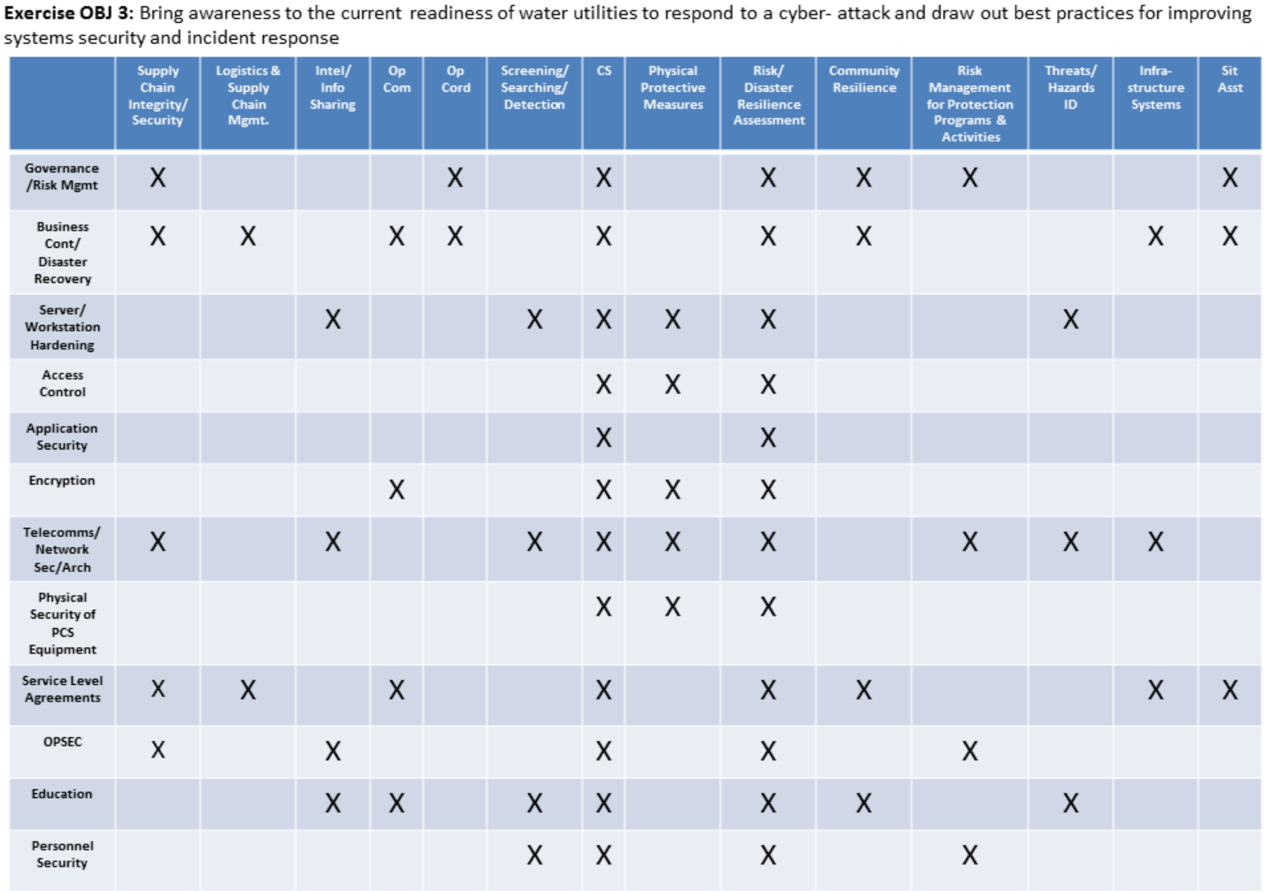
Exercise OBJ 2: Stabilize water infrastructure functions, minimize health & safety threats, and efficiently restore and revitalize systems and services to support a viable resilient community

	Intel/ Info Sharing	Sit Asst	Infrastructure Systems	Op Com	Op Cord	Cyber security	Access Control	Physical Protective Measures	Risk/Disaster Resilience Assessment	Community Resilience	Risk Management for Protection Programs & Activities	Interdiction & Disruption
Governance /Risk Mgmt					X				X	X		
Business Cont/ Disaster Recovery		X	X		X				X	X		
Server/Workstation Hardening												
Access Control					X							
Application Security												
Encryption				X								
Telecomms /Network Sec/Arch		X		X					X	X		
Physical Security of PCS Equipment												
Service Level Agreements		X	X	X	X				X	X		
OPSEC												
Education	X	X										X
Personnel Security												

Most Relevant Questions:

- Are written Service Level Agreements (SLAs) established for all identified external dependencies? Are expectations for response times/restoration included? Are they exercised to ensure external organizations can realistically meet demands?
- Are SLAs with staff and contracted employees established to respond in emergency conditions?
- Is a Crisis Management Team identified with at least one representative from executive management? Does the team have the authority to declare the disaster and coordinate necessary recovery activities?
- Are manual overrides available to allow operation of key processes?
- Are strategies in place to provide redundancy of key system components and can they be implemented within an acceptable timeframe?

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.



