# RESILIENCY AND RESPONSE WORKING GROUP STRATEGIC PLAN

Chair: Adjutant General, Brigadier General Dale Lyles
Co-Chair: Executive Director Stephen Cox

October 2021
Indiana Executive Council on Cybersecurity

# Resiliency and Response Working Group Plan

# Table of Contents

**Committee Members ........ 4**

**Introduction ........ 7**

**Executive Summary ........ 9**

**Research ........ 14**

**Deliverable: State Cyber Exercises ........ 20**

General Information ........ 20

Implementation Plan ........ 21

Evaluation Methodology ........ 26

**Deliverable: Cyber Emergency Response Education to Local Law Enforcement ........ 30**

General Information ........ 30

Implementation Plan ........ 31

Evaluation Methodology ........ 34

**Deliverable: Emergency Manager Cybersecurity Toolkit 3.0 ........ 36**

General Information ........ 36

Implementation Plan ........ 37

Evaluation Methodology ........ 41

**Deliverable: Cyber Annex and Cyber Liaison ........ 43**

General Information ........ 43

Implementation Plan ........ 44

Evaluation Methodology ........ 48

**Deliverable: INNG Cyber State Capabilities ........ 49**

General Information ........ 49

Implementation Plan ........ 50

Evaluation Methodology ........ 53

**Supporting Documentation ........ 55**

Indiana Cyber Exercise News Release and News Coverage ........ 56

Muscatatuck Urban Training Center Homeland Defender Info Sheet ........ 66

Indiana Emergency Manager Cybersecurity Toolkit 2.0 ........ 71

Indiana Cyber Emergency Resiliency Response State Guide ........ 155

Integrated Preparedness Information Handout ........ 166

# Committee Members

## Committee Members

| Last Name | First Name | Organization | Organizational Title | Member Type (Chair/Co-chair/Full-time, As needed) |
|---|---|---|---|---|
| Alley | Mike | Resilient Strategies, LLC | President | Full Time |
| Baldwin | Ashley | Indiana Department of Homeland Security | State Exercise Officer | As Needed |
| Barefoot | Jonathon | IU Health | Vice President | Full Time |
| Cox | Stephen | Indiana Department of Homeland Security | Executive Director | Co-Chair |
| Day | David R. | MISO Energy | Consulting Information Security Analyst | Full Time |
| Tooley | Benjamin | Indiana National Guard | J36 Defensive Cyber Programs | Full Time |
| Hackett | Jeffrey (Col) | Indiana National Guard | External Affairs and Alliances | Co-Chair Proxy |
| Justice | Connie (Dr.) | IUPUI | Professor | Full Time |
| Lucas | John | Citizens Energy Group | Vice President, IT | Full Time |
| Lyles | Dale (BG) | Indiana National Guard | Adjutant General | Chair |
| Moran | Mary | Indiana Department of Homeland Security | Response and Recovery Director | Full Time |
| Neel | David | CyberTek MSSP | Chief Technical Officer | As Needed |
| Musgrave | Anthony | Indiana National Guard | J36 Defensive Cyber Programs | Full Time |
| Reuter | Ed | Indiana Statewide 911 Board | Executive Director | As Needed |
| Rogers | Marcus | Purdue Polytechnic | Professor/Executive Director Cybersecurity Programs/Chief Scientist HTCU | As Needed |
| Rogowski | Peri | Indiana Department of Homeland Security | State Planning Director | As Needed |
| Romero | Joseph | IU Health | Emergency Preparedness Program Manager | Full Time |
| Skalon | Dave | Indiana National Guard | Chief Information Officer | Full Time |

| | | | | |
|---|---|---|---|---|
| Winslow (BG) | Timothy | Indiana National Guard | Director of the Joint Staff | Chair Proxy |
| Goldsmith | Reid | Indianapolis International Airport | Senior Director Information Technology | As Needed |
| Mackey | William | Indiana State University | Instructor | As Needed |
| Dignin | Kelly | Integrated Public Safety Commission | Director of Network Services | Full Time |
| Ferrante | Anthony | FTI Consulting | Global Head of Cybersecurity, Senior Managing Director | As Needed |
| Potchanant | Joe | Indiana University REN-ISAC | Director of Member Services and Support | As Needed |
| Pelletier | Ronald W. | Pondurance | Founding Partner | As Needed |
| Aikman | J. Kurt | MISO Energy | Senior Security Advisor | As Needed |
| Linder | Jared | Family and Social Services Administration | Chief Information Officer | As Needed |
| Vare | Todd | Barnes & Thornburg LLP | Partner | As Needed |
| Redman | Justin | Citizens Energy Group | Manager Water System Control and Planning | As Needed |
| Neely | Dewand | MGT Consulting | Chief Information Officer | As Needed |

# Introduction

# Introduction

The world of cybersecurity is highly complex and cluttered with information, misinformation, and disinformation. As a consequence, it is important to approach it strategically and create simplicity.

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) continues its mission to move efforts and statewide cybersecurity initiatives to the "Next Level." With the ever-growing threat of cyberattacks, protecting Indiana's critical infrastructure is the focus of the IECC. Cybersecurity cannot be solved by one entity alone. The IECC works with private, public, academic, and military partners from all over the state to develop and maintain a strategic framework that establishes goals, plans, and best practices for cybersecurity.

The IECC is comprised of fifteen committees and working groups who have worked together to implement the statewide strategy of 2018 while developing an updated comprehensive strategic plan.

The following implementation plan is one of the fifteen specific plans that encompass the complete *2021 Indiana Cybersecurity Strategic Plan*.

For more information, visit www.in.gov/cybersecurity.

# Executive Summary

# Executive Summary

- **Research Conducted**
    - **Cybersecurity and Infrastructure Security Agency (CISA):** CISA leads the Nation's strategic and unified work to strengthen the security, resilience, and workforce of the cyber ecosystem to protect critical services and American way of life.
    - **National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF):** Helping organizations to better understand and improve their management of cybersecurity risk.
    - **National Institute of Standards and Technology (NIST) Risk Management Framework (RMF):** The NIST Risk Management Framework (RMF) provides a comprehensive, flexible, repeatable, and measurable 7-step process that any organization can use to manage information security and privacy risk.
    - **Multi-State Information Sharing and Analysis Center (MS-ISAC):** The mission of the MS-ISAC is to improve the overall cybersecurity posture of the nation's state, local, tribal and territorial governments through focused cyber threat prevention, protection, response, and recovery.
    - **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.

    - **2018 Pre- thru Post- Cyber Incident Working Group Primary and Secondary Research Conducted:**
        - Each of the sector sub-groups was tasked to create a white paper specific to their area. The goal of these papers is to identify organic cyber capabilities and capability gaps within Indiana to better inform decision makers allowing us to prioritize and apportion limited resources to support the needs of the state's critical infrastructure.
        - Since October 2017, the team has been working to capture and examine other state cyber response plans in an effort to identify the best of the best to assist the IECC in creating our own plan.
        - The team also have been exploring the idea of conducting a "GRIDEX-like" exercise for both the water/wastewater and election sectors.

- **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.
    - The NIST Cybersecurity Framework is voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk. In addition to helping organizations manage and reduce risks, it was designed to foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders.
    - There is an abundance of cybersecurity information and services and resources available to individuals, government agencies, and private sector organizations.
    - Within the past few years, the ability to conduct self-assessments for cybersecurity risk have made improvements.  The NIST CSF provides a list of several free tools to assist small to medium sized business (SMB) conduct internal reviews.
        - https://www.nist.gov/cyberframework/assessment-auditing-resources
    - There currently is no central point of coordination and information sharing for state-level cybersecurity planning, training, and exercise activity.
    - There currently is no centralized point for reporting cyber incident attacks occurring within the State of Indiana and coordination is required among various agencies to respond.
    - Incident Response support of federal or state resources is agency dependent based upon the attack victim’s line of business (healthcare, financial, local government, state government, or whether a crime has been committed).

- **2018 Pre- thru Post- Cyber Incident Working Group Primary and Secondary Research Findings:**
    - Based on initial findings from our research, we see the need to look not only at the Energy sector but also into other sectors especially water and waste-water treatment to coordinate response and prevention. The main effort of most plans appears to be Energy Sector centric, specifically targeting the Electric sub-sector. While an attack on this sector would be far reaching, it is also a sector with much regulation, governance, established response protocols and exercise programs. We propose that the State also look at other sectors to exercise during the planning phase. Two that are valuable are the water/wastewater and State election systems. Unlike Energy where the loss of power is seen immediately, the contamination of a water source assisted by a cyberattack could go undetected and have a far-reaching impact.
    - According to the Indiana Utility Regulatory Commission, there are 555 water utilities in the State of Indiana. The Environmental Protection Agency (EPA) estimates of $14 billion capital investments required over the next 20 years to update its aging infrastructure. These costs will directly compete with capital investment into cybersecurity. Penetration testing is not the total answer. In a Pre-Incident environment and the thousands of organizations spread across all sectors within Indiana, there is simply not enough capability in Department of Homeland Security (DHS), National Guard, or the Private sector to accommodate even a fraction of the need. Our efforts would be better served on "teaching them to fish" method of outreach and training thru sector exercises would be a better use of these limited resources and farther reaching than a penetration assessment alone.
    - We would recommend that the IECC strongly consider developing outreach, training, and exercises for other Sectors.

- **2021 Working Group Deliverables**
    - Exercise
    - Cyber Emergency Response Team (IN-CERT)
    - Emergency Manager Cybersecurity Toolkit 3.0
    - Cyber Annex and Cyber Liaison
    - INNG Cyber State Capabilities

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

- **References**
    - Cybersecurity and Infrastructure Security Agency (CISA)**:** https://www.cisa.gov
    - National Incident Management System (NIMS): https://www.fema.gov/national-incident-management-system
    - Emergency Management Accreditation Program (EMAP): https://www.emap.org/
    - National Institute of Standards and Technology (NIST): Risk Management Framework (RMF): https://csrc.nist.gov/Projects/risk-management/
    - National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF): https://www.nist.gov/cyberframework
    - Multi-State Information Sharing and Analysis Center (MS-ISAC): https://www.cisecurity.org/ms-isac/
    - 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
- American Water Works Agency: https://www.awwa.org/

# Research

# Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
   - Efforts in cyber-preparedness include the following:
     - 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 and Exercise completes Cybersecurity Awareness Workshops for Emergency Management Administrators (EMAs) in districts 1, 2, 3, and 4.
     - Continuity/Cybersecurity workshops are brought into local jurisdictions, designed by Federal Emergency Management Agency (FEMA) and US DHS.
     - A Cyber Incident Response Annex was completed November 2019.

   - 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
     - CyberShield 2019
     - Homeland Defender 2021

2. **What (or who) are the most significant cyber vulnerabilities in your area?**
    - Critical infrastructures and emergency service sectors
    - 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 must 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, and etc.

3. **What is your area's greatest cybersecurity need and/or gap?**
    - Resources to serve all those in need during a multi-event cyber response crisis.
    - 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**. Public Safety**
- The Working Group requested that the following authorities, as listed in the State of Indiana's Cyber Emergency Response Annex, review the following information 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.
    - 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
  - **State**
    - Cyber Security Framework Strategy For the State of Indiana
    - Indiana Code 10-14-3, Emergency Management and Disaster Law
    - A Leader's Guide to Emergencies and Disasters, IDHS
    - Executive Order 13-09, January 2013
    - Indiana Executive Council on Cybersecurity
  - **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 Department of Homeland Security (DHS) Critical Infrastructure (CISector 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 question #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.
    - 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.
    - The Working 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 answering 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.

11. **What do we need to do to attract cyber companies to Indiana?**
    - The Working 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: State Cyber Exercises

# Deliverable: State Cyber Exercises

## *General Information*

1. **What is the deliverable?**
   a. State Cyber Exercises
      i. INCyber TTX – Aug. 11, 2021
      ii. Indiana Homeland Defender – Aug. 13, 2021
      iii. Indiana Homeland Defender – 2023

2. **What is the status of this deliverable?**
   ☐ Completed ☐ In-progress 25% ☐ In-progress 50% ☒ In-progress 75% ☐ Not Started

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

4. **Which of the following categories most closely aligns with this deliverable?**
   ☐ 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. State Cyber Exercise 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?**
   ☒ 2021 ☐ 2022 ☒ 2023 ☐ 2024 ☐ 2025+

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. Indiana Office of Technology (IOT), Indiana Department of Homeland Security (IDHS), Indiana State Polis (ISP), and Indiana National Guard (INNG)

12. **Who should be main lead of this deliverable?**
    a. Cybersecurity Program Director and INNG

13. **What are the expected challenges to completing this deliverable?**
    a. Completing with current resources and communicating the new program to stakeholders who would benefit.

## *Implementation Plan*

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

☐ One-time deliverable

☒ Ongoing/sustained effort

## Tactic Timeline

**INCyber CISA Exercise – August 11, 2021**

| **Tactic** | **Owner** | **% Complete** | **Deadline** | **Notes** |
|---|---|---|---|---|
| Review and Finalize Cyber Annex | Cybersecurity Program Director/IDHS/IOT/ISP/INNG | 100 | Nov. 2019 | |
| Work with USDHS CISA on planning the scenario | Cybersecurity Program Director/IDHS/IOT/ISP/INNG with USDHS CISA | 100 | December 2020 | |
| Prepare with planning partners in initial, mid, and final planning meetings | USDHS CISA and IECC partners | 100 | Jan-July 2021 | |

| | | | | |
|---|---|---|---|---|
| Hold Exercise | USDHS CISA and IECC partners | 100 | Aug. 11, 2021 | |
| Review AAR | Cybersecurity Program Director and USDHS CISA | 100 | October 2021 | |

**INNG Homeland Defender Exercise – August 13, 2021**

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Update INNG "All Hazards" Plan | INNG J3 | 100 | Sep. 2021 | INNG force packages to respond to state emergencies |
| Exercise County EOC IR Processes | IDHS | 100 | Aug. 2021 | Johnson County EOC |
| Initiate cyber IR component to future exercises | IDHS | 100 | Aug. 2021 | |
| Exercise 1st responder TTPs | Multi-Agency | 100 | Aug. 2021 | |

***Homeland Defender II – 2023**

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Exercise joint civilian and military Critical Infx response exercise | INNG J36 and IDHS | 0% | Aug. 2023 | -EOC Command<br>-IDHS Cyber Fusion Cell |
| Exercise County EOC IR Processes using Emergency Manager Cybersecurity Toolkit 3.0 | IDHS | 0% | | See deliverable below |
| Physical breaches | MUTC | | | Physical Location |
| IT/OT defense | MCTC | | | Cyber Range |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☐No ☒ Yes

| Estimated Initial FTE | Estimated Continued FTE | Skillset/Role | Primary Source of Funding | Alternate Source of Funding | Notes |
|---|---|---|---|---|---|
| 1 | | Exercise Planner | Mix INNG and State | DHS and CISA | IDHS SEO (A. Baldwin) or CISA |
| 1 | | Project Officer | INNG | | Will need to manage on-site coordination and range scheduling at MUTC |
| 3 | May require external vendor or IECC partner with range (Purdue?) | IT Virtual Environment | Unknown | Unknown | Need to develop virtual environment (range) to defend which mimics a city or county administration office |

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

a. No Response

| Resource | Justification/Need for Resource | Estimated Initial Cost | Estimated Continued Cost, if Applicable | Primary Source of Funding | Alternate Source of Funding | Notes |
|---|---|---|---|---|---|---|
| | | | | | | |

## Benefits and Risks

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

a. The Exercises 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. Not having a reviewed, trained, and exercised a cyber incident response plan can have a high impact (and cost) 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?**

☐No ☒ Yes

a. Yes, at varying levels. Requires more research and decisions by working group.

**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. Several other states conduct exercises with partners.

## Other Implementation Factors

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

a. Staff, monetary resources, or administrative priorities could change or slow the timeline of the project down. For INNG, legal and financial review of federal funds used in combined training exercise will be required. DHS or CISA may be able to fund without constraints.

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

☐No ☒ Yes

a. Perhaps a change in internal agencies with 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. Water and Wastewater Committee as well as the Healthcare Committee

**27. Can this deliverable be used by other sectors?**

☐No ☒ Yes,

a. 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)?**

☒No ☐ Yes

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

a. It is important to always the benefit of communicating about the success of an exercise while not over sharing for bad cyber actors to take advantage of in the future.

## *Evaluation Methodology*

**Objective 1:** The State of Indiana will develop and execute a Cross-Sector Critical Infrastructure Cyber Table Top Exercise by August 2021.

*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:** IECC will work with INNG to incorporate a cyber attack into a natural disaster exercise during the Homeland Defender Exercise by August 2021.

*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:** The State of Indiana will develop and execute a Cross-Sector Critical Infrastructure Cyber Operational Exercise by 2023.

*Type:* ☒ Output ☐ Outcome

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

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

# Deliverable: Cyber Emergency Response Education to Local Law Enforcement

# Deliverable: Cyber Emergency Response Education to Local Law Enforcement

## *General Information*

1. **What is the deliverable?**
   a. Cyber Emergency Response Education to Local Law Enforcement

2. **What is the status of this deliverable?**
   ☐ Completed ☒ In-progress 25% ☐ In-progress 50% ☐ In-progress 75% ☐ Not Started

3. **Which of the following IECC goals does this deliverable meet?**
   ☐ 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?**
   ☐ 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. The purpose of Cyber Emergency Response Education to Local Law Enforcement Fact Sheet is to inform local agencies so that when a cyber attack occurs, they are educated about who to call and when.

6. **What metric or measurement will be used to define success?**
   a. Completion of the education materials and distribution to local law enforcement agencies in Indiana.

7. **What year will the deliverable be completed?**
   ☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
    a. local government and law enforcement agencies

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. ISP, IDHS, IOT, FBI, USDHS, US Secret Service

## Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. State and Local Government Committee and Cyber Awareness and Sharing Working Group

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. ISP, IDHS, IOT, FBI, USDHS, US Secret Service

12. **Who should be main lead of this deliverable**?
    a. ISP and Cybersecurity Program Director

13. **What are the expected challenges to completing this deliverable?**
    a. Resources and coming to a consensus of the proper steps in a response between state and federal agencies where appropriate.