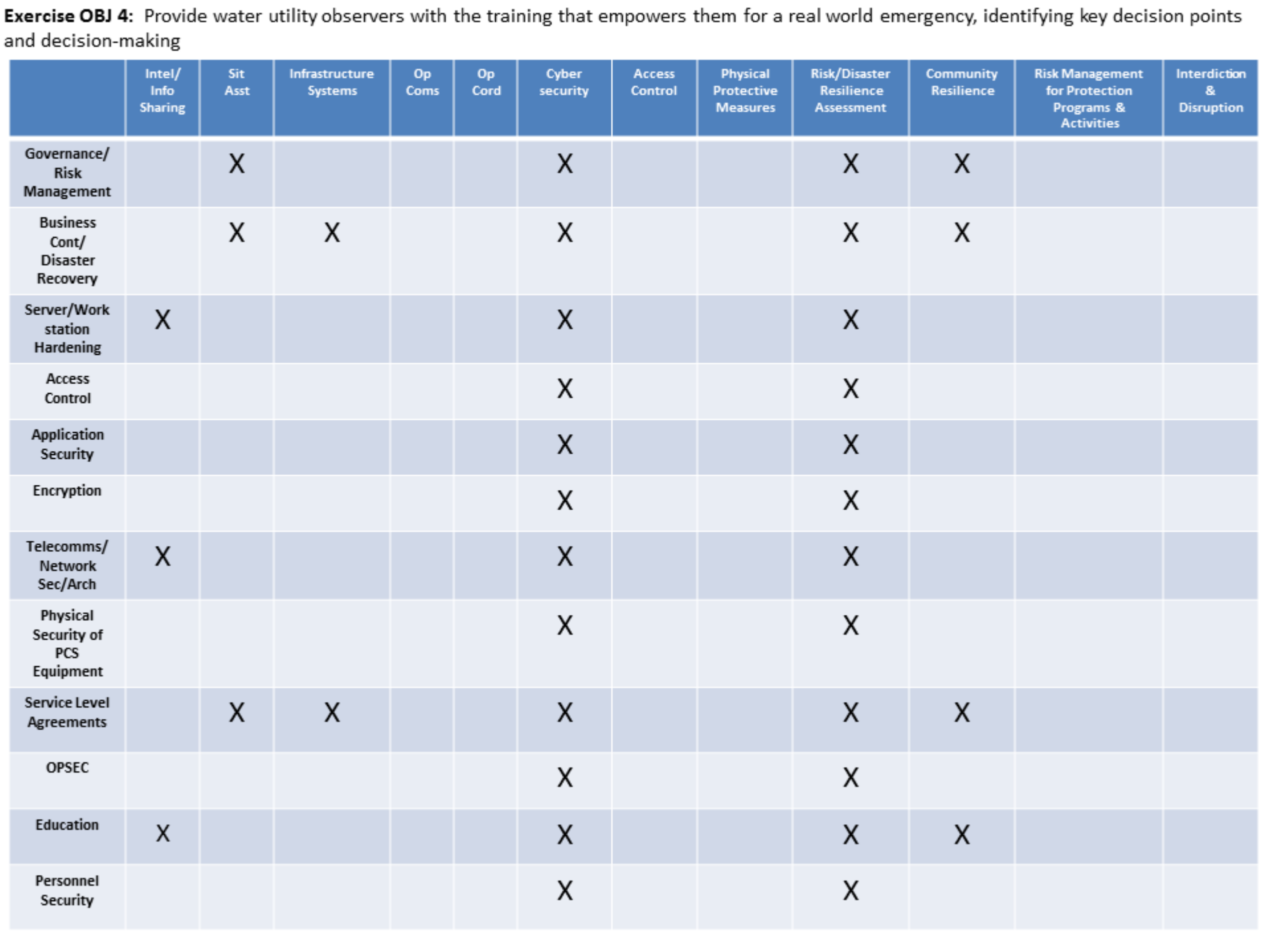
Exercise OBJ 3: Bring awareness to the current readiness of water utilities to respond to a cyber- attack and draw out best practices for improving systems security and incident response

	Supply Chain Integrity/ Security	Logistics & Supply Chain Mgmt.	Intel/ Info Sharing	Op Com	Op Cord	Screening/ Searching/ Detection	CS	Physical Protective Measures	Risk/ Disaster Resilience Assessment	Community Resilience	Risk Management for Protection Programs & Activities	Threats/ Hazards ID	Infra-structure Systems	Sit Asst
Governance /Risk Mgmt	X				X		X		X	X	X			X
Business Cont/ Disaster Recovery	X	X		X	X		X		X	X			X	X
Server/ Workstation Hardening			X			X	X	X	X			X		
Access Control							X	X	X					
Application Security							X		X					
Encryption				X			X	X	X					
Telecomms/ Network Sec/Arch	X		X			X	X	X	X		X	X	X	
Physical Security of PCS Equipment							X	X	X					
Service Level Agreements	X	X		X			X		X	X			X	X
OPSEC	X		X				X		X		X			
Education			X	X		X	X		X	X		X		
Personnel Security						X	X		X		X			

Most Relevant Questions:

- Does the organization have consistent contact with intelligence organizations to stay abreast of current threat TTPs? Are changes made to security procedures based on available intelligence?
- Is a Crisis Management Team identified with at least one representative from executive management? Does the team have the authority to declare the disaster and coordinate necessary recovery activities?
- Is there an Incident Response Plan and does it include a contact list and procedures for contacting necessary personnel?
- Are manual overrides available to allow operation of key processes?
- Are written SLAs established for all identified external dependencies? Are expectations for response times/restoration included? Are they exercised to ensure external organizations can realistically meet demands?
- Are SLAs with staff and contracted employees established to respond in emergency conditions?

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.



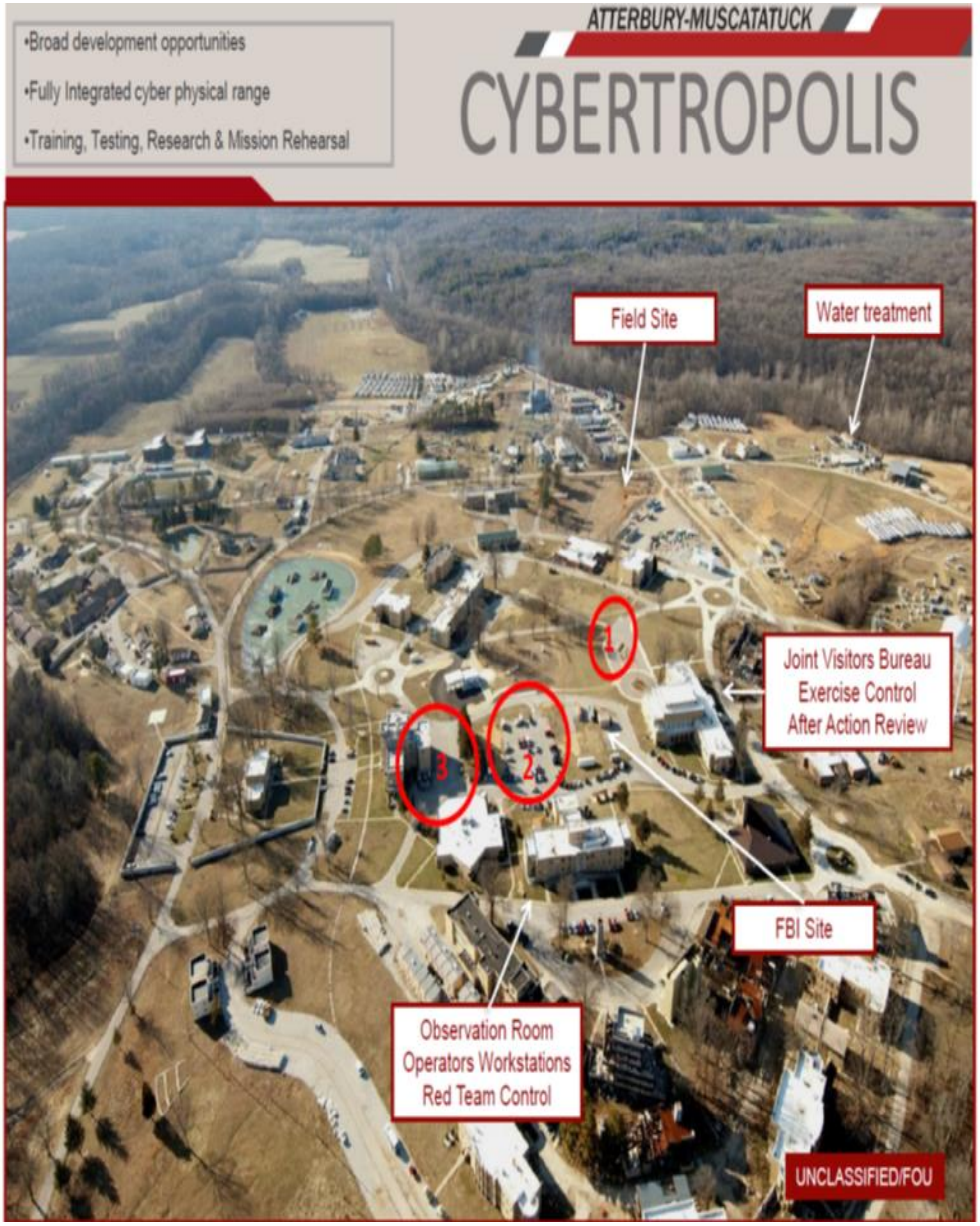
Exercise OBJ 4: Provide water utility observers with the training that empowers them for a real world emergency, identifying key decision points and decision-making

	Intel/ Info Sharing	Sit Asst	Infrastructure Systems	Op Coms	Op Cord	Cyber security	Access Control	Physical Protective Measures	Risk/Disaster Resilience Assessment	Community Resilience	Risk Management for Protection Programs & Activities	Interdiction & Disruption
Governance/ Risk Management		X				X			X	X		
Business Cont/ Disaster Recovery		X	X			X			X	X		
Server/Work station Hardening	X					X			X			
Access Control						X			X			
Application Security						X			X			
Encryption						X			X			
Telecomms/ Network Sec/Arch	X					X			X			
Physical Security of PCS Equipment						X			X			
Service Level Agreements		X	X			X			X	X		
OPSEC						X			X			
Education	X					X			X	X		
Personnel Security						X			X			

Most Relevant Questions:

- Does the organization have consistent contact with intelligence organizations to stay abreast of current threat TTPs? Are changes made to security procedures based on available intelligence?
- Are procurement policies leveraged to limit the number of external support organizations?
- Is a Crisis Management Team identified with at least one representative from executive management? Does the team have the authority to declare the disaster and coordinate necessary recovery activities?
- Are manual overrides available to allow operation of key processes?
- Are strategies in place to provide redundancy of key system components and can they be implemented within an acceptable timeframe?
- Are written SLA established for all identified external dependencies? Are expectations for response times/restoration included? Are they exercised to ensure external organizations can realistically meet demands?
- Are SLA with staff and contracted employees established to respond in emergency conditions?

Appendix C: Muscatatuck Urban Training Center Map & Locations



- “Lot 1” is reserved for ranking officials and specially designated VIPs.
- Players and VIP’s will be asked to park in “Lot 2”.
- Exercise control personnel will be asked to park in “Lot 3”.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Appendix D: Exercise Participants

State, Local and Federal Government
Indiana Department of Homeland Security
Infragard Indiana
Indiana Office of Technology
Indiana National Guard
Indiana Utility Regulatory Commission
Indiana State Police
Indiana Information Sharing & Analysis Center (IN-ISAC)
US Department of Homeland Security
Federal Bureau of Investigation

Utilities
Carmel Utilities
Citizens Energy Group/Citizens Water
Evansville Water and Sewage
Fort Wayne Utilities
Indiana American Water
Indiana Energy Association
Michigan City Water Department

Private Sector
Cyber Leadership Alliance
Frakes Engineering
Pondurance
Rook Security