## *Implementation Plan*

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

☒ One-time deliverable

☐ Ongoing/sustained effort

## Tactic Timeline

| **Tactic** | **Owner** | **% Complete** | **Deadline** | **Notes** |
|---|---|---|---|---|
| Draft Info Sheet | Cybersecurity Program Director and ISP | 0% | February 2022 | |
| Edit and provide to partners for feedback | Cybersecurity Program Director and ISP | 0% | March 2022 | |
| Finalize | Cybersecurity Program Director and ISP | 0% | May 2022 | |
| Distribute | ISP with IECC partners | 0% | June 2022 | |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☒No ☐ Yes

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

a. No Response

| 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?**

a. When a cyberattack occurs, the efficiency and speed of notifying law enforcement agency who is the most appropriate given the organization affected by the attack is imperative especially for attacks that may cause harm.

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

a. It may reduce any initial confusion of requesting enforcement agencies

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

a. If there is confusion of who to contact when, we could have the potential of an organization not receiving the law enforcement assistance and dire secondary consequences could occur as a result of the attack.

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

a. In addition to completion of the deliverable, increasing awareness of local law enforcement agencies.

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

☐No ☒ Yes

a. Other states have been working on communicating with local law enforcement agencies, but they are usually very specific and specialized guidance. Not currently aware of a proactive campaign in other states as of now Other states have been working on communicating with local law enforcement agencies, but they are usually very specific and specialized guidance. Not currently aware of a proactive campaign in other states as of now

**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?**

☐No ☒ Yes

a. There are several federal agencies that have provided similar guidance. There are several federal agencies that have provided similar guidance.

## Other Implementation Factors

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

a. Shifting priorities or disagreement of steps and resources being provided to local law enforcement agencies.

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

☒No ☐ Yes

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

a. It will require a regular review by ISP and the Cybersecurity Program Director

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

a. State and Local Government Committee

**27. Can this deliverable be used by other sectors?**

☐No ☒ Yes

## Communications

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

a. Local government organizations and law enforcement agencies

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

☐No ☒ Yes

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

a. Not at this point.

## *Evaluation Methodology*

**Objective 1:** Indiana State Police and Cybersecurity Program Director work to develop the Cyber Emergency Response Education for Local Law Enforcement by May 2022.

*Type:* ☒ Output ☐ Outcome

*Evaluative Method:*

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

☐ Peer Evaluation/Review<br>
☐ Testing/Quizzing<br>
☐ Benchmark Comparison<br>
☐ Qualitative Analysis<br>
☐ Quantifiable Measurement<br>
☐ Other

**Objective 2:** Indiana State Police and IECC partners distribute the Cyber Emergency Response Education to 80 percent of Local Law Enforcement by June 2022.

*Type:* ☐ Output ☒ Outcome

*Evaluative Method:*

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

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

# Deliverable: Emergency Manager Cybersecurity Toolkit 3.0

# Deliverable: Emergency Manager Cybersecurity Toolkit 3.0

## *General Information*

1. **What is the deliverable?**
    a. Update the state's Cyber Incident Planning and Preparedness Toolkit for Emergency Managers that is compliant with FEMA, USDHS, and NIST.

2. **What is the status of this deliverable?**
☐ Completed ☒ In-progress 25% ☐ In-progress 50% ☐ In-progress 75%☐ Not Started

3. **Which of the following IECC goals does this deliverable meet?**
☐ 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?**
☐ 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?**
☐ 2021 ☐ 2022 ☒ 2023 ☐ 2024 ☐ 2025+

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?**
    ☐ One-time deliverable
    ☒ Ongoing/sustained effort

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Review current resources and templates for incident response toolkit | Resiliency and Response Working Group | 25% | December 2021 | |
| Make edits to toolkit – version 3 | Cybersecurity Program Director | 0% | February 2022 | |
| Develop cyber workshops | IDHS | 0 | January - March 2022 | |
| Conduct cyber workshops | IDHS | 0 | March 2022 | |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☐No ☒ Yes

| Estimated Initial FTE | Estimated Continued FTE | Skillset/Role | Primary Source of Funding | Alternate Source of Funding | Notes |
|---|---|---|---|---|---|
| 1.0 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 |
|---|---|---|---|---|---|---|
| No Response | | | | | | |

## 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 are 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?**

☐No ☒ Yes

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

☐No ☒ Yes

a. 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. information technology and emergency management. 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 require a high knowledge in information technology and emergency management. 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 require a high knowledge in i

## 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?**

☐No ☒ Yes

**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?**

☐No ☒ Yes

a. All sectors would benefit

## 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)?**

☐No ☒ 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 update the Emergency Manager Cyber Response Toolkit 3.0 by March 2022.

*Type:* ☒ Output ☐ Outcome

*Evaluative Method:*

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

**Objective 2:** IDHS will launch a workshop using the Emergency Manager Cyber Response Toolkit 3.0 by April 2022.

*Type:* ☐ Output ☒ Outcome

*Evaluative Method:*

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

# Deliverable: Cyber Annex and Cyber Liaison

# Deliverable: Cyber Annex and Cyber Liaison

## *General Information*

1. **What is the deliverable?**
   a. Finalize IDHS Cyber Annex and train cyber liaisons

2. **What is the status of this deliverable?**
   ☐ Completed ☐ In-progress 25% ☒ In-progress 50% ☐ In-progress 75% ☐ Not Started

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

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

## Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. Update 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? 2018**

   ☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

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. State and Local Government 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), 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?**

    ☐ One-time deliverable
    ☒ Ongoing/sustained effort

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Review Annex from IDHS – Preliminary review with key stakeholders | Cybersecurity Program Director/IDHS/IOT/ISP/INNG | 50 | Qtr. 1 2022 | |
| Edit Annex and review with partners | IDHS | 0 | Qtr. 2 2022 | |
| Finalize and Distribute Annex | IDHS | 0 | Qtr. 3 2022 | |
| Train CLO | IDHS/IOT | 0 | Qtr. 4 2022 | |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☐No ☒ Yes

**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 |
|---|---|---|---|---|---|---|
| None | | | | | | |

## 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 are 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 the review of the 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?**

☐No ☒ Yes

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

☐No ☒ Yes

a. The National Governor's Association and FEMA identified several other states who do not have a cyber annex.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?**

☐No ☒ Yes

**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. None at this time.

**27. Can this deliverable be used by other sectors?**

☐No ☒ Yes

a. All critical infrastructure sectors 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)?**

☒No ☐ Yes

**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 edit and distribute the IDHS Cyber Annex to appropriate parties by Qtr. 3 of 2022.

*Type:* ☒ Output ☐ Outcome

*Evaluative Method:*

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

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

**Objective 2:** IDHS and IECC partners will exercise the IDHS Cyber Annex with the cyber liaisons by December 2023.

*Type:* ☐ Output ☒ Outcome

*Evaluative Method:*

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

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

# Deliverable: INNG Cyber State Capabilities

# Deliverable: INNG Cyber State Capabilities

## *General Information*

1. **What is the deliverable?**
   INNG Cyber State Capabilities

2. **What is the status of this deliverable?**
   ☐ Completed ☒ In-progress 25% ☐ In-progress 50% ☐ In-progress 75% ☐ Not Started

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

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

## Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   The Indiana National Guard is prepared to provide cyber response capabilities to a statewide cyber emergency when directed by a Federal disaster declaration or ordered to State Active Duty by the Governor.

6. **What metric or measurement will be used to define success?**
   Establishment of escalation and notification criteria and processes between the IDHS and the Indiana National Guard to include Memorandums of Agreements.

7. **What year will the deliverable be completed?**
☐ 2021 ☐ 2022 ☐ 2023 ☒ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
IDHS and the Indiana National Guard.

9. **Which state or federal resources or programs overlap with this deliverable?**
CISA, FBI, DoJ, and the ISP

## Additional Questions

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

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
IDHS and the Indiana National Guard.

12. **Who should be main lead of this deliverable?**
IDHS Directory and the Adjutant General of Indiana.

13. **What are the expected challenges to completing this deliverable?**
Current U.S. Federal law has restrictions for use of Title 32 forces and equipment to support state emergency response. Activation of the National Guard by the Governor to support cyber incident response activities requires legal review and guidance for activities NG soldiers would perform on state or local government networks.

## *Implementation Plan*

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

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| IDHS Cyber Annex to the CEMP | IDHS | 0% | 2022 | |
| INNG All-Hazards Cyber Response | INNG | 75% | 2024 | |
| Legal Review, NDA, MOA | Indiana Attorney General and INNG Judge Advocate General | 0% | 2024 | |

| | | | | |
|---|---|---|---|---|
| Passage of the National Guard Cybersecurity Act | U.S. Congress | | | |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☐No ☒ Yes

a. If Yes, please complete the following:

| Estimated Initial FTE | Estimated Continued FTE | Skillset/Role | | Primary Source of Funding | Alternate Source of Funding | Notes |
|---|---|---|---|---|---|---|
| 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.)**

The National Guard would have the regulatory and legal clarification to provide active support during a large-scale cyber emergency.

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

The INNG would be able to provide response forces to bolster the efforts of CISA, the FBI, or the IDHS when responding to cybersecurity related incidents. The costs would be dependent upon the size of the force requested and the duration of the event.

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

INNG response forces remain limited to an advisory role.

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

A co-developed MoA between IDHS and the INNG.

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

   ☐No ☒ Yes

   a. Texas.

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?**

   ☐No ☒ Yes

## Other Implementation Factors

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

   a. Failure to pass the National Guard Cybersecurity Act would continue ambiguity of response capabilities due to overlapping laws, DoDI guidance, and regulations.

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

   ☐No ☒ Yes

   a. Passage of the National Guard Cybersecurity Act would allow the INNG to response to Cyber disasters similar to natural disasters.

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

   a. No Response

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

   a. The National Guard is having internal discussions on how to develop this initiative.

27. **Can this deliverable be used by other sectors?**

   ☐ No ☒ Yes

## Communications

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

   a. No Response

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

   ☒ No ☐ Yes

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

   a. No Response

## *Evaluation Methodology*

**Objective 1:** The Indiana National Guard will inform state leadership of their cyber response capabilities to a statewide cyber emergency when directed by a federal disaster declaration or ordered to State Active Duty by the Governor by December 2024.

*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.

- Indiana Cyber Exercise – News Release and News Coverage
- Muscatatuck Urban Training Center – Homeland Defender Info Sheet
- Indiana Emergency Manager Cybersecurity Toolkit 2.0
- Indiana Cyber Emergency Resiliency Response State Guide
- Integrated Preparedness Information Handout

# Indiana Cyber Exercise
# News Release and News Coverage

# Indiana's Cyber Readiness Advancing Rapidly

Friday, October 1, 2021

If you think about it, protecting a school, hospital, or a city's water supply from a cyberattack is a lot like a football coach drawing up a game plan for playing against the #1 team in the country – every day.

There's game film, playbooks and you always have to account for how you're going to stop the other team's best player from scoring; all the while trying to figure out what else the coach might have up his sleeve. And there's no halftime show to try and adjust to stage a comeback.

That's the challenge facing the State of Indiana in its efforts to continue rapidly moving forward in its mission to further strengthen its cybersecurity resiliency and response.

The progress that's been achieved comes as the State of Indiana and the Indiana National Guard recently hosted two cyber exercises in a partnership with several federal agencies, health care providers, and technology companies, water utility service providers, state, and local government officials, as well as state and federal emergency and law enforcement agencies.

"Conducting these exercises highlights the strength of the cybersecurity structure that exists within the state and underscores the work that's been accomplished over the past three years by

Indiana Governor Holcomb's Executive Council on Cybersecurity with our partners in the military, academic, public and private sectors," said Indiana Department of Homeland Security Executive Director Stephen Cox. "Most importantly, it represents the progress with cyber that's been achieved on behalf of all Hoosiers when we approach cybersecurity as something that is not solved by one entity alone, but by everyone at all corners of the state."

Having a playbook is especially crucial, given the fact there are not only a seemingly endless number of situations in which a cyberattack or incident can occur, but there are all kinds of circumstances and variables that can interfere with a cyber team's strategy for protecting its systems.

**When Water Runs Out…**

A water utility being attacked is not only scary to every city in America, but the reality of it also happening is real.

The Cybersecurity and Infrastructure Security Agency (CISA) has partnered with the State of Indiana and the City of Fort Wayne to exercise how state, federal, mutual aid, and local government would work together in a long-term cyberattack that eliminates the supply of water from the city, with a special emphasis on the secondary effects for the city's hospitals.

As the Cybersecurity Program Director for the State of Indiana, there's no question cybersecurity impacts every aspect of our daily lives. As we've seen with recent cyber incidents – everything from pipelines to water utilities to schools and hospitals – a cyberattack can create substantial effects and damage to our community and our critical infrastructure, disrupting our daily lives and safety.

**When Natural Disasters Hit…**

Following the completion of the tabletop exercise, a second cyber exercise as part of a full-scale functional exercise hosted by the Indiana National Guard for first responders and several military branches as well as search and rescue teams at the Muscatatuck Urban Training Center.

The grounds of the 1,000-acre facility, located in Southern Indiana, is a real city that includes a built-in physical infrastructure, a well-integrated cyber-physical environment, an electromagnetic effects system and human elements. There are more than 190 brick-and-mortar structures with roughly 1.5 million square feet under roof, 1.8 miles of subterranean tunnels, a cave complex, more than nine miles of roads, managed airspace, a 185-acre reservoir, and a cyber live-fire range.

The focus of the Indiana National Guard exercise centered on measuring how federal, state, local and private sectors respond to a devastating earthquake.

"We really need to prepare now for these acts which we've already seen here in Indiana and across the world," said Ron Pelletier, founder and chief customer officer at Pondurance, a cyber security company. "When natural disasters hit all parts of the world, we are seeing more and more targeted cyberattacks in those affected areas. Investing now in preventative measures is the best way to avoid situations like that from becoming worse. It comes down to planning to avoid cyber breaches but being prepared to respond."

As emergency and military teams respond to the effects of the earthquake, the Indiana National Guard also tested the additional response of its incident command leadership while the cyber experts from IU Health, Citizens Energy Group, and Pondurance made the efforts more difficult by attacking the water supply in the aftermath.

**It's Not "If" But "When"...**

Pelletier added that Pondurance hopes disaster drills, such as these two, will raise awareness among policy makers to help fund security programs and protocols. "National, state, and community security is truly at risk here, and we need to take action now to preserve it. Waiting for the dam to burst before you repair it is a terrible maintenance strategy, and that's exactly the situation we have here across power grids, water supplies, healthcare, you name it."

Having the ability to draw on the resources and expertise required at a moment's notice to keep people safe in the event of a cyber incident or attack relies on making certain that the state and its partners have a line of communications that's always open to make sure the State of Indiana provides a response that's most effective, regardless of the circumstances.

Many of those who are participated in both state exercises also serve on the Indiana Executive Council on Cybersecurity (IECC). As defined in Executive Order 17-11 from Indiana Governor Eric Holcomb, the IECC is a first-of-its-kind collaboration, whose work as an organization within state government, is responsible for guiding the state's cybersecurity policy, It is comprised of 35 Council members and 250 advisory members, all of whom are subject matter experts represent a wide range of businesses, industries and professions, including education, finance, utilities and insurance, among many others.

The State of Indiana and its partners offer best practices, guides, toolkits, and resources to allow all organizations and critical infrastructures to mitigate, but also prepare for a cyberattack. For more information about the IECC or the State of Indiana's Cyber Strategy, visit www.in.gov/cyber.

For more information about CISA's cybersecurity services and resources, visit www.cisa.gov.

LOCAL NEWS

# Indiana holds full-scale cybersecurity disaster drill

Lessons learned in the day-long drill at Muscatatuck will be used to help hospitals and utilities all across the state.

Indiana tests preparedess with cybersecurity disaster drill

Author: **Jennie Runevitch**

Published: **4:24 PM EDT August 17, 2021**
Updated: **7:49 PM EDT August 17, 2021**

MUSCATATUCK, Ind. — Hackers are increasingly hitting governments, utilities, and hospitals — critical infrastructure across the country — during severe storms or natural disasters.

That's why the state of Indiana just held a full-scale disaster drill to test and better prepare Hoosier response.

When a natural disaster strikes, damage from weather isn't the only threat anymore. Experts say right while we're at our most vulnerable, cyberattacks are now targeting hospitals, electric grids, and water systems.

It's happened a lot during hurricanes and wildfires and leaders in Indiana say it'll likely happen here, too.

"It is a staggering threat when we talk to our counterparts in Louisiana, in Texas, in Florida. When there are hurricanes coming at them, all of a sudden, they see the bad actors trying to get in their systems increase by a thousand-fold," said Chetrice Mosley Romero, the state of Indiana's Cybersecurity Program Director. "Bad actors watch the news and watch the weather channel just as much as the good people do, right? So, they're saying, 'hey - they're going to be affected. They're going to be distracted so we should go after that.'"

Enter "Operation Homeland Defender".

The massive cybersecurity drill, held over the weekend at Muscatatuck Urban Training Center, included the Indiana National Guard, local first responders, Indiana Task Force One, Indiana-based Pondurance, IU Health and Citizens Energy.

They conducted a simulated emergency, then injected a cyberattack.

*Credit: DVIDS via Indiana National Guard*

First, an earthquake hit, then in the chaos of trying to protect people and property, here come the hackers.

"So, we have people who come in and actually attack the water system and shut it down and now you have firefighters and rescue first responders who no longer have water," Mosley-Romero explained. "What can really make a bad day worse? Water's typically the top one."

Crews involved in the drill didn't know this was a cyberattack at first.

The exercise teaches that, so first responders know in the future that hackers are a possibility during disasters.

The groups also experience, in real time, how to plan and respond.

"So we have a red team that attacks the system and then we have a blue team who responds to that attack, closes up the system and then also educates the water utility on what they could've done to prevent the attack altogether," Mosley-Romero said.

Protecting health care and critical infrastructure, just when people need it the most, is the goal of this exercise.

Lessons learned in the day-long drill at Muscatatuck will be used to help hospitals and utilities all across the state.

"It isn't just one entity that solves it all, it is a 'all hands are on deck' situation because all of us are touching things that are plugged in, so all of us are really part of the cyber problem," Mosley-Romero said. "But we're also part of the cyber solution."

The state of Indiana has developed cybersecurity toolkits, for not only cities and businesses but also regular citizens.

You can even test yourself, to see how well you're protected. Find the information, tips and quizzes here.