Academia
Indiana University
Purdue University

Appendix E: Exercise Planning Team Members

Participant	Role
David Kane	Exercise Co-Director
Jennifer de Medeiros	Exercise Co-Director
Jim McHugh	Exercise Co-Director
Participant	**Role**
Doug Rapp, CLA	Exercise Planning Team Leader
Participant	**Role**
Jennifer de Medeiros	Exercise Planning Core Team
Jim McHugh	Exercise Planning Core Team
Cliff Campbell	Exercise Planning Core Team
John Lucas	Exercise Planning Core Team
Doug Rapp	Exercise Planning Core Team
LTC Dave Skalon	Exercise Planning Core Team
MAJ Stacy Kennedy Barker	Exercise Planning Core Team
Tad Stahl	Exercise Planning Core Team
Nick Sturgeon	Exercise Planning Core Team
Andy Mapes	Exercise Planning Core Team
John Erickson	Exercise Planning Core Team
Chris Collins	Exercise Planning Core Team
Michael Taylor	Exercise Planning Core Team
JJ Thompson	Exercise Planning Core Team
Mark Vogler	Exercise Planning Core Team
Participant	**Role**
John Lucas	Technical Working Group
Chris Collins	Technical Working Group
JJ Thompson	Technical Working Group
Mark Vogler	Technical Working Group
Cliff Campbell	Technical Working Group
Michael Taylor	Technical Working Group
Landon Lewis	Technical Working Group
Tom Gorup	Technical Working Group
Toby Church	Technical Working Group
Tony Vespa	Technical Working Group
Joe Smith	Technical Working Group
Sabrina Couturier	Technical Working Group
Dan Ford	Technical Working Group
Rushabah Vyas	Technical Working Group
Participant	**Role**
John Erickson	Public Affairs
Amber Kent	Public Affairs
David Roorbach	Public Affairs
Stacy Kennedy Barker	Public Affairs
Jennifer de Medeiros	Public Affairs

Participant	Role
Jonathan Witham	Legal
Brad Gavin	Legal
Jim Ehrenberg	Legal
Kelsey Colvin	Legal
Jeremy Comeau	Legal
Ryan Locke	Legal
Participant	**Role**
MAJ Stacy Kennedy Barker	MUTC
CAP Jonathan Rupel	MUTC
LTC Dave Skalon	MUTC
Phil Barker	MUTC
Gary Deckard	MUTC

SECTION 4: INFORMATIONAL APPENDICES

The following section includes background and example information related to cybersecurity threats and attacks on the power grid.

Appendix F: Background Information

BlackEnergy Malware

BlackEnergy was first identified several years ago as a type of malware used to launch distributed denial of service attacks (DDoS) and steal information. The majority of BlackEnergy's computer coding appears designed to conduct highly sophisticated monitoring and recording of data – a tactic known as "sniffing." However, more recent versions of BlackEnergy, such as BlackEnergy3, have evolved into an advanced persistent threat (APT) tool used in significant geopolitical operations, including Russia, Poland, and most recently Ukraine.

Experts worry that versions of BlackEnergy could be programmed to damage pieces of critical infrastructure by hacking into its control system, since its complexity hints at a highly skilled team of hackers with a broad technical background. This latest version of BlackEnergy is "modular," making it much easier for hackers to quickly change how the malware works, and significantly harder for security analysts to find and root it out.

Also worrisome is the proliferation of BlackEnergy malware. The US Department of Homeland Security has already identified BlackEnergy malware deep within industrial control systems that operate critical infrastructure, and evidence is mounting that the bug has already been deployed around Europe and is "sleeping" until activated. Cybersecurity analysts say they are sure the bug will continue to spread, and that will lead to many more blackouts and "mysterious" malfunctions in national power grids, transportation, and other industrial infrastructure.

SQL Injection

SQL injection ("Improper Neutralization of Special Elements Used in an SQL Command") is at the top of the most recent CWE/SANS Top 25 Most Dangerous Software Errors list and must be taken seriously. [1] SQL injection occurs when untrusted user-supplied data is entered into a web application and that data is then used to dynamically create a SQL query to be executed by the database server.

If a web application is vulnerable to SQL injection, then an attacker has the ability to influence the SQL that is used to communicate with the database. The implications of this are considerable. Databases often contain sensitive information; therefore, an attacker could compromise confidentiality by viewing tables. An attacker may also jeopardize integrity by changing or deleting database records using SQL injection. In other words, an attacker could modify the queries to disclose, destroy, corrupt, or otherwise change the underlying data. It may even be possible to login to a web application as another user with no knowledge of the password if non-validated SQL commands are used to verify usernames and passwords. If a user's level of authorization is stored in the database it may also be changed through SQL injection allowing them more permissions then they should possess. If SQL queries are used for authentication and authorization, an attacker could alter the logic of those queries and bypass the security controls set up by the admin.

Web applications may also be vulnerable to second order SQL injection. A second order SQL injection attack occurs when user-supplied data is first stored in the database, then later retrieved and used as part of a vulnerable SQL query. This type of SQL injection vulnerability is more difficult to locate and exploit. Exploitation does not end when the database is compromised, in some cases an attacker may be able to escalate their privileges on the database server, allowing them to execute operating system commands.

Remote Access Trojans

Remote Access Trojans (RATs) provide cybercriminals with unlimited access to infected endpoints. Using the victim's access privileges, they can access and steal sensitive business and personal data – including intellectual property and personally identifiable information. While automated cyberattacks allow cybercriminals to attack browser-based access to sensitive applications, RATs are used to steal information through manual operation of the endpoint on behalf of the victim. Most Advanced Persistent Threat (APT) attacks take advantage of RAT technology for reconnaissance, bypassing strong authentication, spreading the infection, and accessing sensitive applications to exfiltrate data. RATs are commercially available (e.g. Poison Ivy, Dark Comet) and can be maliciously installed on endpoints using drive-by-download and spear phishing tactics.

Phishing

The act of tricking individuals into divulging sensitive information and using it for malicious purposes is not new. Social engineering attacks have occurred on the internet throughout its existence. Before widespread use of the internet, attackers used the telephone to pose as a trusted agent to acquire information. The term "phishing" has origins in the mid-1990s, when it was used to describe the acquisition of ISP account information. However, today the term has evolved to encompass a variety of attacks that target sensitive information.

Hackers targeting user information are able to profit from the increased adoption of online services for many day-to-day activities, including banking, retail, and email communication. Users of these services provide a target of opportunity in that they possess information of value. Along with an increase in the number of potential targets, there are three major factors that hackers have been able to take advantage of:

> **Unawareness of threat** - If users are unaware that their information is actively being targeted by hackers, they may lack the perspective needed to identify phishing threats and may not take the proper precautions when conducting online activities.
>
> **Unawareness of policy** - Phishing scams often rely on a victim's unawareness of organizational policies and procedures for dealing with suspicious email communication. Employees unaware of the policies of an organization are likely to be more susceptible to the social engineering aspect of a phishing scam, regardless of technical sophistication.
>
> **Hacker technical sophistication** - Hackers conducting phishing scams are leveraging technology that has been successfully used for activities such as spam, distributed denial of service (DDoS), and electronic surveillance. Even as organizations are becoming aware of phishing, hackers have responded with technical tricks to make phishing scams more deceptive and effective.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

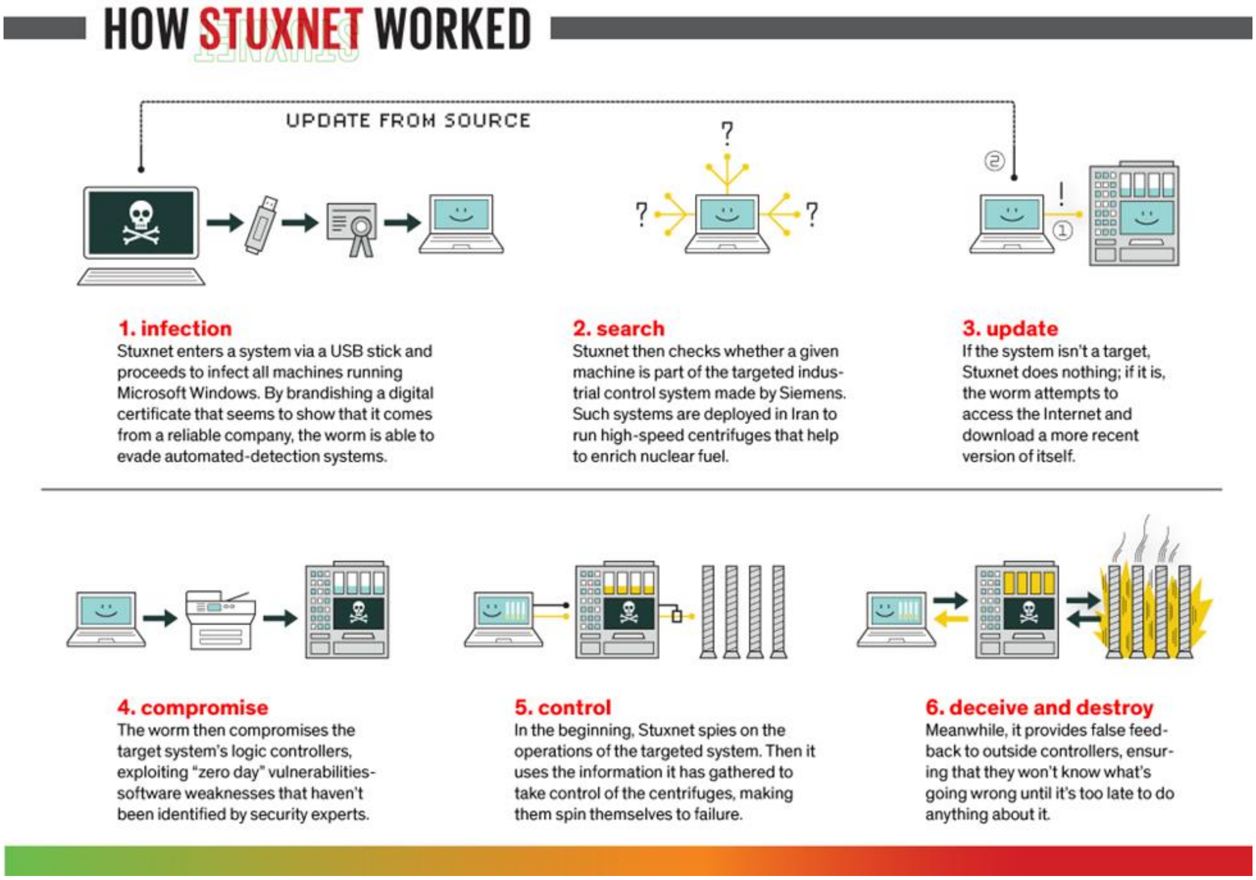
Appendix G: Case Studies

Stuxnet

One of the most famous cases involving the infection of an air-gapped system is Stuxnet, the virus/worm designed to sabotage centrifuges used at a uranium enrichment plant in Iran.

Although a computer virus relies on an unwitting victim to install it, a worm spreads on its own, often over a computer network. First, it targeted Microsoft Windows machines and networks, repeatedly replicating itself. Then it sought out Siemens Step7 software, which is also Windows-based and used to program industrial control systems that operate equipment, such as centrifuges. Finally, it compromised the programmable logic controllers, the heart of a SCADA system. The worm's authors could thus spy on the industrial systems and even cause the fast-spinning centrifuges to tear themselves apart, unbeknownst to the human operators at the plant.

.



1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

Verizon 2015 Data Breach Report

Phishing campaigns are still surprisingly effective. In the 2015 Data Breach Report, Verizon states that 23% of included recipients were found to have opened phishing messages and no less than 11% clicked on corresponding attachments. In addition, if a hacker sends out 10 emails, there is an astonishing 90% chance that at least one person will fall victim to their attack. The Verizon report also demonstrates that phishing attacks produce extremely fast results. Two of Verizon’s security awareness partners sent out 150,000 phishing emails to see how many people would open the emails and what percentage would click on the links inside them. The data showed that 50% of recipients opened the email and clicked on phishing links within the first hour, with the first clicks coming in after only one minute. This report proves just how easy it is for hackers to gain access to sensitive information via simple phishing attacks. Large businesses are even more prone to these types of attacks because it can be hard to monitor the email activities of a large workforce depending on the resources each organization has.