## Related Articles

**Attempted ransomware attack prompts Eskenazi Health to shut down systems and divert patients**

**New cybersecurity order issued for US pipeline operators**

**$10 million rewards bolster White House anti-ransomware bid**

ABOUT MEMBERSHIP EVENTS / PRODUCTS POLICY / ADVOCACY NEWS / RESOURCES

ABOUT MEMBERSHIP EVENTS / PRODUCTS POLICY / ADVOCACY

NEWS / RESOURCES SEARCH

Create
ccount | Login

Pay Your
Invoice

Search ...

PRESS RELEASES ›

STUDIES / REPORTS

MEDIA INQUIRIES / SPOKESPEOPLE

BIZVOICE MAGAZINE

MULTIMEDIA

BLOG

‹ Previous Next ›

# COLLABORATION KEY AS INDIANA PREPARES FOR MAJOR CYBERATTACKS

September 29th, 2021

By Adam Berry

The U.S. military is used to fighting battles on the land and sea and in the air.

But now, there’s a new battleground – in space. Cyberspace.

So when the Indiana National Guard prepares for natural and man-made disasters, you can bet they call in an ample supply of cybersecurity firepower. This summer, officials from the Indiana National Guard and state of Indiana conducted two drills to prepare for disasters and layered into the plan a new, higher level of cybersecurity.

That’s because an emerging – and troubling – trend is creating the need to change the emergency preparedness playbook.

Cyber criminals are copying the way traditional scammers

HEALTH CARE SAVINGS

EMPLOYMENT POSTERS

follow storms and get vulnerable people to pay cash for cleanup, only to abscond with the money and doing no real work.

Cyber criminals have begun to follow natural disasters too, but their targets are often water and power supply operations, hospitals and other critical operations – hitting them with cyber ransom attacks when they are most vulnerable.

Unlike the hackers of old, these bad guys aren't necessarily after a data heist. Hackers today want to highjack an online system and hold it hostage until a hefty – often six- or seven-figure – ransom is paid. Ransom attacks have increased 400% this year over last year, and a whopping 800% since the onset of the pandemic, according to the FBI.

And the price to get untangled from these attacks is escalating as fast. A ransomware attack on Baltimore in 2019, for example, cost the city $18.2 million.

The ransomware threat is so concerning, the Indiana National Guard has tapped Indianapolis-based cyber security firm Pondurance to help conduct disaster drills that layer on cyber threats.

"We're seeing more initiative by these bad actors to exploit these opportunities," says Ron Pelletier, founder and chief customer officer at Pondurance.

"They come in while people and entities are already under duress and distracted," adds Pelletier, an appointed member of the Indiana Executive Council on Cybersecurity (IECC). "It happened recently during the freezing conditions in Texas and created some real havoc. It's becoming more and more prevalent as bad actors become more enterprising. We have to take steps to be prepared."

The IECC was created in 2016 by then Governor Mike Pence to do just that. Governor Eric Holcomb moved to continue the IECC in 2018.

Many of the efforts to bolster Indiana's cybersecurity started in early 2015, says Chetrice Mosley-Romero, cybersecurity program director at the Indiana Office of Technology and Indiana Department of Homeland Security. "It dawned on state officials that in a real, true cybersecurity emergency we will need a collaborative approach across agencies and organizations."

Since the IECC's creation, Indiana's position in the world of cybersecurity has changed dramatically. It's essentially gone from one of the worst U.S. states in terms of cybersecurity preparedness to one of the best.

While pleased with this turn of events, Mosley-Romero remains humble. She knows that blowing the trumpet too loudly on the state's fortification could make it a target for hackers looking to prove their chops.

Mosley-Romero can keep her trumpet put away. The National Governors Association is taking care of that. The organization recently rated Indiana as one of the top five U.S. states in terms of cybersecurity preparedness. That's quite a change from where the state was just a few years ago.

That ranking, Mosley-Romero explains, is "due to our collaboration, and the fact that we rely on our partnerships for implementation. We were at the bottom before we had the IECC. The things we've done at a policy level and with some of our private sector partners is what's led to our success going from the bottom tier to the top."

The IECC not only brought on Pondurance, which is doing its part for free, it's also enlisted the likes of Citizens Energy Group and IU Health among others. The IECC is also reaching out to work with as many local municipalities around the state as possible. "We're trying to demystify cybersecurity," Mosley-Romero says. "We have to make this comprehendible to local communities. We have to connect this to something they care about. By doing that, we can get to baselines across counties."

This comprehensive approach means "we're not just hitting the breadth of cybersecurity; we're hitting the depth too. We have the most comprehensive approach of any other state, and we didn't have that before the formation of the IECC."

Part of that comprehensive approach is training drills.

Officials for the state and the Indiana National Guard hosted two cyber exercises last month in partnership with several federal agencies, health care providers, technology companies, water utility service providers, local government officials, and state and federal emergency and law enforcement agencies.

Pelletier hopes disaster drills, such as these two will raise awareness among policy makers to help fund security programs and protocols.

"National, state and community security is truly at risk here, and we need to take action now to preserve it," he states. "Waiting for the dam to burst before you repair it is a terrible maintenance strategy, and that's exactly the situation we have here across power grids, water supplies, healthcare, you name it."

The first drill was a "tabletop" or virtual exercise that simulated a cyberattack on water system during the July 4 weekend. Holidays are a common time for cybercriminals to hit.

Following the tabletop exercise, a full-scale functional exercise was hosted by the Indiana National Guard for first responders and several military branches as well as search and rescue teams at the Muscatatuck Urban Training Center in southern Indiana.

More than 500 soldiers, airmen and civilian emergency responders from across the state for three days exercised Indiana's response to a catastrophic earthquake and the ensuing chaos, including cyberattacks.

"When natural disasters hit all parts of the world, we are seeing more and more targeted cyberattacks in those affected areas," Pelletier says. "Investing now in preventative measures is the best way to avoid situations like that from becoming worse."

The drills, while perhaps the most visible of what the IECC is involved in, are just the tip of the iceberg. The organization has 121 objectives and 69 deliverables, and has completed 80% of those, Mosley-Romero says.

The state's overall cybersecurity approach is so unique, Mosley-Romero says she fields a constant stream of calls from other states wanting to hear what Indiana is doing for cybersecurity preparedness. "I've talked to dozens of states," she says.

Mosley-Romero stresses that the state isn't holding anything back.

"Our approach to working with other states is like our approach to working with cities and towns across Indiana," she says. "We're all connected, and you're only as strong as your weakest link. The more we collaborate, the better for everyone."

*Adam H. Berry is vice president of economic development and technology at the Indiana Chamber of Commerce. He joined the organization in 2019.*

**Share This Story, Choose Your Platform!**

# Muscatatuck Urban Training Center
# Homeland Defender Info Sheet

# Homeland Defender 2021

**Exercise Director:** LTC Robert Brake (INNG)

**Executive Council:** Chief Tom Neal (IN TF1) & LTC Robert Brake (INNG)

**Safety Director:** CSM Ty Benham (INNG)

**Operations Director:** Chief Jay Settergren (IN-TF1)

**Operational Support:** CPT Pemberton (INNG)

**MSEL Directors:** DC Steve Coover (MFD & IN-TF1) & LTC Robert Brake (INNG)

INDIANA NATIONAL GUARD

# HOMELAND DEFENDER 2021

POC: LTC Rob Brake

## Exercise Mission

INNG host a Full Scale Exercise from 13-15AUG21 vic MUTC involving local and state resources in order to (IOT) reinforce existing relationships, create new ones and share best practices within the 1st responder community.

## Exercise Purpose

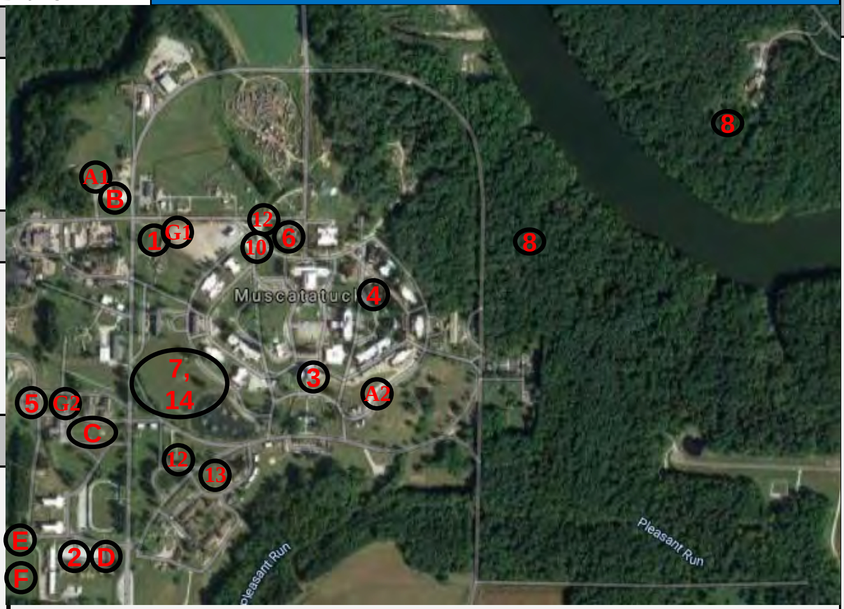
Conduct a joint training event that includes local, state & military partners, focused at the Team level, in order to increase unit/team proficiencies and integration with other 1st responders within the State of Indiana Response Forces.

## Exercise Intent

**Exercise Commander Intent:** Provide a realistic training opportunity for units to collectively train together IOT increase readiness and share tactics, techniques, and procedures via a scalable and nested exercise over a 2 day, weekend exercise. Once completed units, can receive a facilitated AAR based on individual unit training requirements.

**Key Tasks:** Alert & Mobilize, Deploy, Site Occupation, Joint /combined Operations & Redeploy all IAW NIMS.

**End State:** Create a realistic collective exercise from H-hour – OP3, that supports Local and State Inter Agency Integration followed by after action reviews IOT ensure State Partners meet individual and team training objectives, increase readiness and share techniques between Agencies.



## Concept of Operation

A series of earthquakes occur that quickly exceeds local resources requiring assistance from Regional and State Agencies in order to meet lifesaving operational requirements.

As a result multiple agencies and units receive an Alert Orders to Deploy to staging locations. O/O units will move forward IOT conduct Site Occupation & link up with the Incident Management Team (IMT) IOT receive missions for Full Scale Operations. Once units are Mission Complete, they will begin recovery operations and redeploy to home station.

## Operational Lanes:

Lane #1: Initial Command Post & Rail Yard
Lane #2: Unified Command / IMT CMD Post
Lane #3: Hospital Chemical & Radiation
Lane #4: Round Robin Skills Training
Lane #5: Cafeteria Collapse
Lane #6: School Collapse
Lane #7: TF1 Air Load Operations
Lane #8: Lost Personnel WAS
Lane #9: CYBER Ransom
Lane #10: Chaplain Teams
Lane #11: NGRF Alert and Staging Operations
Lane #12: Area Security Operations
Lane #13: Crowd Control Activities
Lane #14: Lifeline Operations

Site A: Staging (Sites 1 & 2)
Site B: MFD & CST CMD Post
Site C: CERFP & TF1 CMD Post
Site D: NGRF CMD Post
Site E: White Cell Team
Site F: Ravenswood Support site
Site G: DECON Sites ( 1& 2)

## Participants/Enablers: 369 (82) BOG -501

| | |
|---|---|
| CST – 20 (2) | MFD – 16 (6) |
| TF1 IN – 6 (15) | 81st TC – (10) |
| CERFP – 208 (5) | IOT – 15 (3) |
| CAP – 2 | JCSD – 40 |
| NGRF – 40 (5) | UPAD – 6 (2) |
| 38th CAB – (4) | ASOS – 4 |
| Ravenswood – (24) | JFHQ-IN – (4 ) |
| IDHS Dist 8 IMT – 12 | |
| 127th CB – (2) | |
| | Additional: |
| ( ) = non-participant / support role | Role Players – (50) |

IPR #1
10SEP20

**CDC**
06-08OCT20
CAIN/MUTC

IPR #2
1NOV20

IPR #3
4DEC20

**IPC**
2-3MAR21
MS Teams

**MPC**
16-17MAR21
MUTC

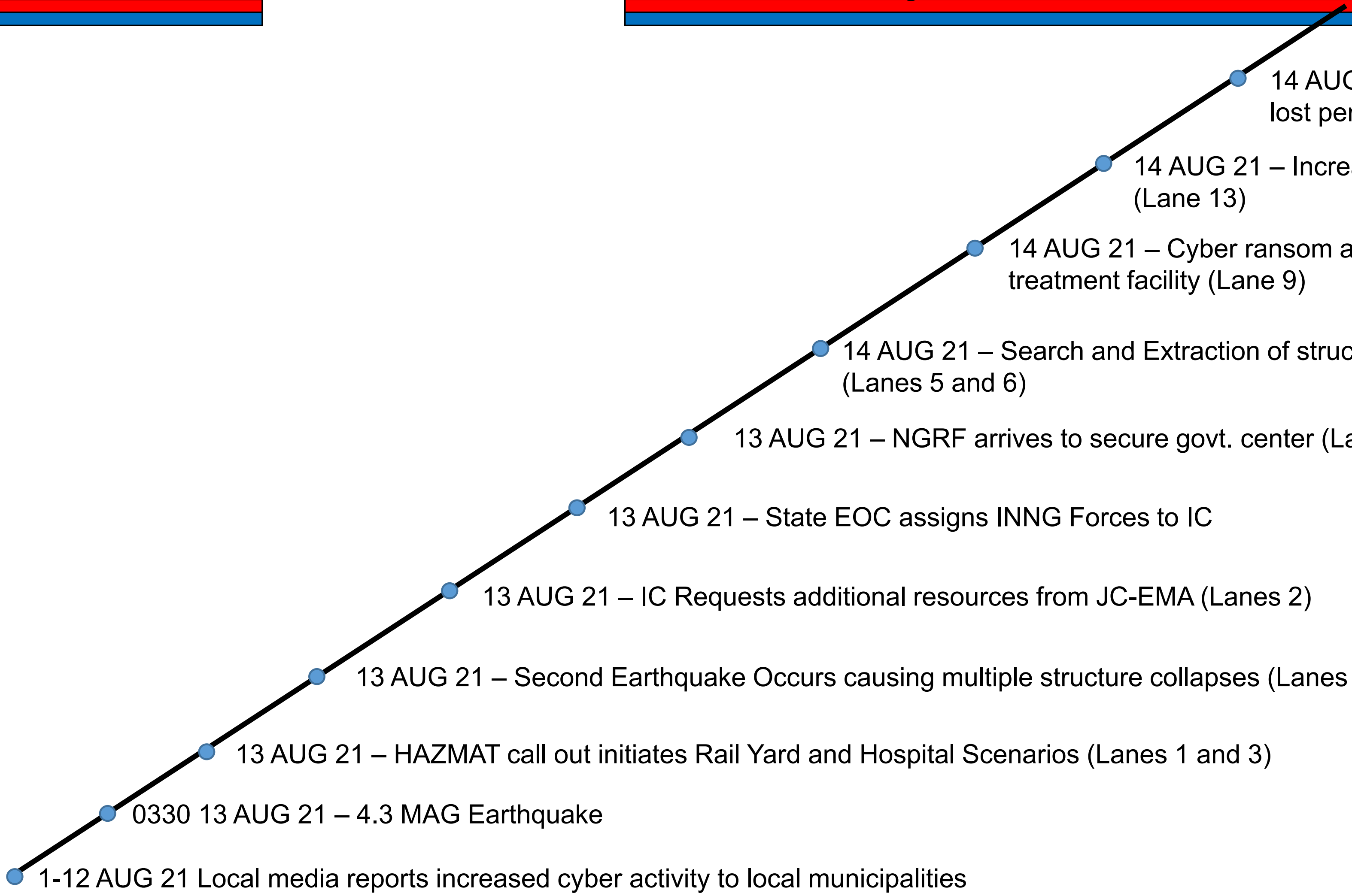
**FPC**
11-12MAY21
MUTC

IPR #4
21JUN21

IPR #5
19JUL21

**Execution**
13-15AUG21
MUTC

# Homeland Defender Key Events Timeline



14 AUG 21 – Wide area search for lost personnel (Lane 8)

14 AUG 21 – Increase civil unrest at govt. center (Lane 13)

14 AUG 21 – Cyber ransom attack at water treatment facility (Lane 9)

14 AUG 21 – Search and Extraction of structure collapses (Lanes 5 and 6)

13 AUG 21 – NGRF arrives to secure govt. center (Lane 12)

13 AUG 21 – State EOC assigns INNG Forces to IC

13 AUG 21 – IC Requests additional resources from JC-EMA (Lanes 2)

13 AUG 21 – Second Earthquake Occurs causing multiple structure collapses (Lanes 5 and 6)

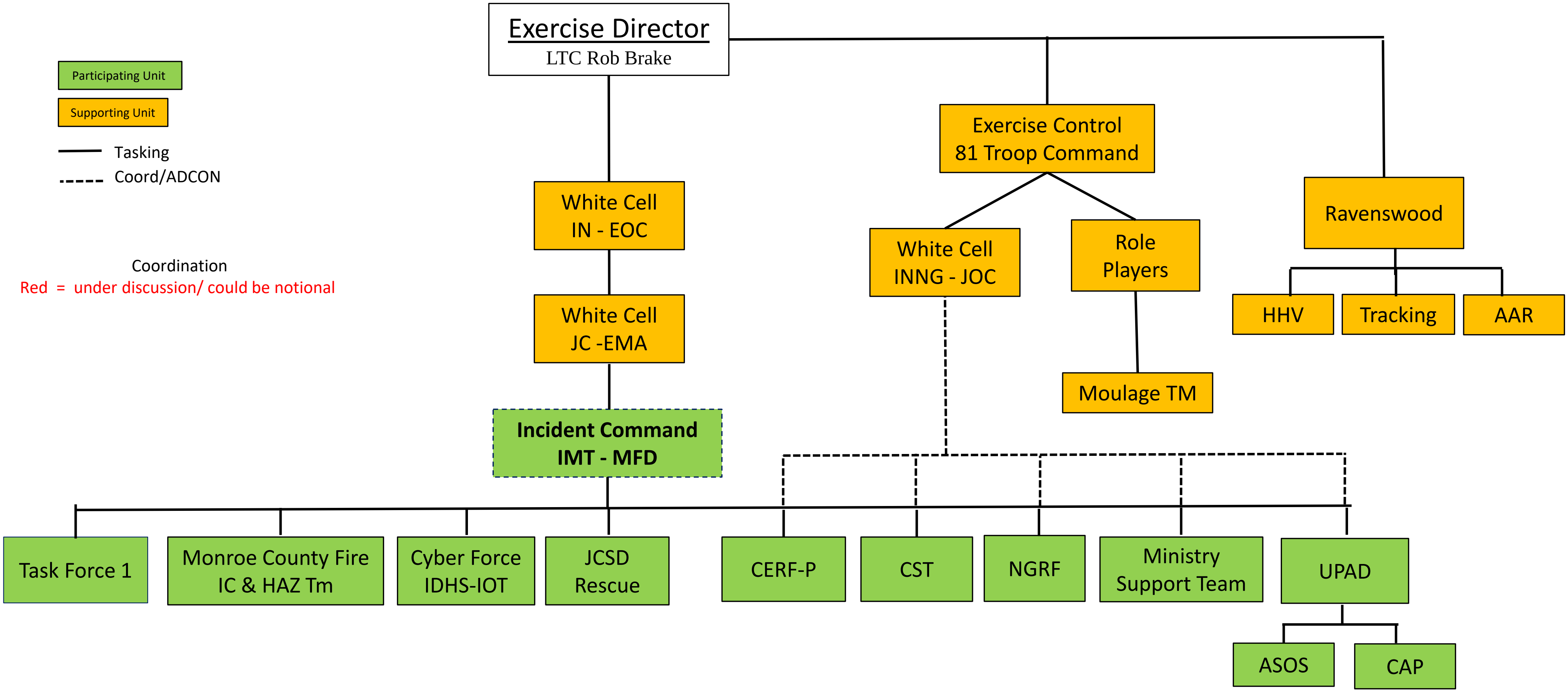
13 AUG 21 – HAZMAT call out initiates Rail Yard and Hospital Scenarios (Lanes 1 and 3)