When referring to the phishing attacks on the utility sectors, BlackEnergy used Microsoft Office documents containing malicious macros in phishing/spear-phishing attacks where the target receives an email containing an attachment with a malicious document. The document itself contains text trying to convince the victim to run the macro in the document. If victims are successfully tricked, they end up infected with BlackEnergy Lite. From there the attacker can pivot anywhere inside the network affecting critical utility controls and services.

KWC Water Plant

Hackers infiltrated a water utility’s control system and changed the levels of chemicals being used to treat tap water, according to Verizon Security Solutions. Verizon describes the attack against the "Kemuri Water Company,” a pseudonym for a real firm in an unspecified country, in this month’s IT security breach report. A "hacktivist" group with ties to Syria compromised Kemuri's computers after exploiting unpatched web vulnerabilities in a payment portal that was connected to the public Internet.

The hack, which involved SQL injection and phishing - was made easier because login credentials for the operational control system were stored on the web server. The system regulated valves and ducts that controlled the flow of water and chemicals used to treat it. Verizon discovered four separate connections over a 60-day period. During these connections, the threat actors modified application settings with little apparent knowledge of how the flow control system worked. In at least two instances, they managed to manipulate the system to alter the amount of chemicals that went into the water supply and thus handicap water treatment and production capabilities so that the recovery time to replenish water supplies increased. Fortunately, based on alert functionality, KWC was able to quickly identify and reverse the chemical and flow changes, largely minimizing the impact on customers. No clear motive for the attack was found.

The hacktivists had manipulated the valves, controlling the flow of chemicals twice – though fortunately to no particular effect. It seems the activists lacked either the knowledge or the intent to do any harm. The same hack also resulted in the exposure of personal information of the utility’s 2.5 million customers. There’s no evidence that this has been used for fraud.

Appendix H: Cybersecurity Glossary

Access control: The process of granting or denying specific requests for or attempts to: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities.

Advanced Persistent Threat: An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception).

Alert: A notification that a specific attack has been detected or directed at an organization's information systems.

Antivirus software: A program that monitors a computer or network to detect or identify major types of malicious code and to prevent or contain malware incidents – sometimes by removing or neutralizing the malicious code.

Blue Team: A group that defends an enterprise's information systems when mock attackers (i.e., the Red Team) attack, typically as part of an operational exercise conducted according to rules established and monitored by a neutral group (i.e., the White Team).

Bot: A computer connected to the Internet that has been surreptitiously / secretly compromised with malicious logic to perform activities under the command and control of a remote administrator.

Bot master: The controller of a botnet that, from a remote location, provides direction to the compromised computers in the botnet**.**

Computer network defense: The actions taken to defend against unauthorized activity within computer networks.

Continuity of Operations Plan: A document that sets forth procedures for the continued performance of core capabilities and critical operations during any disruption or potential disruption.

Cyber ecosystem: The interconnected information infrastructure of interactions among persons, processes, data, and information and communications technologies, along with the environment and conditions that influence those interactions.

Cyber infrastructure: An electronic information and communications systems and services and the information contained therein.

Cybersecurity: The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.
Denial of Service: An attack that prevents or impairs the authorized use of information system resources or services.

Distributed Denial of Service (DDoS): A denial of service technique that uses numerous systems to perform the attack simultaneously.

Encryption: The process of transforming plaintext into cipher text.

Firewall: A capability to limit network traffic between networks and/or information systems.

Hacker: An unauthorized user who attempts to or gains access to an information system.

Industrial Control System: An information system used to control industrial processes such as manufacturing, product handling, production, and distribution or to control infrastructure assets.

Inside(r) threat: A person or group of persons within an organization who pose a potential risk through violating security policies.

Keylogger: Software or hardware that tracks keystrokes and keyboard events, usually surreptitiously/secretly, to monitor actions by the user of an information system.

Malicious code: Program code intended to perform an unauthorized function or process that will have adverse impact on the confidentiality, integrity, or availability of an information system.

Passive attack: An actual assault perpetrated by an intentional threat source that attempts to learn or make use of information from a system, but does not attempt to alter the system, its resources, its data, or its operations.

Penetration testing: An evaluation methodology whereby assessors search for vulnerabilities and attempt to circumvent the security features of a network and/or information system.

Phishing: A digital form of social engineering to deceive individuals into providing sensitive information.

Red Team: A group authorized and organized to emulate a potential adversary’s attack or exploitation capabilities against an enterprise’s cybersecurity posture.

Remote-Access Trojan: A malware program that includes a back door for administrative control over the target computer. RATs are usually downloaded invisibly with a user-requested program or sent as an email attachment.

Spyware: Software that is secretly or surreptitiously installed into an information system without the knowledge of the system user or owner.

Supervisory Control and Data Acquisition: A generic name for a computerized system that is capable of gathering and processing data and applying operational controls to geographically dispersed assets over long distances.

Threat: A circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact (create adverse consequences for) organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society.

Trojan horse: A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

Virus: A computer program that can replicate itself, infect a computer without permission or knowledge of the user, and then spread or propagate to another computer.

Watering Hole Attack: a security exploit in which the attacker seeks to compromise a specific group of end users by infecting websites that members of the group are known to visit. The goal is to infect a targeted user's computer and gain access to the network at the target's place of employment.

White Team: A group responsible for refereeing an engagement between a Red Team of mock attackers and a Blue Team of actual defenders of information systems.

Worm: A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.

Appendix I: Acronyms

AAR: After action report

APT: Advanced persistent threat

AWWA: American Water Works Association

CS: Cybersecurity

DDoS: Distributed denial of service

DHS: Department of Homeland Security

DMZ: Demilitarized Zone

EEG: Exercise evaluation guide

EMA: Emergency management agency

FOUO: For Official Use Only

HMI: Human-Machine Interface

HS: High Service

HSEEP: Homeland Security Exercise & Evaluation Program

ICS: Industrial control system

I/IS: Intelligence & Information Sharing

IDHS: Indiana Department of Homeland Security

IN-ISAC: Indiana Information Sharing & Analysis Center

INNG: Indiana National Guard

IOT: Indiana Office of Technology

IS: Information Security

IT: Information Technology

MUTC: Muscatatuck Urban Training Center

OC: Operational Coordination

OCOM: Operational Communications

PCS: Process Control System

PLC: Program Logic Controller

RAT: Remote-Access Trojan

SCADA: Supervisory Control & Data Acquisition

EXPLAN: Exercise Plan

TTPs: Tactics, Techniques, and Procedures

USB: Universal Serial Bus

VLAN: Virtual Local Area Network

National Governors Association (NGA)
Workshop Cyber Toolkit Materials

August 2018

August 23: Cybersecurity Risk Toolkit

- Chetrice Mosley Presents Indiana Cybersecurity Scorecard
  - Changing the culture of cybersecurity
  - We could not find risk assessments that were basic enough and non-IT
  - Scorecard can apply to any entity (risk assessment in the toolkit is more operational and specific to emergency managers)
- Carlos Garcia, IU Emergency Management and Joe Romero – IU Health Presentation
  - We want emergency managers to understand the cyber threat and know how to respond pre-disaster, during disaster, and post-disaster
  - We need mitigation
  - We need preparedness—planning, training, exercise
  - We need response
  - New threat environment
    - Emergency managers simply do not have enough background to even ask the right questions on cybersecurity
    - Emergency managers tend to be reluctant to admit they do not know something, or admit they need help
    - The assessment models are just as confusing as the problem
  - Goal
    - Treat cyber risk as every other hazard
    - Convincing someone with no IT background to treat this as every other hazard
      - Assess the situation (risk assessment tool)
      - Plan (incident planning template)
      - Train and exercise (guides)
    - Key features of toolkit
      - Align NIST and FEMA/USDHS guidance
      - Preparedness Cycle model
      - Non-technical target audience
      - Ease of use
    - Risk assessment methodology
      - Incorporates NIST 800-30, CPRI, CARVER models
      - Risk measures: vulnerability, threat, impact recovery, preparedness
        - RISK = (vuln + threat + impact) – (recovery + preparedness)
        - We did not factor in probability or likelihood, assuming that the person would not know
      - User-friendly interface, easy to understand questions (turbo tax for cyber)
      - Specific to adversarial threats, most common attacks
      - Assesses internal risk based on self-reporting
    - Question: Are you going to compare entities that fill out the risk assessment?
      - Joe: No, it will be focused on the local government entity alone
- Speaker presentations

- Matt Barrett, NIST
    - The language of the CF closely aligns with the disaster management mentality of pro, during, and post-incident
    - IPDRR → 22 categories → 98 subcategories ; the value proposition is around communication and standardization—you can focus on whichever level of abstraction you need
    - You have to understand the technical ramifications of non-technical relationships
- Olga Livingston, USDHS
    - The CSF is very useful, but it does not touch on quantification of risk
    - DHS already provides assessments that range from strategic to very tactical, technical assessments
        - Cyber risk resilience review—already touches on some of the questions you already have in the risk scorecard
        - External dependency analysis
        - Cyber infrastructure survey
        - Cyber Hygiene
        - Risk and vulnerability assessment
        - More technical ones
        - Recommendation: Identify ONE core system that is critical for your business function, fix that one, then go to the next. Do not try to do everything at the same time.
    - Quantification of risk
        - ROI
            - Need to communicate loss
            - How are tools going to help you reduce the loss
        - You need more than a heatmap, you need to communicate the benefit of the cybersecurity investment, and that will allow you to explain investment to someone who might rather spend the money on a fire truck
    - DHS needs much better data to figure out the average cost of a cyber incident
        - One dataset from insurers says
            - Average is about $400,000
            - Median is $50,000
        - Other datasets say something completely different
    - Note that you need to introduce uncertainty into analysis, and pure ranking does not capture that
    - You need to form a partnership with your universities, look at students for capstones to help you solve these problems
- Doug Hormann, Raytheon
    - Risk analysis
    - First we identify critical elements in the system
    - Probability derives from

    - Accessibility
    - Exploitability (pairings of threats and vulnerabilities)
    - Capability of adversaries (threat analysis)
  - Indiana has to think about information sharing—how are emergency managers going to share information about the threats
  - Explaining what categories actually mean is critical
  - Key question: how are emergency managers going to deal with vulnerabilities that they do identify?
- Amanda Joyce, Argonne National Laboratory
  - Identifying the key people in the organizations who can actually answer the questions are often not the same person, and figuring out who can answer these assessment questions is the first priority
  - We will never reduce risk to zero
  - CPRI: this is what DHS uses in their cyber infrastructure survey tool, based on a comparability model because it lets you know where you stand in comparison to others, so then you can ask the people who are doing better, how they do it
  - We usually do not have visibility into all of our assets
  - How can you define intangible risk? You cannot necessarily quantify all risk, such as political risk for local officials
- Andrea LeStarge, Deloitte
  - Convergence of physical and cybersecurity to understand overall risk
  - Deloitte worked with another state on something very similar to what is happening in Indiana
  - Leverage threat liaison officers to get you connected to cyber liaison officers, because they are the ones who can help you fill out the tool you are designing
  - Lots of duplication across the response enterprise, so we looked at all the functions, and we had an entire matrix that went through each of the IPDRR
  - Information sharing is critical, so you need to adapt your SAR program to cybersecurity
  - We had a governor's executive order stemming from the President's EO, saying this state will have a response plan, we will disseminate a questionnaire to "open the door," then allowing the CLOs and TLOs to undertake more detailed assessments, we then created a tactical operations plan
- Questions
  - How do you incorporate human behavior?
    - It falls under the PROTECT component for training.
    - System protection, intrusion detection, adversary analysis—there is a human component in all of that; but you cannot fix stupid, so what are the administrative, procedural, and technical controls that you can implement that assumes humans will make the mistake
    - This is also why training and exercising is so important, because it allows you to assess whether behavior is actually changing