0330 13 AUG 21 – 4.3 MAG Earthquake

1-12 AUG 21 Local media reports increased cyber activity to local municipalities

As of 1227 12AUG2021

# Task ORG



🟩 Participating Unit

🟨 Supporting Unit

Tasking

Coord/ADCON

Coordination

Red = under discussion/ could be notional

Exercise Director
LTC Rob Brake

White Cell
IN - EOC

White Cell
JC -EMA

Incident Command
IMT - MFD

Exercise Control
81 Troop Command

White Cell
INNG - JOC

Role
Players

Moulage TM

Ravenswood

HHV

Tracking

AAR

Task Force 1

Monroe County Fire
IC & HAZ Tm

Cyber Force
IDHS-IOT

JCSD
Rescue

CERF-P

CST

NGRF

Ministry
Support Team

UPAD

ASOS

CAP

# Indiana Emergency Manager Cybersecurity Toolkit 2.0

# INDIANA EMERGENCY MANAGER CYBERSECURITY TOOLKIT

SEAL OF THE STATE OF INDIANA

1816

October 2019

*Developed by the Indiana Executive Council on Cybersecurity*

# TABLE OF CONTENTS

Instructions: Please click on the section of the toolkit you would like to skip to in this digital packet.

- Welcome Letter
- How To Use This Toolkit
- Emergency Manager Cyber Situational Awareness Survey
- Cybersecurity Incident Response Plan Template
- Cybersecurity Training and Exercise Guide
- Cybersecurity Attacks in Indiana: Quick Response Guide
- Cyber Emergency Resiliency and Response State Guide
- Additional Emergency Manager Cybersecurity Resources
- Bibliography

For more information, visit www.in.gov/cyber.

October 23, 2020

Dear Emergency Managers,

To help our communities continue to be strong and protected while staying connected, Governor Eric J. Holcomb's Executive Council on Cybersecurity has developed this *Indiana Emergency Manager Cybersecurity Toolkit* for local government emergency managers to use as they navigate through the complexities of cybersecurity at a local level.

With October being National Cybersecurity Awareness Month, it is the perfect time for Indiana to launch the first-of-its-kind toolkit you can start using today. As emergency managers we need to convey the importance of this pervasive and serious threat to the many partners in our communities we already coordinate with every day on other threats and hazards. This ever-growing threat is becoming more and more of a concern as many of our own local governments in Indiana have been attacked in the last several months. The best way to approach this new threat environment is like all others: we assess, we plan, we train, and we exercise to best be prepared when a cyberattack happens.

I am looking forward to your input on this cybersecurity toolkit that is meant to be a resource for emergency managers throughout the state. Your feedback will help as we seek to improve it over the coming months.

I hope this also provides the necessary information and tools to get you started so your community is better equipped to prepare and plan for a threat that is increasing by the day with your leadership, peers, and community partners.

Sincerely,

Stephen Cox

Indiana Department of Homeland Security Executive Director &

Indiana Executive Council on Cybersecurity Chair

# HOW TO USE THIS TOOLKIT

# HOW TO USE THIS TOOLKIT

The world of cybersecurity is highly complex and cluttered with information, misinformation, and disinformation. As a consequence, it is important to approach it strategically and create simplicity. This *Indiana Emergency Manager Cybersecurity Toolkit*, developed by the Indiana Executive Council on Cybersecurity, outlines a way to begin conversations with your local partners as simply and directly as the complexity of the effort allows.

This toolkit is primarily for emergency managers who serve their local communities and is organized into four main sections: a survey to assist emergency managers in planning with partners they work with to develop emergency and continuity of operations plans; a cybersecurity incident response plan template; a training and exercise guide; and several additional resources to assist in navigating this new and pervasive threat.

The toolkit can be used holistically or piece-by-piece, depending on how deep you want to go with your planning what you would do if your organizations experience a cyber attack.

This toolkit and additional information for emergency managers can also be found at www.in.gov/cybersecurity/3818.htm.

# EMERGENCY MANAGER CYBER SITUATIONAL AWARENESS SURVEY

# EMERGENCY MANAGER CYBER SITUATIONAL AWARENESS SURVEY

## INSTRUCTIONS

Below are instructions for the Emergency Manager Cyber Situational Awareness Survey. This survey was made to assist local government emergency managers who want to better assess the areas within their purview while developing and exercising their cyber emergency incident response and continuity of operations plans. This Emergency Manager Cyber Situational Awareness Survey was developed by the Indiana Executive Council on Cybersecurity, National Governors Association Cybersecurity Academy participants, as well as Indiana State University. This survey is meant to begin conversations between an emergency manager and his/her local government partners as well as provide a collective overview of the emergency manager's area through a risk profile using the information provided.

Using this survey and working with the Cybersecurity Program Director from the Indiana Department of Homeland Security and Indiana Office of Technology, an emergency manager will be provided with a comprehensive risk profile provided by the State of Indiana in partnership with Indiana State University so an emergency manager is better informed as to what he or she should be focusing on when planning for a cyber attack. All information provided to the state will be kept confidential.

Emergency Manager Cyber Situational Awareness Survey Instructions:

1. The Emergency Manager, who is the main point of contact for the state, retrieves the Emergency Manager Cyber Situational Awareness Survey PDF file online at https://www.in.gov/cybersecurity/3818.htm.
2. The Emergency Manager completes the "Emergency Management Overview" (EMO) page to document the critical infrastructure (CI) and key resource systems within their oversight.
3. Using the critical infrastructure and key resource systems identified in the EMO as a point of reference, the Emergency Manager communicates with a point of contact who is responsible for each individual CI and key resource system(s) identified, and requests they complete the survey for their area.
4. Those responsible for the CI and key resource systems complete his or her copy of the Cyber Situational Awareness Survey (CSAS). The survey can be done on the fillable PDF or completed by hand.
5. Those responsible for the CI and key resource systems send their completed survey back to the Emergency Manager.

6. Once the EMA collects all the completed surveys, he or she will send their overview survey sheet and all the surveys completed (saved or scanned) to the State of Indiana Cybersecurity Program Director Chetrice Mosley at MosleyCLM@iot.in.gov.
7. The State of Indiana, working with a secure lab at Indiana State University, will then complete an analysis and develop a custom confidential Risk Profile for each Emergency Manager.
8. The Risk Profile will then be provided to each Emergency Manager allowing them to: better inform their planning, heighten training, and create appropriate exercises for their areas of responsibility. Emergency Managers will then communicate to their leadership the current status of their cybersecurity posture and priorities.

If you have any questions, please feel free to email the State of Indiana Cybersecurity Program Director Chetrice Mosley at MosleyCLM@iot.in.gov or call her at 317-607-3178.

# Emergency Manager Cyber Situational Awareness Survey

| | |
|---|---|
| Name of County: | Name of City: |
| Address: | |
| Phone: | IDHS District: |
| Email Address: | Population of area supervised: |

**What critical infrastructure and key resource systems do you oversee as an emergency manager in your organization? Select all that apply.**

| |
|---|
| **Communications** |
| County or Municipality Owned Telecommunication Services (Cable, Broadband, etc.) |
| **Dams** |
| **Educational Facilities (K-12 School Systems)** |

| | |
|---|---|
| **Emergency Services** | |
| | Law Enforcement |
| | 9-1-1 Operations |
| | Emergency Management |
| | Fire & Rescue |
| | Emergency Medical Services |
| **Energy** | |
| | County or Municipality – Ran Electricity |
| | County or Municipality – Owned Oil |
| | County or Municipality – Owned Natural Gas |
| **Elections** | |

| | |
|---|---|
| **Government Facilities** | |
| | Offices and Office Building Complexes<br>Housing for Government Employees<br>Correctional Facilities<br>Embassies, Consulates, and Border Facilities<br>Courthouses<br>Libraries and Archives |
| **Healthcare & Public Health** | |
| | Public Health Departments<br>County or Municipality Owned Hospitals or Health Facility |

| |
|---|
| **Political Offices** |
| Auditor<br>Assessor<br>County Commissioner<br>Sheriff |
| **Transportation Systems** |
| Aviation<br>Highway & Motor Carrier<br>Maritime Transportation Systems<br>Mass Transit & Passenger Rail<br>Pipeline Systems<br>Freight Rail<br>Postal & Shipping |

| |
|---|
| **Wastewater – Publicly owned wastewater treatment systems** |
| **Water – Public drinking water systems** |
| **Other:______________________________** |

# CYBER SITUATIONAL AWARENESS SURVEY (CSAS)

| | |
|---|---|
| **Organization Name:** | **Name of Person Completing Survey:** |
| **Address:** | |
| **Phone:** | **Email:** |

## *Organization Information*

**1.** How many employees are there in your organization? ________

**2.** How many employees have information/technology related duties? ________

**3.** How many employees have cybersecurity related duties? ________

**4.** How many times in the last 5 years has your organization been the victim of a cyberattack? ________

**Yes** **No**

**5.** Do you have cybersecurity policies?

**6.** Do you outsource your cybersecurity needs?

**7.** Do you include security requirements in your agreements with vendors?

**8.** Has your organization completed a cyber assessment in the last 2 years?

# CYBER SITUATIONAL AWARENESS SURVEY (CSAS)

## *Voice Communications*

**9**. What voice communication systems does your organization use? Select all that apply.

Voice Over Internet Protocol (VOIP) Telephones or Services:

Uses voice over Internet Protocol (IP) technologies for placing and transmitting telephone calls over an IP network, such as the Internet, instead of the traditional public switched telephone network (PSTN) with an analog phone.

Analog Telephones (POTS):

Voice-grade telephone service employing analog signal transmission over copper loops, aka plain old telephone service or plain ordinary telephone service.

Digital Handheld Radios:

Person-to-person two-way radio voice communications systems which use portable, mobile, base station, and dispatch console radios. These systems are used by police, fire, ambulance, and emergency services, and by commercial firms such as taxis and delivery services.

Digital Console Radios:

Same as above description but in non-mobile form.

Satellite Telephones:

Type of mobile phone that connects to other phones or the telephone network by radio through orbiting satellites instead of terrestrial cell sites, as cellphones do.

Radio over Internet Protocol (RoIP):

Like Voice over Internet Protocol (VoIP), but augments two-way radio communications rather than telephone calls.

# CYBER SITUATIONAL AWARENESS SURVEY (CSAS)

## *Voice Communications (cont.)*

☐ Employer-Issued Cellular Smartphone (e.g. iPhone, Android):

Smartphone owned, issued, supported, and paid for by the employer, and the employee typically agrees to specific usage guidelines.

☐ Personal Cellular Smartphones (e.g. iPhone, Android):

Smartphone that is owned, supported, and paid for by an individual.

☐ Other: ___________________________________

## *Data Communications*

**10**. What data communication systems does your organization use? Select all that apply.

☐ Government Email (.gov):

The .gov top-level domain (TLD) facilitates collaboration among government-to-government, government-to-business, and government-to-citizen entities.

☐ Commercial Email (.com/.net) (e.g. Gmail, Yahoo, iCloud):

Free web-based email service (webmail) providers. Typically accessed via web browser or smartphone app.

☐ Wireless Local Area Network:

A wireless computer network that links two or more devices using wireless communication to form a local area network (LAN) within a limited area (WIFI).

# CYBER SITUATIONAL AWARENESS SURVEY (CSAS)

## *Data Communications (Cont.)*

Organization Provided Internet Service:

Your company, organization, etc… is provided access to the Internet via a 3rd party Internet Service provider (ISP).

Mobile WiFi Hotspots:

An ad hoc wireless access point that is created by a dedicated hardware device or a smartphone feature that shares the phone's cellular data.

Publicly Accessible Website:

A collection of related network web resources, such as web pages, multimedia content, which are typically identified with a common domain name, and published on at least one web server. Notable examples are wikipedia.org, google.com, and amazon.com.

Organization Email (.com/.org):

A business email address / service given to an employee by the company where they work.

Wired Local Area Network:

A computer network that interconnects computers within a limited area such as a residence, school, laboratory, university campus or office building.

Commercial Internet Service (Xfinity, Comcast, Spectrum):

An organization that provides services for accessing, using, or participating in the Internet.

Government Provided Internet Service:

Your company, organization, etc… is provided access to the Internet via a Government Internet Service provider, ex: Local, County, City, State of Indiana, or Federal.

Internal Network / Website (Intranet):

A computer network for sharing corporate information, collaboration tools, operational systems, and other computing services only within an organization, and to the exclusion of access by outsiders to the organization.

# CYBER SITUATIONAL AWARENESS SURVEY (CSAS)

## *Data Communications (Cont.)*

Restricted Website (e.g. anything that uses HTTPS):

A controlled private network that allows access to partners, vendors and suppliers or an authorized set of customers – normally to a subset of the information accessible from an organization's intranet.

Other: ___________________________________

## *Data Types*

**11**. What data types does your organization use? Select all that apply.

Sensitive / FOUO Information:

Unclassified information of a sensitive nature, not otherwise categorized by statute or regulation, the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national interest.

Law Enforcement Sensitive Information:

Denotes information that was compiled for law enforcement purposes and should be afforded security in order to protect certain legitimate Government interests

Protected Critical Infrastructure Information:

Critical infrastructure information means information not customarily in the public domain and related to the security of critical infrastructure or protected systems.

# CYBER SITUATIONAL AWARENESS SURVEY (CSAS)

## *Data Types (cont.)*

Vital Public Records:

Records of life events kept under governmental authority, including birth certificates, marriage licenses (or marriage certificates), and death certificates. In some jurisdictions, vital records may also include records of civil unions or domestic partnerships.

Medical Records:

Protected health information includes all individually identifiable health information, including demographic data, medical histories, test results, insurance information, and other information used to identify a patient or provide healthcare services or healthcare coverage.

Court Records:

The official written documentation of what happened during a trial or a hearing.

Purchasing / Contract Records:

Typical contract types include fixed-price, cost-reimbursement, incentive contracts, time-and-materials, labor-hour contracts, indefinite-delivery contracts, Bilateral, Unilateral, Express, Contract Under Seal, etc.

Credit Card Information:

Includes: Primary Account Number (PAN), Cardholder Name, Expiration Date, Service Code, Full track data (magnetic-stripe data or equivalent on a chip), CAV2/CVC2/CVV2/CID, PINs/PIN blocks.

Bank Account Information:

Includes Social Security number, Online login or password, One Time Password (OTP), Debit or credit card number, ATM card number or PIN, Routing number, Account number, Personal check, Paystub, Driver's license information, Children's personal information.

Personally Identifiable Information (e.g. social security Numbers, bank account numbers, email addresses):

Data that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.

Other: ___________________________________

# CYBER SITUATIONAL AWARENESS SURVEY (CSAS)

## *Data Storage & Equipment*

**12**. Where is your data stored and what equipment is used in organization? Select all that apply.

Organization-Managed Data Center - In-Building:

A dedicated space within a building, or a group of buildings used to house computer systems and associated components, such as telecommunications and storage systems.

Organization Data Center – Offsite:

A building, dedicated space within a building, or a group of buildings[4] offsite, used to house computer systems and associated components, such as telecommunications and storage systems

Vendor Managed Data Center – Cloud Based:

A remote version of a data center – located somewhere away from your company's physical premises – that lets you access your data through the internet.

Network Infrastructure (e.g. routers, switches, hubs):

The hardware and software resources of an entire network that enable network connectivity, communication, operations and management of an enterprise network. It provides the communication path and services between users, processes, applications, services and external networks/the internet.

Desktop Computers:

A personal computer designed for regular use at a single location on or near a desk or table due to its size and power requirements.

Tablets (iPad, Surface):

A mobile device, typically with a mobile operating system and touchscreen display processing circuitry, and a rechargeable battery in a single, thin and flat package

Secured Employee Drives:

A technology that encrypts the data stored on a hard drive using sophisticated mathematical functions

Desktop Printers / Scanners:

Personal printers are primarily designed to support individual users, and may be connected to only a single computer.

# CYBER SITUATIONAL AWARENESS SURVEY (CSAS)

## *Data Storage & Equipment* (cont.)

Networked Printers/Scanners:

Networked or shared printers and/or scanners.

Cellular Telephones:

A portable telephone that can make and receive calls over a radio frequency link while the user is moving within a telephone service area.

Local Servers – In-Office:

A computer program or a device that provides functionality for other programs or devices.

External Hard Drives:

An external hard drive is a portable storage device that can be attached to a computer through a USB or FireWire connection, or wirelessly.

CD-ROM:

A pre-pressed optical compact disc with the capacity to hold approximately 700MB of data.

Networked Shared Drives:

A computer attached to a network that provides a location for shared disk access, i.e. shared storage of computer files (such as text, image, sound, video) that can be accessed by the workstations that are able to reach the computer that shares the access through a computer network.