      - The NICE Framework is certainly relevant when it comes to training and behavior, because it does touch on behavior and intangible properties of behavior
      - It can be easier to measure behavior when you get more tactical, e.g., phishing
      - From an emergency management perspective, attribution is not necessarily possible, which is why information sharing is so important
  - Risk Assessment Tool Presentation
    - Key questions
      - Are we sure they will be able to answer all these questions?
      - Does the tool conflate risk assessment for the emergency manager versus risk assessment for the entire county?
    - Vulnerability
      - Critical infrastructure: need to discuss this piece of the vulnerability assessment
        - Initial thought was to include those that counties would have authority to manage
        - Does it need to include more sectors?
        - Does it need to include non-critical infrastructure?
        - Does it make sense to start with just the emergency managers, and then that becomes the conversation starter with the critical infrastructure companies—you cannot make this too big
    - Threats: methods of attack generated automatically
      - Who is the "we" in "we are vulnerable to these threats?" Are the attack vectors those that apply to the emergency manager's organization, or vectors that apply to all organizations under their potential purview?
    - Impact: criticality and harm
    - Recovery
      - How do you define normal operations?
    - Preparedness
    - Scoring
      - Based on NIST 800-30
    - Heat map displaying most serious problems

Facilitation

- Who is the audience?
  - District coordinators
  - Emergency management directors
  - County elected officials
    - Basic education level in some cases
  - County emergency managers
    - They have a large workload, so we need to make the assessment simple
  - This could be delegated to other audiences

- Reason for focusing strictly on emergency manager is because they are the focal point, the central point of coordination for law enforcement, EMS, and others, and they will have the path to success
- Purpose of assessment
    - Educate the center of the storm
    - Provide information to educate others
    - Start conversations with local practitioners/subject matter experts
    - Understand the threat to appropriately mitigate
    - Integrate cyber into all-hazards approach
    - Demystify cybersecurity
    - Decision aid to inform action
    - Know what risks they accept
        - **Either define it, add probability, or eliminate this**
    - Convene cross-sector representatives
    - Inward facing preparedness
    - Intelligence gathering
    - Ultimately, this is looking inward, within the emergency management agency

- This is meant to generate the conversation with those who own the infrastructure
- None of this is weighted yet; but it could be weighted based on the criticality of its impact
- How do you figure out which needs the most help
- What is the so what? What happens afterwards?
    - This moves to the plan factor
    - What is the state going to do next?
        - Inform the state of where to put their money to assist folks
- Maybe it is better to look at this as this as a survey to open the door, and then we do a real, in-depth assessment
- The action this is supposed to create is to create a response plan; to kick start the preparedness process
- Have to assess how the agencies can protect themselves, before they can support everyone else (putting their oxygen mask on first)
- What is the outcome you are trying to change?
    - Creating an IRP
    - Exercising IRP

Pros	**Cons/Improvements**
It is a clear process and feedback	Need to define terminology: put it in simple terms. E.g. ransomware is extortion Identify/define the jargon words
Hover-over feature is good	Does not delineate intent or capabilities of attackers
Turbo Tax phrase is useful	Does not address lifecycle

	Get rid of overall score because it will make people panic or misinterpret their actual risk. Make sure to call out the red areas, and not aggregate it with the green, so you can see what the true negative impact is. Need to change the mindset that just because you have an 80/100 score, that is not good enough. Don't want to lull people into a false sense of security
Self-assessment	Set a risk tolerance, perhaps
	No weighting of CI
	Shouldn't put CI at the same level as the other Infrastructures, because the latter are all dependencies on CI
	Need to be careful of what people's motives are when they do self-assessments
	Need to describe the threshold for what is "yes" or "no" when selecting an option
	Ends up treating all CI as the same
	Lack of what next
	Does not address the probability of the threat occurring; realistically, it would be useless/impossible
	No human factor
	Maybe we look at this as a survey to open the door, and then perform a real, in-depth assessment. If you call it an assessment, then people will not want to score low. But survey is more benign
	Pushing a lot of terms, and the cyber concept in general, without any context/training
	Is IT technology equipment too narrow? How do you define it
	Need to show that all hazards can effect cybersecurity (heat wave can impact technology)
	Need to include mutual aid and how it applies to cyber

Vulnerability

What is missing?

- Government facilities
    - Need to define this
    - Need to define emergency services
- Where are they key nodes for where communications come into the county?
- Network infrastructure needs to include security equipment
- How do you quantify the human vulnerability?
- Policies to operations

Threats

- Need to simplify methods
- Differentiate between techniques and methods; ensure that methods of attacks and their payloads are correct and defined
- Consider using anecdotes with each threat type and the risk associated with that

Impact

- The impact to the CI never changes; what matters is how you reduce the risk to avoid that impact
- This is business impact analysis

Recovery

- Recovery is restoration of services
- Need to include short term and long-term recovery
- Need to translate/crosswalk terminology
- Adjust this so it includes long term outage of a service, perhaps
- DR Recovery strategy without accounting for attacks
- Need to ask if they have a DR strategy and then ask specifics

Preparedness

- Prevention, detection, mitigation under preparedness
    - Information security (password management, firewalls, cyber hygiene, what are you doing to keep data safe?)
    - Training and education (also includes cyber hygiene)
- Need to simplify the answers. Want to know the readiness posture
    - Example: do you have a written information security plan? Needs to be concise
        - Do you hold/or participate in exercise and drills
- Need to have the hover box be very detailed