Thumb Drives:

A USB flash drive -- also known as a USB stick.

Other: ___________________________________

# CYBER SITUATIONAL AWARENESS SURVEY (CSAS)

**13**. On a scale of 1 to 5, with 1 being least confident and 5 being most confident, how confident are you in your accounting for your organizations’ voice communications, data communications, data types, and data storage and equipment?

| | | | | |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |

## *Operations Impact*

**14**. On a scale of 1 to 5, with 1 being no impact on your day-to-day operations and 5 being the most impact on your day-to-day operations (e.g. you must close), what level would your organization’s operations be affected If taken down by a cyberattack?

| | | | | | |
|---|---|---|---|---|---|
| Operation Systems | ☐1 | ☐2 | ☐3 | ☐4 | ☐5 |
| Voice Communication Systems | ☐1 | ☐2 | ☐3 | ☐4 | ☐5 |
| Email System | ☐1 | ☐2 | ☐3 | ☐4 | ☐5 |
| Databases of Information | ☐1 | ☐2 | ☐3 | ☐4 | ☐5 |

## CYBER SITUATIONAL AWARENESS SURVEY (CSAS)

| *Public Safety and Health Impact* | Yes | No |
|---|---|---|
| **15.** If your operation systems are down/compromised will the health and/or safety of the public be at risk? | | |
| **16.** If your information systems are down/compromised will the health and/or safety of the public be at risk? | | |
| **17.** If your communication systems are down/compromised will the health and/or safety of the public be at risk? | | |
| **18.** If your email system is down/compromised will the health and/or safety of the public be at risk? | | |

### Preparedness and Response

**19.** Does your organization have multi-factor authentication?

**20.** Does your organization install computer updates and/or patches regularly?

**21.** Do you install your updates and/or patches automatically?

**22.** Does your organization have a cyber emergency response plan in place to address a cyberattack on your organization?

# CYBER SITUATIONAL AWARENESS SURVEY (CSAS)

| Preparedness and Response (cont) | Yes | No |
|---|---|---|
| **23.** Does your organization provide your employees cybersecurity awareness and/or training? | | |
| **24.** Does your organization have a continuity of operations plan? | | |
| a) If yes, does your continuity of operations plan account for a cyber attack? | | |
| **25.** Are your organization's 'smart' devices (such as security cameras, thermostats, HVACs, alarm systems, etc.) periodically monitored and scanned for security vulnerabilities and malicious software? | | |

# CYBER SITUATIONAL AWARENESS SURVEY (CSAS)

## Recovery

**26**. In the event of a critical information system disruption or loss, what backup or redundant systems are in place for your organization?

**System Types**

| | | | | | | |
|---|---|---|---|---|---|---|
| **Operation Systems** | Multiple automatic backup systems are in place | An automatic or manual backup system is in place | A manual backup system is in place | Improvised system backups can be employed | No backup system is in place | I do not know |
| **Email Systems** | Multiple automatic backup systems are in place | An automatic or manual backup system is in place | A manual backup system is in place | Improvised system backups can be employed | No backup system is in place | I do not know |
| **Information from Databases** | Multiple automatic backup systems are in place | An automatic or manual backup system is in place | A manual backup system is in place | Improvised system backups can be employed | No backup system is in place | I do not know |

**27**. On a scale of 1 to 5, with 1 being least confident and 5 being most confident, how confident are you in your preparation, response, and recovery abilities in the event of a cyberattack?

| | | | | |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |

# CYBERSECURITY INCIDENT RESPONSE PLAN TEMPLATE

[NAME OR ORGANIZATION OR ADD LOGO]

# [DOCUMENT TITLE]

[DOCUMENT SUBTITLE]

ORGANIZATION, DEPARTMENT OR AUTHOR NAME
DATE

CYBERSECURITY INCIDENT RESPONSE PLAN TEMPLATE

DRAFT FOR REVIEW

**Table of Contents**

I. INTRODUCTION ........ 28

A. PURPOSE ........ 28

B. SCOPE ........ 28

C. SITUATION OVERVIEW ........ 28

D. PLANNING ASSUMPTIONS ........ 29

II. CONCEPT OF OPERATIONS ........ 29

A. DETECT ........ 29

B. RESPOND ........ 29

C. RECOVER ........ 33

III. ASSIGNMENT OF RESPONSIBILITIES ........ 34

IV. DIRECTION, CONTROL, AND COORDINATION ........ 34

V. INFORMATION COLLECTION, ANALYSIS, AND DISSEMINATION ........ 34

VI. COMMUNICATIONS ........ 34

VII. ADMINISTRATION, FINANCE, AND LOGISTICS ........ 34

VIII. PLAN DEVELOPMENT AND MAINTENANCE ........ 35

IX. POLICIES, AUTHORITIES, AND REFERENCES ........ 35

# I. INTRODUCTION

## A. PURPOSE

General statement of what the response plan is meant to accomplish. The statement should be supported by a brief synopsis of the plan’s contents.

## B. SCOPE

States specifically the facilities, groups, departments, units, or personnel to which the plan applies.

## C. SITUATION OVERVIEW

1. Describes, in very general terms, the current planning environment and the types of cybersecurity threats the planning organization must be prepared to manage.

2. Types of cybersecurity threats

a) Adverse Impact to Organization. These events have significant impact on the normal operations but do not fall into any of the following categories.

b) Alteration/Compromise of Information. These events involve the unauthorized altering of information or incidents that involve the compromise of information.

c) Denial of Service Attacks. These events are attacks that affect the availability of critical resources such as email servers, web servers, routers, gateways, or communication infrastructure.

d) Loss or Theft. These events involve the potential compromise of sensitive material. This includes the compromise of user accounts and passwords that could allow unauthorized persons to access IT resources.

e) Probes and Scans. These events include probing or scanning networks for critical services or security weaknesses. It also includes nuisance scans.

f) Unauthorized Access and Unsuccessful Attempts. These events include all successful unauthorized accesses and suspicious unsuccessful attempts.

g) Virus/Worms/Malicious Code. These events are performed by hackers in an attempt to gain privileges and/or information, to capture passwords, and to modify audit logs to hide unauthorized activity. The attempts include the use of mobile code such as viruses, Trojan horses, worms, and scripts. This category includes any virus or code that is intended to disrupt or annoy users.

3. Relative probability and potential impact of threats.

4. Vulnerability of critical systems.

5. Dependency of external organizations, vendors, or government agencies.

6. Current asset identification, hazard prevention, protection, and mitigation measures that are in place.

D. PLANNING ASSUMPTIONS

1. Describes what the planning team assumes to be facts for planning purposes in order to execute the plan.

2. During response operations, the assumptions indicate areas where adjustments to the plan have to be made as the facts of the incident become known.

II. CONCEPT OF OPERATIONS

A. DETECT

1. Procedures, processes, and systems in place for monitoring and detecting threats and anomalies.

2. Description of how continuous threat monitoring and detection is maintained.

3. Processes in place for evaluating effectiveness of monitoring, detection, and protective measures.

B. RESPOND

1. Threat Notification:

a) Upon detection of an event or threat, describes the process for preliminary alert messaging which communicates the existence of an emergency situation and provides basic incident information necessary to initiate an effective response.

b) Where will initial notifications originate?

c) Who will receive initial notifications? Establishes initial point of contact for initial incident alerts by position or job title

d) What information is provided in the initial notification?

2. Situation Assessment:

a) Process of gathering initial incident information, establishing situational awareness, determining severity of impacts, assessing needs, and determining whether to activate the incident response operations.

b) Incident triage and analysis process to determine nature, complexity, and severity of incident.

c) Incident response priorities based on existing or anticipated impacts to normal operations. Examples:

(1) Protect human life and safety. Protection of human life always takes precedence over all other considerations.

(2) If applicable, protect classified data as regulated by government statutes and regulations.

(3) Protect sensitive data, including proprietary, financial, law enforcement, scientific, and managerial data.

(4) Prevent system damage (e.g., loss or alteration of system files, damage to hard drives).

(5) Minimize disruption of computing resources. In many cases, it is better to shut down a system or disconnect from a network than to risk damage to data or systems.

d) Thresholds and trigger points for escalating and mobilizing response activity if an incident becomes more critical.

e) Identify and describe the actions that will be taken to monitor the movement and future effects that may result from the emergency.

f) Describe how the initial assessment is disseminated/shared in order to make protective action decisions and establish response priorities.

3. Response Plan Activation

a) Establishes which individuals by position/job title who have the authority to activate the response plan and initiate response operations.

b) Describes response process flow.

c) Details decision-making process for plan activation and initiation of coordinated response activity.

d) Procedures for assembling, and deploying personnel, supplies, and equipment to support the response to an incident.

4. Alert and Warning

a) Processes for reporting threats, events, and anomalies to elected and appointed officials, community leadership, management, personnel, law enforcement, and external stakeholders.

b) Establishes minimum reporting information requirements. (i.e. date, time, name and title of reporting person, location, systems/applications affected, etc.)

c) Identify and describe the actions that will be taken to coordinate, manage, and disseminate notifications effectively to alert/dispatch response and support agencies.

d) Identify and describe the actions that will be taken to notify and coordinate with adjacent jurisdictions.

5. Response Operations

    a) Describes deployment and management of response tasks, personnel, and resources to ensure life safety, stabilize the incident, isolate threat, limit impact, and protect property.

    b) Details how command and control is established (i.e. Incident Command, EOC, etc.)

    c) Development of incident response goals and objectives (i.e. incident action plan)

6. Demobilization

    a) Organized deactivation and release from duty of emergency response resources and personnel.

    b) Describe process of developing demobilization plan.

    c) Identify the individual by role, position, or job title that has the authority to release personnel and resources from duty.

    d) Outline decision-making process for determining when demobilization will take place

    e) Establish criteria for releasing personnel and resources.

7. Incident Close Out and Response Deactivation

    a) Identify processes for collection of required documentation.

    b) Identify processes to manage the accounting of supplies, equipment, and other materials.

    c) Describe formal transition process/change of command from response to recovery operations.

    d) Notification process to internal and external stakeholders of formal end to response operations, transition to recovery operations, and /or return to normal activity.

C. RECOVER

1. Describe process of preserving and restoring critical applications, systems and services in order to resume normal operations.

2. Disaster Recovery

   a) Identify individuals by position/job title that would have operational authority over recovery activity, if different from response phase.

   b) Establish process for implementing the organization’s information technology (IT) disaster recovery plan.

3. Business Continuity

   a) Discuss implementation of existing plans to ensure continuity of critical government services and business activity, and expedite resumption of normal operations.

4. System/Application Restoration

   a) Describe procedures to restore systems to the original state and validate the system has been cleared of any detected threats.

   b) Describe how affected and restored systems are tested and validated before being brought back online.

5. After Action Review (AAR) and Improvement Planning

   a) Detail process used by the jurisdiction to review and discuss the response in order to identify strengths and weaknesses in the emergency management and response program.

   b) Describe how the jurisdiction ensures that the deficiencies and recommendations identified in the AAR are corrected/completed.

III. ASSIGNMENT OF RESPONSIBILITIES

A. General list of tasks to be performed, by position and/or department, without the procedural details included in standard operating procedures.

B. Organizational charts can also be inserted here (i.e. Incident Command, Emergency Operations Center, Security Operations Center, Crisis Management Team, etc.)

IV. DIRECTION, CONTROL, AND COORDINATION

A. Identifies the individuals by position/job title that have operational and management authority over response operations.

B. Outlines how response activity and resource management is coordinated internally as well as with external stakeholders, vendors, agencies, and organizations.

V. INFORMATION COLLECTION, ANALYSIS, AND DISSEMINATION

A. Identifies the type of information needed, the source of the information, who uses the information, how the information is shared, the format for providing the information, and any specific times the information is needed.

VI. COMMUNICATIONS

A. Describes the communication protocols and coordination procedures used between response organizations during emergencies and disasters.

VII. ADMINISTRATION, FINANCE, AND LOGISTICS

A. Outlines general support requirements and the availability of services and support for incident response, as well as general policies for managing resources.

B. Describes pre-incident, operational, and post-incident documentation requirements

C. Existing contracts and contracting requirements for material resources, staffing, and vendor-managed services.

D. Purchasing and procurement requirements.

E. Cost tracking and funding requirements.

F. Inventory, supply, and resource tracking.

G. Processes for addressing legal issues and regulatory requirements.

## VIII. PLAN DEVELOPMENT AND MAINTENANCE

A. Discusses the overall approach to planning and the assignment of plan development and maintenance responsibilities.

B. Assigns responsibility for the overall planning and coordination to a specific individual by job title within the organization.

C. Establishes process and schedule for plan development, review, training, exercise, evaluation, and improvement.

## IX. POLICIES, AUTHORITIES, AND REFERENCES

A. Lists of laws, statutes, ordinances, executive orders, regulations, and formal agreements relevant to emergencies.

B. Specifies the extent and limits of the emergency authorities granted to the senior official, including the conditions under which these authorities become effective and when they would be terminated

C. Identifies state, national, international, and professional standards that apply to the plan.

D. Establishes any pre-delegation of emergency authorities that may not be described in other planning documents.

# CYBERSECURITY TRAINING AND EXERCISE GUIDE

# CYBERSECURITY TRAINING AND EXERCISE GUIDE

## Table of Contents

I. Introduction .......... 38

A. Purpose .......... 38

B. Scope .......... 38

C. Situation .......... 39

D. Assumptions .......... 40

II. Training .......... 40

A. Essential Cybersecurity Awareness Training for All Users .......... 40

B. Cybersecurity Training for Emergency Managers .......... 42

C. Emergency Management Training for IT Professionals .......... 43

III. Exercise .......... 44

A. Exercise Planning .......... 44

B. Special Considerations .......... 47

C. Discussion-Based Exercises .......... 47

D. Operations-Based Exercises .......... 48

E. Exercise Scenario Ideas .......... 48

F. Evaluation and Improvement .......... 57

IV. Information Resources for Training and Exercise .......... 58

V. Guide Development and Maintenance .......... 58

# I. Introduction

## A. Purpose

As part of an all-hazards approach to emergency management, the *Cybersecurity Training and Exercise Guide* provides general information and instructions for establishing and implementing an effective cybersecurity training and exercise program.

The contents of this Guide are intended to align state and federal emergency management training and exercise requirements with cybersecurity training and education standards established by the National Institute of Standards and Technology (NIST). In addition to NIST, this Guide incorporates concepts and elements from the Homeland Security Exercise and Evaluation Program (HSEEP), National Incident Management System (NIMS), Emergency Management Accreditation Program (EMAP), and National Fire Protection Association (NFPA).

## B. Scope

The Guide is intended for emergency managers in municipal, county, and local government agencies. It may also be useful to individuals responsible for emergency preparedness and business continuity functions in other public sector, private sector, healthcare, and academic organizations.

There are a wide variety of potential cyber threats and a constantly evolving list of methods and tactics used to conduct cyberattacks. The training and exercise activity outlined here is focused on cyber incidents that may:

-Pose an immediate threat to public health, safety, and security;

-Impact or disrupt the delivery of essential government and social services; or

-Require a coordinated, multi-agency, multi-disciplinary response

## C. Situation

Cybersecurity incidents and cyberattacks on computers, information networks, and communications systems are now part of the complex threat environment emergency managers must face.

In the State of Indiana, numerous high-profile cyberattacks have occurred in recent years. Targets of these attacks included government agencies, healthcare facilities, community organizations, businesses, school systems, and universities. Attacks have occurred in every region of the state and affected communities and organizations large and small, rural and urban.

Most of these incidents have involved the theft of sensitive data or ransomware attacks. These incidents had significant financial and public relations impacts, but did not pose an immediate safety threat. However, cyberattacks are increasingly targeting critical infrastructure sectors. A successful cyberattack on critical infrastructure could cause real-world operational damage and trigger cascading impacts that threaten public safety.

Nationally, in the vast majority of cybersecurity incidents, it was a lack of awareness and coordination that allowed the attacks to occur and delayed the response to the incidents. The problem was a failure to train and educate all people who are access points to information and operations systems, not a failure of technology or lack of resources.

Collaborating with information technology (IT) professionals and integrating cybersecurity training into a comprehensive emergency management program can help reduce the risk of a cyberattack, improve incident response, and limit the impacts should an attack occur.

This Guide is being used to address training gaps identified in a formal cybersecurity risk assessment and/or incident response planning process.

### D. Assumptions

In developing this document, it was assumed the government entity or organization intending to use the Guide had the following measures and practices in place:

- The Guide is being used to address training gaps identified in a formal cybersecurity risk assessment and/or incident response planning process.
- An individual, group, department, agency or third-party vendor is assigned and is responsible for managing information technology resources and information security for the government agency or organization.
- There are established organizational rules and policies in place for the safe and secure use of computers, tablets, mobile devices, personal devices, and any other internet-capable electronic devices issued to or used by an employee.
- Employees are made aware of device usage rules and IT incident reporting procedures.
- The user of this Guide is familiar with the concepts and practices outlined in the Homeland Security Exercise and Evaluation Program (HSEEP).
- Emergency managers have a basic awareness of cybersecurity threats and intend to include information technology professionals in cyber incident response planning, training and exercise activity.

## II. Training

Training is essential for protecting information and operation network systems and effectively responding to a cybersecurity incident. Training recommendations and suggested online, classroom, and resident training courses for emergency managers, IT professionals, and cybersecurity stakeholders are included in this section.

These courses can provide a basic understanding and awareness for both cybersecurity and emergency management concepts. The goals are for emergency managers and IT professionals to “speak each other’s language” and promote joint planning, training, and exercise activity.

### A. Essential Cybersecurity Awareness Training for All Users

People in an organization are both the greatest vulnerability and best line of defense in regard to cybersecurity. Training can be delivered as part of formal or ad hoc new employee training, ongoing in-service training, or as-needed at the direction of IT managers, supervisors, or executives.

Recommended best practices for cyber hygiene and critical information security training content are outlined in this section. Additional cybersecurity training can be found on Indiana's Cybersecurity Hub at www.in.gov/cybersecurity/3811.htm.

1. Basic Device and System Usage: Training that provides all users of an organization's information technology resources, including staff, managers, executives, and contract employees, awareness of policies and rules regarding the acceptable use of information devices and systems. This could include:

    - Mobile telephone, device, and application use
    - Computer use and portable data storage
    - Access to data networks, servers, drives, and folders
    - Internet browsing and social media restrictions
    - Approved use of official email and messaging applications
    - Personal mobile device and computer use for official business

2. Information Security Awareness: Instruction regarding the need and importance of information security, privacy measures, and cyber hygiene within an organization to protect valuable data, devices, and network systems. Examples include:

    - Physical security and protective measures for computers and mobile devices
    - Use of strong passwords for computers, mobile devices, email, and network access
    - Secure use of external data storage devices such as flash drives and external hard drives
    - Employee role in maintaining and supporting routine software updates, antivirus software, and firewall protections
    - Requirements for remote network access and use of virtual private networks
    - Use of public, personal, or unsecured Wi-Fi networks
    - Cyberattack methods, vectors, and tactics
    - Recognizing social engineering attempts, phishing emails, and malicious websites
    - Awareness of cybersecurity threats to mobile devices including location services, USB charging devices, mobile apps, malicious QR codes and texts messages

3. Incident Response Procedures: Internal processes and procedures for reporting and initially responding to unexplained computer or system malfunctions, unusual or suspicious network activity, loss of data or data access, detection of malicious software, or a confirmed cyberattack. Information provided in training could include:

    - Primary and alternate points of contact and methods for reporting a suspected or confirmed cybersecurity incident.
    - Essential information to provide when reporting an incident.
    - Immediate actions the user must take to help contain a suspected or confirmed cybersecurity threat.
    - The user's role in supporting an incident response including analysis, containment, eradication, evidence gathering, and recovery.

## B. Cybersecurity Training for Emergency Managers

These course recommendations are intended to familiarize emergency managers with cybersecurity terminology, core concepts, and best practices.

Training providers include the FEMA Emergency Management Institute (EMI), Texas A&M Engineering Extension Service (TEEX), Norwich University (NUARI), University of Texas San Antonio (UTSA), and the Criminal Justice Institute (CJI).

Detailed course information is available in the FEMA National Preparedness Course Catalog.

Basic
AWR-136: Essentials of Community Cyber Security (TEEX, Classroom)
AWR-175-W: Information Security for Everyone (TEEX, Online)
AWR-176-W: Disaster Recovery for Information Systems (TEEX, Online)

Intermediate

AWR-169-W: Cyber Incident Analysis and Response (TEEX, Online)

AWR-177-W: Information Risk Management (TEEX, Online)

AWR-366-W: Developing a Cyber Security Annex for Incident Response (NUARI, Online)

IS0523: Resilient Accord: Exercising Continuity Plans for Cyber Incidents (EMI, Online)

E0553: Resilient Accord: Cyber Security Planning Workshop (EMI, Classroom)

Advanced

AWR-353-W: Using the Community Cyber Security Maturity Model (UTSA, Online)

MGT-384: Community Preparedness for Cyber Incidents (TEEX, Classroom)

MGT-385: Community Cyber Security Exercise Planning (TEEX, Classroom)

MGT-452: Physical & Cybersecurity for Critical Infrastructure (TEEX, Classroom)

MGT-456: Integration of Cybersecurity Personnel into the EOC for Cyber Incidents (NUARI/TEEX, Classroom)

## C. Emergency Management Training for IT Professionals

These course recommendations are intended to provide IT professionals and cybersecurity stakeholders with foundational knowledge of emergency management. This includes Incident Command System, NIMS, emergency operations centers, exercise planning, and how IT professionals can be integrated into a coordinated response to a major cybersecurity incident.

Basic

IS0908: Emergency Management for Senior Officials (EMI, Online)

IS0100.c: ICS 100 Introduction to the Incident Command System (EMI, Online)

IS0200.c: ICS 200 Basic Incident Command for Initial Response (EMI, Online)

IS0700.b: National Incident Management System (EMI, Online)

IS0235.c: Emergency Planning (EMI, Online)

Intermediate

IS0546.a: Continuity of Operations Awareness (EMI, Online)

IS0120.c: An Introduction to Exercise (EMI, Online)

IS0775: Emergency Operations Center Management and Operations (EMI, Online)

AWR-366-W: Developing a Cyber Security Annex for Incident Response (NUARI, Online)

IS0523: Resilient Accord: Exercising Continuity Plans for Cyber Incidents (EMI, Online)

Advanced

MGT-456: Integration of Cybersecurity Personnel into the EOC for Cyber Incidents (NUARI/TEEX, Classroom)

E0553: Resilient Accord: Cyber Security Planning Workshop (EMI, Classroom)

PER-257: Cyberterrorism First Responder (UTSA, Classroom)

PER-371: Cybersecurity Incident Response for IT Personnel (CJI, Classroom)
E8515: Cybersecurity Symposium (EMI, Resident Course)

# III. Exercise

Cybersecurity incidents are complex. The response to these incidents is often equally complex, involving groups which are not traditional disaster response or emergency support function partners. Conducting exercises with IT professionals, private sector representatives, and community stakeholders is critical to ensure an effective, coordinated response to a cyberattack.

The nature of cybersecurity threats makes them unique. However, conducting exercises to test and evaluate response capabilities can be accomplished using well-established practices familiar to emergency managers. This section will provide best practices, planning considerations, and suggestions drawn from HSEEP to plan and conduct cybersecurity exercises.

## A. Exercise Planning

1. Exercise Participants: Those taking part in an exercise will vary depending on the nature, scope, and scale of the exercise being planned. This will likely include both traditional and non-traditional partners. Participants to consider could include:

   a) Emergency Support Function (ESF) organizations

   b) Chief Information Officer/IT Director for jurisdiction or organization

   c) IT /Data/Cybersecurity contractor for jurisdiction or organization

   d) Attorney or general counsel for jurisdiction or organization

   e) County Commissioners/County Council Members

   f) Municipally-elected officials/Mayors/Town Manger

   g) City/Town Council members

   h) Auditor, Treasurer, Assessor, Recorder, Surveyor

   i) Prosecutor, Clerk/Clerk of Courts

   j) Township Trustees or designee

   k) Human resources/Personnel department for jurisdiction or organization

   l) Electric power utility or electric cooperative

   m) Water/Wastewater/Stormwater utilities

   n) Natural gas utility

   o) Telecommunications provider or telephone cooperative

p) Hospitals, healthcare facilities, and providers

q) School district representatives

r) Cooperative extension service program representative

s) Chamber of Commerce/Local economic development stakeholders

t) Zoning/Building/Area planning commission members

u) Americans with Disabilities Act/Accessibility Office representative

v) Mass transit/rural transit service providers

w) Vendor-managed and contract service representatives

x) County insurance coverage provider

2. Exercise Planning Team: The composition of the Exercise Planning Team should reflect the agencies, groups, and organizations participating in the exercise. Incorporating subject-matter experts involved in incident planning, response, and recovery will help ensure the exercise scenarios are realistic, challenging, and adequately test key response functions.

    a) Planning Meetings: The complex nature of cybersecurity exercise design and development requires well organized meetings to ensure exercise success. In some situations, participants may be unfamiliar with exercise planning methodology and may never have taken part in a disaster exercise.

    b) Concept and Objectives Meeting: Identify the type, scope, objectives, and purpose.

    c) Initial Planning Meeting: Lay the foundation for exercise development.

    d) Midterm Planning Meeting: A forum for discussing organization, staffing concepts, and exercise logistics.

    e) Master Scenario Events List (MSEL) Meeting: A forum for creating and reviewing the scenario injects and timeline.

    f) Final Planning Meeting: Forum for reviewing exercise logistics, processes, and procedures.

    g) After-Action Meeting: Feedback for participating jurisdictions on their performance and plans for improvement.

3. Documentation: The requirement for exercise documentation will vary depending on the type and size of exercise being conducted, as well as the number and variety of participants.

**Seminar, Workshop, or Game:**

a) Budget

b) Required pre-exercise meeting sign-ins and agendas

c) Presentations (if applicable)

d) Agenda for exercise event

e) Exercise participant rosters/sign-in sheets

f) Executive summary

**Tabletop Exercise:**

a) Budget

b) Required pre-exercise meeting sign-ins and agendas

c) Agenda for exercise event

d) Situation manual

e) Exercise evaluation guides

f) Exercise participant rosters/sign-in sheets

g) After action report/improvement plan

**Drill, Functional, and Full-Scale Exercise:**

a) Budget

b) Required pre-exercise meeting sign-ins and agendas

c) Agenda for exercise event

d) Exercise plan

e) Master scenario events list

f) Controller and evaluator handbook

g) Exercise evaluation guides

h) Exercise participant rosters/sign-in sheets

i) After action report/improvement plan

## B. Special Considerations

Private-sector organizations and critical infrastructure stakeholders may require additional documentation before and after an exercise. There may be legal, regulatory, or internal policy compliance documentation requirements.

These may include memorandums of understanding, sector-specific reporting forms, or non-disclosure agreements.

## C. Discussion-Based Exercises

- Seminars: Orient participants or provide an overview of plans, policies, and procedures. Example: Review of Cybersecurity Incident Response Plan with cybersecurity stakeholders, emergency responders, or elected/appointed officials.
- Workshops: Focus on development of a planning product by the attendees. Example: Develop annexes, standard operating procedures, or checklists to support the activation of an incident response plan. These could be notification checklists, response and containment processes, or recovery procedures.
- Games: Simulation of operations that often involves two or more teams designed to depict an actual or hypothetical situation. Example: Groups of participants test their abilities to recognize and report phishing emails.
- Tabletop Exercise: Guided discussion following an incident scenario used to assess response plans, policies, and procedures. Example: Senior officials, ESF representatives, and IT professional are presented with a series of simulated network system failures and information injects. Participants talk through their coordinated response to a ransomware attack scenario.

## D. Operations-Based Exercises

- Drills: Test of a single operation or function in a single agency or organization. Example: Incident notification procedures and systems are tested to ensure all cyber incident response stakeholders receive alert messages.

- Functional Exercises: Tests individual capabilities, multiple functions, or activities within a function; however movement of personnel and equipment is simulated. Example: Emergency operations center is activated and ESF representatives respond to a simulated cyberattack scenario. Participants manage command, control, and coordination functions in real-time.

- Full-Scale Exercises: Combines command and control elements of a functional exercise with the actual deployment of operational personnel and resources to test incident response capabilities under realistic conditions. Example: IT professionals, public safety officials, and ESF agencies respond to a large-scale cyberattack which impacts critical infrastructure. This would include the deployment of resources and personnel in response to immediate and cascading community impacts of the attack.

## E. Exercise Scenario Ideas

- **Scenario 1**: **Phishing Trip**

  **Target**: Elected and Appointed Officials, System Access Credentials

  **Attack Method**: Spear Phishing

  **Triggering Incident Description**:

  County commissioners, county sheriff's department, and staff members in the county auditor's office receive emails requesting confirmation of their usernames and passwords for their official email accounts. The message says there has been suspicious activity in their email account and their account will be disabled unless they provide the requested information. In some cases, the username and passwords for other systems and databases were requested. The email appears to come from a current county employee with a legitimate email address. Some staff members report providing their username and password information. No system disruptions or suspicious system activity has been observed or reported.

  **Inject Discussion**:

  Who within your organization is notified?

  What is your organization's initial response?

  How do you warn and communicate with employees, contractors, and vendors?

What actions are taken to determine if malware is present or if data has been compromised?

Do you require external agencies or vendor-managed services?

Is law enforcement notified?

- **Scenario 2: The Hacktivist**

  **Target**: Local Government Websites

  **Attack Method**: SQL Injection, Denial of Service

  **Triggering Incident Description**:

  A well-known activist group threatens to shut down local government computer networks on social media. The next morning, multiple agency websites are offline. Some sites are defaced with vulgar, anti-government messages and the insignia of a hacking group. Other sites show error messages or are blank. An initial investigation also shows servers are being overloaded by internet traffic from thousands of sources simultaneously.

  **Inject Discussion**:

  Who within your organization is notified? What is that notification process?

  Are IT disaster recovery and incident response plans in place?

  What is your jurisdiction's initial response to the incident?

  What local, county, and/or state agencies are involved in the response?

  Do you require external or vendor-managed services to restore systems?

  Is law enforcement notified?

  How is public information, social media, and news media messaging managed?

- **Scenario 3: The Break-In**

  **Target**: Financial Data and Personally Identifiable Information

  **Attack Method**: Spyware, Data Extracting Malware

  **Triggering Incident Description**:

  Your jurisdiction is notified by federal and state law enforcement that a large amount of sensitive information from your jurisdiction's databases is being sold on a criminal website. The information included names, social security numbers, addresses, dates of birth, mother's maiden names, checking account, and credit card account information of residents, employees, and contractors. An initial network investigation identified malware that recorded log-in credentials and extracted data from several systems and databases. It is unclear how long the data breach has been in place.

**Inject Discussion**:

What is your organization's initial response?

Who is the lead response agency? Who are the supporting agencies?

Do you require external agencies or vendor-managed services?

How do you identify and warn those affected by the data breach?

Does your jurisdiction have insurance that covers costs related to the breach?

What legal or regulatory issues may result?

- **Scenario 4: The Lockout**

  **Target**: Local Government Computers, Networks, and Data

  **Attack Method**: Ransomware

  **Triggering Incident Description**:

  County employees in multiple local government offices and agencies report being unable to log in to their computers. Those that are able to log in to their computers are unable to access email, public records, and essential databases. Telephones and fax machines are also reported to be offline at several office locations. Fire, law enforcement, and EMS departments have been affected. Public safety communications has been impacted, but computer aided dispatching and 911 telephone systems are still operating normally. A local school system and several municipalities are also reporting similar problems. A message appears on computer screens declaring the computers and systems are locked and will only be released if the hacker is paid $50,000 in bitcoin currency.

  **Inject Discussion**:

  What is your organization's response?

  Are IT disaster recovery and incident response plans in place?

  Are business continuity and continuity of operations plans in place?

  How would your organization communicate internally and externally?

  Does your jurisdiction have cybersecurity insurance?

  Does your jurisdiction have access to bitcoin currency?

  Who is authorized to approve or deny the ransom payment?

  What are the potential cascading impacts to local government and community?

- **Scenario 5: False Alarm**

  **Target**: Outdoor Warning and Mass Notification Systems

**Attack Method**: Spyware, Credential Theft, DMTF Signal Spoofing

**Triggering Incident Description**:

At 11:30 PM, outdoor warning sirens across the county begin to sound. There is no severe weather or local emergency. Sirens were not activated by emergency management or other public safety agency. Attempts to access the siren control system and shut off sirens remotely are unsuccessful. Attempts by emergency management to shut off nearby sirens manually are also unsuccessful. Sirens momentarily deactivate, but immediately reactivate. Public safety dispatchers receive dozens of 911 calls from residents in a matter of minutes. Emergency management also receives reports that text messages falsely reporting a train derailment and hazardous chemical spill are being received on cellphones across the county.

**Inject Discussion**:

What is your organization’s response?

What agencies have access to the jurisdiction’s outdoor warning and/or emergency mass notification systems?

How can siren and notification system vendors be engaged to assist?

How would you quickly communicate accurate information to the public and media outlets?

What instructions would you provide to the public?

- **Scenario 6: Dispatch Flood**

  **Target**: Public Safety Answering Points

  **Attack Method**: Botnet, Telephony Denial of Service

  **Triggering Incident Description**:

  Public safety dispatchers begin receiving numerous 911 calls which immediately disconnect when answered. Police officers are initially dispatched to the hang-up call locations as the volume of calls grow over several minutes. Nearly 200 calls appear to be originating from the same 20 to 30 mobile telephones in the local area. When arriving on scene, police officers investigating the hang-up calls find residents are unaware of the 911 calls. Upon inspection, the cellphones making the calls appear to be locked with blank screens. Owners are unable to unlock the telephones or power them off. Owners reported that the cellphones “froze” when they clicked on a link in a social media app. similar incidents were reported by public safety agencies in adjacent counties.

  **Inject Discussion**:

  What is your organization’s initial response?

  What back-up systems, processes, facilities, or mutual aid agreements are in place?

How would you quickly communicate accurate information to the public and media outlets?

What instructions would you provide to the public?

How would commercial telecommunications and cellular telephone service providers assist? How can vendor assistance be requested?

Is state or federal assistance required? How is assistance requested in this situation?

- **Scenario 7: Flu Season**

  **Target**: Hospital Information Network

  **Attack Method**: Ransomware

  **Triggering Incident Description**:

  It is the height of a very severe flu season. Below zero temperatures and heavy snow are straining local emergency medical services and fire department resources. The emergency department in the community's largest hospital is experiencing a high volume of patients. The hospital is operating at near capacity. The hospital goes on full diversion due to patient volume and reported information network issues. Hospital staff are unable to access the electronic medical records system. The email system also experienced intermittent outages before going completely offline. Facilities staff are unable to access and control heating and ventilation systems. Temperature, air pressure, and humidity in the hospital can no longer be controlled. The system issues are initially blamed on the weather, until a ransomware message appears on multiple computer screens. The message demands $100,000 in bitcoin to restore the hospital's computer systems.

  **Inject Discussion**:

  How would public safety and public health agencies assist?

  Does the hospital have business continuity and emergency operations plans in place?

  What vendor-managed services would be required to maintain safe patient care activity at the hospital?

  Can other hospitals in the area manage the additional patient volume diverted from the affected hospital?

  Does the hospital have cybersecurity insurance?

  Is the hospital willing to pay the ransom?

  At what point would partial or full evacuation of the hospital be required?

- **Scenario 8: From Bad to Worse**

  **Target**: Emergency Management, Emergency Support Functions

  **Attack Method**: Email Extortion, Ransomware, Distributed Denial of Service

  **Triggering Incident Description**:

  A major flood has been impacting large areas of the state for several days and there is widespread damage across the county. The county emergency operations center has been activated to coordinate local response operations. There has been extensive local and national media coverage of the flood and the community's response. Mid-morning on the 5th day of operations, the emergency management director and several other county officials receive an email threatening to shut down the county's information networks unless a payment of $300,000 in bitcoin is made by the end of the day. Similar threats are received via the county's official social media sites. Shortly after the threats are received, the county government's email system and websites go offline for exactly 30 minutes, then come back online. Access to critical information databases is also lost, then restored. The hackers claim responsibility for the outage and threaten to increase the ransom amount and severity of attacks if the ransom payment is not received.

  **Inject Discussion**:

  Are IT disaster recovery and incident response plans in place? How are these plans activated?

  Are continuity of operations plans in place? How are these plans activated?

  How would an alternate EOC location be activated?

  Does the jurisdiction have cybersecurity insurance?

  Who has the authority to approve or deny the ransom payment? What is that process?

  What state or federal notifications or requests for assistance would be made?

  How is public information, social media, and news media messaging managed?

- **Scenario 9: Troubled Waters**

  **Target**: Water Utility Control Systems

  **Attack Method**: Industrial Control System Malware

  **Triggering Incident Description**:

  A local fire department responds to a large fire at the community's primary water treatment plant. Plant personnel report the fire started in an area of the plant that houses high lift water pumps. These pumps discharge treated drinking water into water mains and storage tanks for distribution. They also stated that just before the fire began, they were unable to access the computer system that controlled the pumps. The pumps began to cycle on and off, running at very high RPMs, then quickly shutting down. Attempts to access the control systems on site and from remote computer terminals failed. After several minutes, all of the pumps in the plant burned out and failed, with one pump catching fire. The plant can no longer maintain pressure within the system, which provides water to most of the county and large portions of adjacent counties. Water sampling of storage tanks also showed dangerously high levels of chemicals used to disinfect water at the plant. During a detailed analysis of the control systems, highly sophisticated malware was detected. The malware had caused the pumps to malfunction, altered the amount of disinfectant used to treat the water, and locked operators out of the system. The water supply for residents, hospitals, schools, manufacturing, and firefighting is now unavailable, and will likely be offline for weeks.

**Inject Discussion**:

How would the county's response be activated and coordinated?

How would the community be notified of the incident and warned of water contamination?

How could InWARN mutual aid resources be requested?

Is local, state, and/or federal law enforcement notified?

What state and federal resources could be requested?

How could drinking water be distributed to the community?

How would water for healthcare facilities be provided?

Would evacuation of hospitals be necessary?

How would schools be affected?

How could water for firefighting be supplied?

How would wastewater treatment be impacted?

What are the potential sanitation and public health hazards?

Are there legal and regulatory issues that must be addressed?

How could weather conditions affect potential impacts and response operations? (i.e. Winter vs. Summer)

- **Scenario 10: The Blackout**

  **Target**: Electric Power Utilities

  **Attack Method**: Advanced Persistent Threat, Industrial Control System Malware

  **Triggering Incident Description**:

  It is late Monday afternoon, the day before Election Day. Weather is fair across the Midwest with no severe weather or extreme temperatures. At 4:45 PM EST, multiple cable news networks begin to report a major power outage in the City of Detroit. Within 30 minutes of the initial news reports, widespread power outages are reported across Michigan, Wisconsin, Minnesota, and northern Ohio. At 5:40 PM power outages begin to occur across Central Illinois and Northwest Indiana.

At 6:15 PM, power outages occur across your entire county. Simultaneously, adjacent counties experience widespread outages. All fire stations, police stations, and healthcare facilities in the county are on generator power. The county public safety answering point and emergency operations center are also operating on generator power. 911 service is operational, but is quickly being overwhelmed by emergency calls and inquiries from the public. County Emergency Management is notified the Indiana State Emergency Operations Center is activated.

By 8:00 PM, multiple power companies and regional transmission organizations confirm massive power outages in seven states across the Midwest. The cause of the blackout, as well as when power will be restored, is unknown. Locally, nearly all traffic lights in the county are out. Numerous vehicle accidents and major traffic backups are reported. Grocery stores, gas stations, hardware, and home improvement stores are frantically requesting law enforcement assistance to deal with security and crowd control problems. Fire departments are responding to multiple fires at electric power substations and pole-mounted transformers across the county. EMS response is delayed due to the volume of calls and traffic congestion. Water and wastewater treatment plants remain operational, but are on emergency generator power. There are sporadic landline telephone and internet service outages, but cellular telephone systems are operating normally.

At 10:00 PM, the U.S. Department of Homeland Security (USDHS) confirms the power outages were caused by a massive cyberattack against power companies and regional power management organizations. The identity of the attacker and the method of attack are not announced.

In Indiana, it is estimated 90 % of the state is without electricity. Only a few counties in Northeastern Indiana have power. Areas of the Midwest not affected by the blackout include the City of Chicago and areas of Northern Illinois, Southwestern Michigan, and most of Central and Southern Ohio. The State of Kentucky is not impacted by the power outage. The Governor of Indiana formally declares a state of emergency, activates the National Guard, and requests federal assistance.

24 hours after the attack began, USDHS officials confirm the attack is sophisticated, coordinated, and consistent with the capabilities of a nation state. The President of the United States issues a Major Disaster Declaration. Cyber incident response operations have isolated and contained the impacts to the Midwest. Electrical power in the rest of the U.S. is unaffected. Across the Midwest, major physical damage to power generation plants, power transmission, and power distribution infrastructure has occurred. Due to the extent of the damage and compromise of control systems, the local electric power utility reports repair and power restoration in the county may not begin for two to three weeks. Full restoration of power to all areas of the county may take up to three months.

**Inject Discussion**:

How would the county's incident response be activated and coordinated?

How would Emergency Support Functions be mobilized and staffed?

How would situational awareness be established and maintained?

What are your jurisdiction's incident priorities, goals, and objectives?

What emergency response and continuity of operations plans are in place? How would these plans be implemented?

What are the immediate public safety, security, and health concerns?

How would critical county information networks and telecommunication systems be maintained and protected during an extended power outage. How would county and/or contract IT professionals be integrated into the incident response?

How would local elected officials be engaged? What emergency orders would need to be issued?

How would the county EOC establish and maintain communications with local, county, district, volunteer, state, and federal partners during a prolonged power outage?

How would resource needs be assessed and requests for assistance communicated?

How long can critical public safety, healthcare, water/wastewater utility, and telecommunications facilities operate on emergency generator power without refueling?

What are the anticipated fuel needs for vehicles and generators? What type of fuel is required?

How would public information, warnings, and alerts be managed and communicated?

How would critical staffing needs be met? (i.e. public safety, healthcare, mass care)

How would potable water be provided to the community if water utility systems fail?

How would natural gas utilities in your area be affected?

How would wastewater treatment and community waste management services be maintained?

How would transportation infrastructure and services be affected? (i.e. streets, highways, rail, airports, public transportation)

During a prolonged power outage lasting weeks or months, how would fuel distribution and fuel use be prioritized? How could community fuel rationing be implemented and maintained?

What could be done to help maintain retail food and fuel services at grocery stores and gas stations?

How would food be provided to the community if grocery stores could not remain open?

What are the anticipated long-term mass care and sheltering needs?

How would access and functional needs populations, residents of long-term care facilities, and those in home healthcare programs receive assistance?

What is the impact on local school systems?

How would volunteers and donations be managed?

What are the potential financial issues that would need to be addressed? (i.e. county employee payroll, purchasing, cost tracking, damage costs, documentation, bank closures)

What government and social services could be maintained? (i.e. courts, county offices, WIC)

How would the election, scheduled for the day after the attack occurred, be affected?

How would local government assist power companies in repairing damaged infrastructure?

Once damaged equipment was repaired and control systems brought back online, how would local government agencies support the safe reenergizing of the local power grid and restoration of power?

How would economic impacts to the community be mitigated? How would long-term recovery activities be managed?

How would county and/or contract IT professionals be integrated into long-term recovery activity?

## F. Evaluation and Improvement

The evaluation phase for all exercises includes a formal exercise evaluation, an integrated analysis, and an After Action Report/Improvement Plan (AAR/IP) that identifies strengths and areas for improvement of an agency’s preparedness, based on exercise performance. Recommendations developed during evaluation are used in improvement planning phase.

During improvement planning, the corrective actions identified in the evaluation phase are assigned, with due dates, to responsible parties; tracked to implementation; and then validated during subsequent exercises.

The importance of applying lessons learned, from both successes and failures, cannot be overstated. True cybersecurity preparedness can only be accomplished through a constant cycle of effective planning, training, exercise, and improvement

## IV. Information Resources for Training and Exercise

Indiana Cybersecurity Hub

www.in.gov/cyber

Indiana Cybersecurity Hub – Emergency Response and Recovery

https://www.in.gov/cybersecurity/3813.htm

Indiana Information Sharing and Analysis Center (IN-ISAC)

https://www.in.gov/cybersecurity/in-isac/

Indiana Department of Homeland Security Exercise Guide

https://www.in.gov/dhs/files/IDHS-Exercise-Guide-v4.pdf

FEMA National Training and Education Division (NTED)

https://www.firstrespondertraining.gov/frts/npccatalog

Homeland Security Exercise and Evaluation Program (HSEEP) Toolkit

https://preptoolkit.fema.gov/hseep-resources

Industrial Control Systems Cyber Emergency Response Team (ICS CERT) Training

https://www.us-cert.gov/ics/Training-Available-Through-ICS-CERT

United States Cyber Emergency Response Team (US CERT) Training

https://niccs.us-cert.gov/training

National Institute of Standards and Technology (NIST) Cybersecurity Framework

https://www.nist.gov/cyberframework

## V. Guide Development and Maintenance

This Guide was developed by the Emergency Services and Exercise Subcommittee of the State of Indiana Governor's Executive Council on Cybersecurity. The Subcommittee was chaired by the Executive Director of the Indiana Department of Homeland Security. Subcommittee members included multi-disciplinary representatives from public sector, private sector, and academic organizations including:

- Citizens Energy Group
- Indiana American Water
- Indiana Department of Homeland Security
- Indiana Department of Transportation
- Indiana Statewide 911 Board
- Indiana University
- Indiana University Health
- Ivy Tech Community College
- Resilient Strategies, LLC
- Ritter Strategic Services

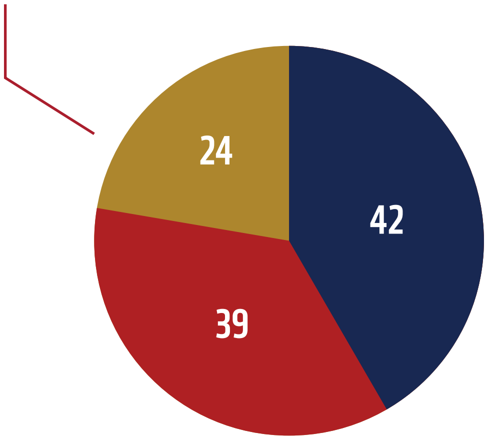
The Guide will be reviewed, revised, and maintained by the Indiana Department of Homeland Security, in collaboration with the members of the Emergency Services and Exercise Subcommittee, and at the direction of the Cybersecurity Program Director.

# CYBERSECURITY ATTACKS IN INDIANA: QUICK RESPONSE GUIDE

# CYBERSECURITY ATTACKS IN INDIANA: QUICK RESPONSE GUIDE

**105** total breaches reported over the last 12 months

**94%** of malware continues via email



| | |
|---|---|
| 42 | State, County and Municipalities Government |
| 39 | K-12 and Higher Education |
| 24 | County / Local Healthcare (not privately owned) |

## REPORT A CYBER CRIME

When an organization's experiencing a cyber attack, follow these steps to report the cyber crime.

### STEP 1 - CONTACT LAW ENFORCEMENT

- FBI Internet Crime Complaint Center (IC3) Alert authorities of suspected criminal or civil violations.
- **Indiana State Police (ISP)** Cybercrime & Investigative Technologies specialize in conducting cyber crime investigations.
- If there is an immediate threat to public health or safety, call 911.

### STEP 2 - ADDITIONAL REPORTING SUCH AS:

- **Indiana Attorney General** requires organizations report any security breach resulted in exposure of personal information. For more information, click here.
- **Regulators:** Regulated organizations may need to report cyber crimes to other state or federal agencies.
- **Secretary of State:** If necessary, contact the SOS offices regarding any related cyber incidents at electionsecurity@sos.in.gov.
- **Federal Government:** This fact sheet explains how to report cyber crimes to many federal agencies.

### STEP 3 - UTILIZE ADDTIONAL RESOURCES

Utilize additional resources about tips regarding avoiding ransomware, National Governors Association Response Planning Memo, National Emergency Readiness Team information, Department of Homeland Security's National Cybersecurity and Communications Integration Center, and more for 24/7 cyber situational awareness, incident response, and management center at www.in.gov/cybersecurity/3807.htm.

### STEP 4 - INFORMATION SHARING

It's important to share cyber crime information with other organizations to protect critical infrastructure, the State of Indiana, and our nation. Learn more at www.in.gov/cybersecurity/3819.htm.

***Source: HIPPA Breach reporting, public news, Indiana Attorney General Breach reporting from July 2018 – July 2019; 2019 Verizon Data Breach Report**

# CYBERSECURITY ATTACKS IN INDIANA: QUICK RESPONSE GUIDE

## THREE STEPS TO RESILIENCY AGAINST RANSOMWARE NOW

### STEP 1 - BACK UP YOUR SYSTEM - NOW AND DAILY

Immediately and regularly back up all critical agency and system configuration information on a separate device and store the back-ups offline, verifying their integrity and restoration process. If recovering after an attack, restore a stronger system than you lost, fully patched and updated to the latest version.

### STEP 2 - REINFORCE BASIC CYBERSECURITY AWARENESS AND EDUCATION

Ransomware attacks often require the human element to succeed. Refresh employee training on recognizing cyber threats, phishing and suspicious links – the most common vectors for ransomware attacks. Remind employees of how to report incidents to appropriate information technology staff in a timely manner, which should include out-of-band communication paths.

### STEP 3- REVISIT AND REFINE CYBER INCIDENT RESPONSE PLANS

Agencies must have a clear plan to address attacks when they occur, including when internal capabilities are overwhelmed. Make sure response plans include how to request assistance from external cyber first responders, such as state agencies, CISA and the MS-ISAC, in the event of an attack.

## EMERGENCY MANAGER RESOURCES

To find cybersecurity toolkit, planning templates, guides, resources, and more for emergency managers, visit https://www.in.gov/cybersecurity/3818.htm.

***Source: HIPPA Breach reporting, public news, Indiana Attorney General Breach reporting from July 2018 – July 2019; 2019 Verizon Data Breach Report**

# CYBER EMERGENCY RESILIENCE AND RESPONSE STATE GUIDE

# CYBER EMERGENCY RESILIENCY AND RESPONSE STATE GUIDE

## Table of Contents

1.0 Introduction .......... 64

2.0 Purpose .......... 64

3.0 Scope .......... 64

4.0 Cyber Emergency Preparation and Response Plan Core Group .......... 65

5.0 Cyber Emergency Preparation Process .......... 68

6.0 Response Process .......... 69

7.0 Plan Maintenance .......... 70

## 1.0 Introduction and Definitions

The Indiana Cyber Emergency Resiliency and Response State Guide (State Guide) was created to communicate the roles of an effective emergency response to a cyber emergency from the Executive Branch of Indiana government and indicate what roles partners may have during a cyberattack.

Determining which organizations should be involved and the roles they will play has proven challenging at all levels of government for nontraditional catastrophic emergencies such as a cyber attack. Emergency managers often have a difficult time understanding the technical nature of a cyber attack and how that fits in an emergency response while still developing decision-making processes that are true to an all-hazards approach. Below are emergency management resources to assist in planning and responding to a cyber attack.

### Cyber Emergency VS Cyber Incident

The State of Indiana defines a **cyber emergency** as any actual, imminent, or potential incident that will adversely affect public health, safety, or security; the environment; or economic prosperity on a level materially significant to the State of Indiana or its operations that requires a coordinated state response.

The State of Indiana defines a **cyber incident** as it is described in the Presidential Policy Directive 41, which is “an event occurring on or conducted through a computer network that actually or imminently jeopardizes the confidentiality, integrity, or availability of computers, information or communications systems or networks, physical, or virtual infrastructure controlled by computers or information systems, or information resident thereon.”

## 2.0 Purpose

The State Guide the roles, considerations, and process to effectively coordinate the proper resources to proactively protect and defend state-owned data systems and networks during a cyber emergency. This will also provide clarification to the state’s role in assisting local units of government in a cyber-related incident as well as coordinating with private sector partners.

## 3.0 Scope

The State Guide will be utilized when the following criteria are met:

- A cyber emergency involving activation of state level continuity of operations (COOP), or continuity of government (COG) plans.
- A cyber event that has a material impact on public safety.
- A threat or incident involving state-level, cyber-critical infrastructure.
- When requested by:
  - A local government entity
  - Director of the Indiana Office of Technology
  - Director of the Department of Homeland Security
  - The Adjutant General of Indiana

- When directed by:
  - The Governor of Indiana

## 4.0 Cyber Emergency Resiliency and Response Partners

The State of Indiana relies on a core group of agencies to assess the circumstances, determine an emergency, and deliver the response needed from state government. Inclusion in the core group is driven by the essential expertise and capabilities needed from the Executive Branch to assess and potentially assist in a response to the cyber emergency situation. As with many other threats and hazards, the success of resiliency and response must rely on the state, federal, public, military, and private partners.

### STATE AGENCIES AND PARTNERS

#### OFFICE OF THE GOVERNOR

The Governor provides overall direction and control for the preparation and carrying out of all emergency actions, including development and execution of the State's Comprehensive Emergency Management Plan. State agencies will support emergency operations in accordance with Executive Order 17-02.

#### INDIANA DEPARTMENT OF HOMELAND SECURITY

IDHS is tasked to coordinate the state's emergency plans, and serve as the coordinating agency for state efforts for preparedness for, response to, mitigation of, and recovery from emergencies and disasters. As with other hazard-related emergencies, IDHS manages the operations of the State Emergency Operations Center.

#### INDIANA OFFICE OF TECHNOLOGY

IOT oversees and manages the IN-ISAC. IOT is responsible for the security of state government information networks and all domains and is responsible for protecting the State's IT infrastructure from internal and external cybersecurity threats. IOT will assist IDHS during an cyber emergency activation with situational awareness, identifying external decision-makers, and accessing the necessary mitigation resources and lead remediation efforts if the event affected state government infrastructure.

#### INDIANA STATE POLICE

The ISP Office of Intelligence and Investigative Technologies (OIIT) focuses on cybersecurity incidents with a criminal nexus. The Cybersecurity Crime and Investigative Technologies Section and the Crime Analysis Section conduct activities related to cybersecurity forensics, cybersecurity crime investigations including those involving network intrusion and exploitation, electronic surveillance, and crimes against children.

The Indiana Intelligence Fusion Center (IIFC) collaborates with the IN-ISAC to conduct criminal intelligence analysis and incident reporting involving cybersecurity crimes. In the event that a criminal nexus is suspected in a cybersecurity emergency, law enforcement will investigate. Post-recovery, the IIFC may work with the IN-ISAC to help generate analytical after-action reports for external partners.

### INDIANA NATIONAL GUARD

The INNG has a Cybersecurity Mission comprised of experts in both preparedness and response efforts. As with other state emergencies, IDHS Executive Director may request deployment of cybersecurity force packages to support incident response.

### INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY

Signed by Governor Eric. J Holcomb on January 9, 2017, the Indiana Executive Council on Cybersecurity (IECC or Council) was continued through Executive Order 17-11 with the recognition that a cross-sector body of subject-matter experts is required to form an understanding of Indiana’s cyber risk profile, identify priorities, establish a strategic framework of Indiana’s cybersecurity initiatives, and leverage the body of talent to stay on the forefront of the cyber risk environment.

Led by the Indiana Department of Homeland Security, Indiana Office of Technology, Indiana State Police, and the Indiana National Guard, the Council is made up of government (local, state, and federal), private-sector, military, research, and academic stakeholders to collaboratively move Indiana’s cybersecurity to the Next Level. With 35 Council members and more than 250 advisory members, the Council delivered a comprehensive strategy plan to Governor Holcomb September 2018.

Moreover, the experts of the Council are charged with providing best practices, resources, and information to increase the state resiliency against cyberattacks. In addition to the private and public partners, state agencies and elected officials such as the Indiana Economic Development Corporation, Indiana Secretary of State, Indiana Attorney General, and many more have come together to increase the resiliency.

In a cyber emergency, experts from the Council may be included as a part of the Cybersecurity Advisory Group.

### CYBERSECURITY ADVISORY GROUP

The Indiana Cybersecurity Advisory Group (CAG) provides operational guidance and subject-matter expertise in support of a coordinated state cybersecurity incident response. The CAG will assess the incident and organize the strategic response to give to IDHS’s Emergency Operations Center. The CAG also develops, coordinates and recommends courses of action and response strategies. Designated agency representatives include the IOT Chief Information

Security Officer, or designee, ISP Commander, Intelligence and Investigative Technologies or designee, INNG Defensive Cybersecurity Programs Lead, or designee, Indiana Cybersecurity Program Director, IDHS Division Director, Response and Recovery, or designee and selected subject-matter experts.

## FEDERAL AGENCIES

### U.S. DEPARTMENT OF HOMELAND SECURITY

The Department of Homeland Security (DHS) is the designated lead agency during a cybersecurity incident requiring a federal response. Their primary functions are to identify the source of disruption and help remove it, determine how they gained access, assess the damage, and provide guidance to the organization on how to make their system more secure.

### FEDERAL BUREAU OF INVESTIGATIONS

The FBI is the lead federal agency for investigating cybersecurity-attacks by criminals, overseas adversaries, and terrorists. Specially trained FBI agents and analysts based at the FBI Indianapolis Field Office investigate computer intrusions, theft of intellectual property and personal information, child pornography and exploitation, and online fraud.

### U.S. SECRET SERVICE

The Secret Service maintains Electronic Crimes Task Forces, which focus on identifying and locating international cybersecurity criminals connected to cybersecurity intrusions, bank fraud, data breaches, and other computer-related crimes. The Secret Service also runs the National Computer Forensic Institute, which provides law enforcement officers, prosecutors, and judges with cybersecurity training and information to combat cybersecurity crime.

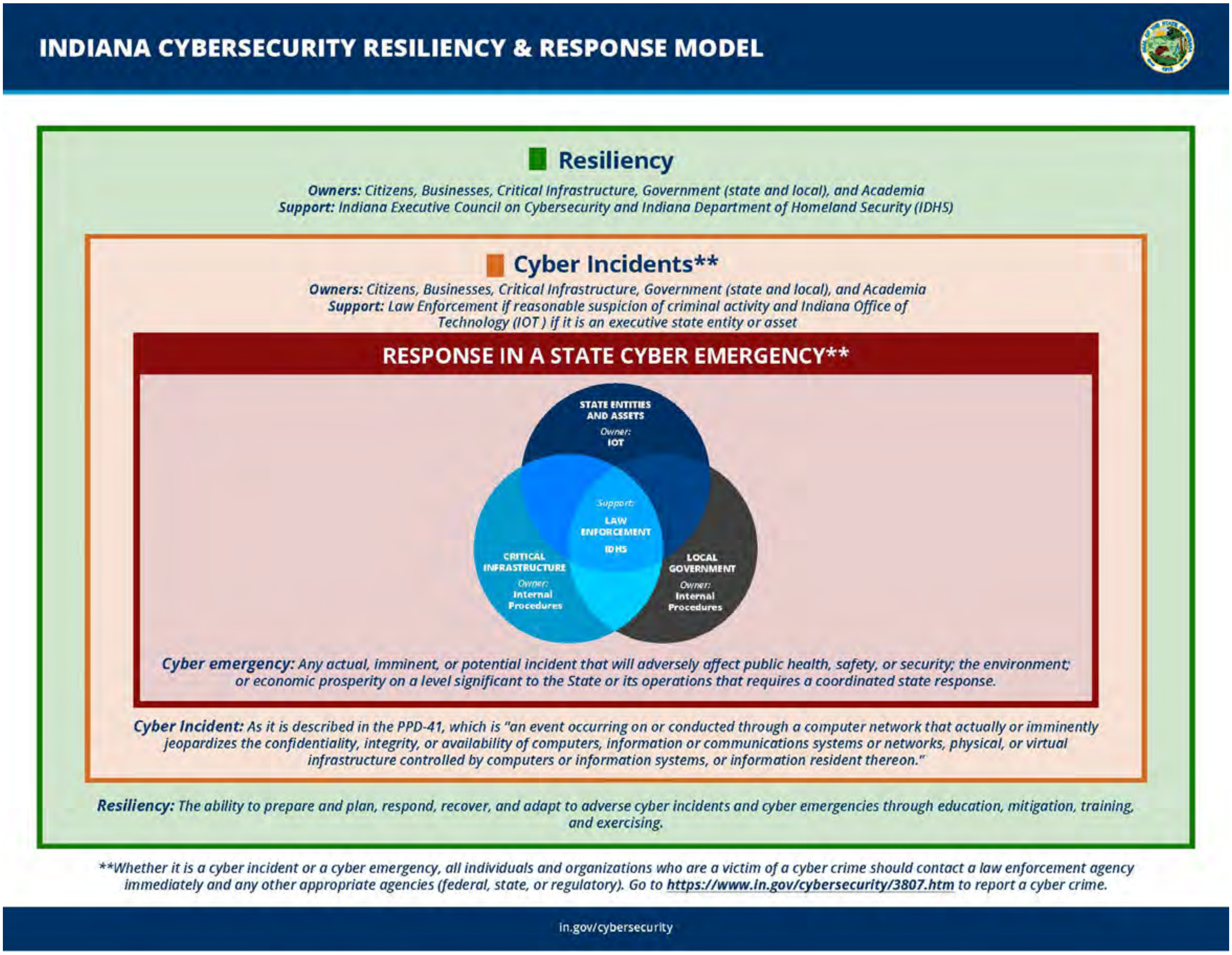
### U.S. DEPARTMENT OF JUSTICE

DOJ’s Offices of U.S. Attorneys and its’ Criminal and National Security Divisions, working with federal law enforcement agencies, use criminal and national security authorities to investigate, prosecute, and disrupt cyber threats and to apprehend cyber threat actors. Information and evidence obtained pursuant to appropriate legal process are used to identify the source of cyber incidents and to gather pertinent cyber threat information.

## 5.0 Cyber Emergency Resiliency Efforts

The State of Indiana core agency group include the Indiana Department of Homeland Security, Indiana Office of Technology, Indiana National Guard, and Indiana State Police.

This core agency group assists and leads in the overseeing of the cybersecurity resiliency efforts of the Indiana Executive Council on Cybersecurity and the ability for the state to be prepared to enable the rapid and effective response needed by state government constituents during a cyber emergency or cyber incident as appropriate. The following Indiana Cybersecurity Resiliency and Response Model further identifies the owners and support organizations during the resiliency phase, a cyber incident, and a cyber emergency.



INDIANA CYBERSECURITY RESILIENCY & RESPONSE MODEL

🟩 Resiliency

***Owners:*** *Citizens, Businesses, Critical Infrastructure, Government (state and local), and Academia*
***Support:*** *Indiana Executive Council on Cybersecurity and Indiana Department of Homeland Security (IDHS)*

🟧 Cyber Incidents**

***Owners:*** *Citizens, Businesses, Critical Infrastructure, Government (state and local), and Academia*
***Support:*** *Law Enforcement if reasonable suspicion of criminal activity and Indiana Office of Technology (IOT ) if it is an executive state entity or asset*

RESPONSE IN A STATE CYBER EMERGENCY**

STATE ENTITIES AND ASSETS
*Owner:*
IOT

*Support:*
LAW ENFORCEMENT
IDHS

CRITICAL INFRASTRUCTURE
*Owner:*
Internal Procedures

LOCAL GOVERNMENT
*Owner:*
Internal Procedures

***Cyber emergency:*** *Any actual, imminent, or potential incident that will adversely affect public health, safety, or security; the environment; or economic prosperity on a level significant to the State or its operations that requires a coordinated state response.*

***Cyber Incident:*** *As it is described in the PPD-41, which is "an event occurring on or conducted through a computer network that actually or imminently jeopardizes the confidentiality, integrity, or availability of computers, information or communications systems or networks, physical, or virtual infrastructure controlled by computers or information systems, or information resident thereon."*

***Resiliency:*** *The ability to prepare and plan, respond, recover, and adapt to adverse cyber incidents and cyber emergencies through education, mitigation, training, and exercising.*

***Whether it is a cyber incident or a cyber emergency, all individuals and organizations who are a victim of a cyber crime should contact a law enforcement agency immediately and any other appropriate agencies (federal, state, or regulatory). Go to **https://www.in.gov/cybersecurity/3807.htm** to report a cyber crime.*

in.gov/cybersecurity

## 6.0 Response Process

### Report a Cyber Crime

When an organization’s experiencing a cyber attack, the following these steps should be taken.

Step 1: Contact Law Enforcement

- FBI Internet Crime Complaint Center (IC3)
- Indiana State Police (ISP) Cybercrime and Investigative Technologies
- If there is an immediate threat to public health or safety, call 911.

Step 2: Additional Reporting

In addition to reporting the cyber attack, an organization should consider contacting other agencies to report the attack, which include:

- **Indiana Attorney General** requires organizations report any security breach resulted in exposure of personal information. For more information, click here.
- **Regulators:** Regulated organizations may need to report cyber crimes to other state or federal agencies.
- **Secretary of State:** If necessary, contact the SOS offices regarding any related cyber incidents at electionsecurity@sos.in.gov
- **Federal Government:** This fact sheet explains how to report cyber crimes to many federal agencies.
- **Indiana Department of Homeland Security** at WatchDesk@dhs.IN.gov.

Step 3: Utilize additional resources

For additional tips regarding avoiding ransomware and information from the National Governors Association Response Planning Memo, National Emergency Readiness Team information, Department of Homeland Security’s National Cybersecurity and Communications Integration Center, and more visit www.in.gov/cybersecurity/3807.htm.

Step 4: Information Sharing

It’s important to share cyber crime information with other organizations to protect critical infrastructure, the State of Indiana, and our nation. Learn more at www.in.gov/cybersecurity/3819.htm.

It is important to note that once the State of Indiana is notified, the following process was created with a single objective: Get the emergency into the hands of capable, representative, and empowered individuals to bring Indiana government resources and relationships quickly to the aid of those suffering from a cyber emergency.

Once a request for assistance is received by one or more state agencies, the core agency group will convene and assess the traits and impacts of the cyber incident or emergency and the value of their resources as they apply to an effective response to the emergency, whether it is with state resources or working with other key public and private partners. Cyberattacks shared with the State of Indiana will stay at the highest level of leadership and only shared with need-to-know parties. After each cyber event reported to one or more of the core agency group, a post-emergency evaluation will be completed by the state's Cybersecurity Program Director to rate response effectiveness, identify additional needs, and process adjustments.

## 7.0 Plan Maintenance

The State of Indiana Department of Homeland Security Executive Director, Indiana Office of Technology Chief Information Officer (CIO), and Indiana Cybersecurity Program Director are responsible for overall administration and maintenance of this State Guide.

# ADDITIONAL EMERGENCY MANAGER CYBERSECURITY RESOURCES

# ADDITIONAL EMERGENCY MANAGER CYBERSECURITY RESOURCES

Below you will find a variety of additional resources for emergency managers regarding preparing, responding, and recovering from a cyberattack.

- MS-ISAC Security Primer on Ransomware
- US DHS Cybersecurity and Infrastructure Security Agency (CISA) Ransomware Website
- National Governors Association Disruption Response Planning Memo
- NASCIO Cyber Disruption Planning Guide
- Emergency Services Sector Cybersecurity Initiative
  A Department of Homeland Security resource to better understand and manage cyber risks and to coordinate the sharing of cyber information and tools between subject matter experts (both inside and outside the federal government) and the Emergency Services Sector disciplines.
- Emergency Services Sector Cybersecurity Framework Implementation Guidance
- US DHS Emergency Services Sector Cybersecurity Best Practices
- Ready.gov
  Ready.gov is a national public service campaign designed to educate and empower the American people to prepare for, respond to, and mitigate emergencies, including cybersecurity.
- US DHS Cybersecurity and Infrastructure Security Agency (CISA) Cyber Resilience Review (CRR)
  The CRR is a no-cost, voluntary, non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices. The CRR may be conducted as a self-assessment or as an on-site assessment facilitated by DHS cybersecurity professionals. The CRR assesses enterprise programs and practices across a range of ten domains including risk management, incident management, service continuity, and others. The assessment is designed to measure existing organizational resilience as well as provide a gap analysis for improvement based on recognized best practices.

  - Information Sheet - Summary of the CRR process.
  - Method Description and User Guide - Walk-through for how an organization can conduct a CRR self-assessment.
  - Self-Assessment Package - Self-assessment form and report generator.
  - Question Set with Guidance - Self-assessment question set along with accompanying guidance.
  - CRR NIST Framework Crosswalk - Cross-reference chart for how the NIST Cybersecurity Framework aligns to the CRR.
- National Cyber Incident Response Plan (NCIRP)
  The NCIRP, developed by the United States Computer Emergency Readiness Team (US-CERT), describes a national approach to dealing with cyber incidents; addresses the important role that the private sector, state and local governments, and multiple federal agencies play in responding to incidents and how the actions of all fit together for an integrated response.
- National Cybersecurity and Communications Integration Center (NCCIC)
  A 24/7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the federal government, intelligence community, and law enforcement.

For more information for individuals, businesses, government, educators, and more, visit www.in.gov/cyber.

# BIBLIOGRAPHY

# BIBLIOGRAPHY

In addition to the following resources used to create the *Indiana Emergency Manager Cybersecurity Toolkit*, a significant amount of work and resources were from the experts from the Indiana Executive Council on Cybersecurity, feedback from Indiana Emergency Managers at all levels (city, county, district, private, and state), and national partner agencies such as US Department of Homeland Security, FEMA, National Governors Association Cybersecurity Academy, CIA, FBI, US Secret Service, and National Guard.

Research conducted to develop this toolkit also included information from the following organizations:

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.

Cybersecurity and Infrastructure Security Agency (CISA): Responsible for protecting the Nation's critical infrastructure from physical and cyber threats. This mission requires effective coordination and collaboration among a broad spectrum of government and private sector organizations.

Executive Order 13800 - Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure: Emphasizes four core areas: securing and modernizing federal networks, protecting the critical infrastructure that maintains the American way of life, deterring America's adversaries in cyberspace, and building a stronger cybersecurity workforce.

*Other more specific citied references include, but are not limited to:*

Federal Emergency Management Agency (FEMA). "National Incident Management System (NIMS)," October 2017. https://www.fema.gov/national-incident-management-system. (accessed September 2018)

Emergency Management Accreditation Program (EMAP). "Emergency Management Accreditation Program (EMAP)," 2001. https://www.emap.org/ (accessed September 2018).

National Fire Protection Association (NFPA) Standard 1600. "NFPA Standard 1600," June 2018. https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=1600 (accessed September 2018).

Centers for Medicare and Medicaid Services (CMS). "Emergency Preparedness Rule," November 16, 2016. https://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/SurveyCertEmergPrep/Emergency-Prep-Rule.html (accessed September 2018)

The Joint Commission. "Emergency Management Standard," https://www.jointcommission.org/emergency_management.aspx (accessed September 2018)

The White House. "Presidential Policy Directive -- United States Cyber Incident Coordination (PPD 41)" July 26, 2016.: https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential- policy-directive-united-states-cyber-incident (accessed September 2018)

Federal Emergency Management Agency (FEMA). "Homeland Security Exercise Evaluation Program (HSEEP)", https://www.fema.gov/hseep (accessed September 2018)

U.S. Department of Health and Human Services. “Health Insurance Portability and Accountability Act (HIPAA) Security Rule”, February 20, 2003. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (accessed September 2018)

U.S. Department of Homeland Security (DHS). “U.S. Computer Emergency Readiness Team (US-CERT)”., https://www.us- cert.gov/ (accessed September 2018)

Communications Sector Coordinating Council (CSCC) and Communications Sector Government Coordinating Council (CGCC). “Communications Sector-Specific Plan.” *Cybersecurity and Infrastructure Security Agency*. Department of Homeland Security and, 2015. https://www.cisa.gov/sites/default/files/publications/nipp-ssp-communications-2015-508.pdf. (accessed October 2019)

Dams Sector Coordinating Council (CSCC) and Dams Sector Government Coordinating Council (DGCC). “Dams Sector-Specific Plan.” *Cybersecurity and Infrastructure Security Agency*. Department of Homeland Security, 2015. https://www.cisa.gov/sites/default/files/publications/nipp-ssp-dams-2015-508.pdf. (accessed October 2019)

Emergency Services Sector Coordinating Council (ESSCC) and Emergency Services Sector Government Coordinating Council (ESSGCC). “Emergency Services Sector-Specific Plan.” *Cybersecurity and Infrastructure Security Agency*. Department of Homeland Security and, 2015. https://www.cisa.gov/sites/default/files/publications/nipp-ssp-emergency-services-2015-508.pdf. (accessed October 2019)

U.S. Department of Energy (DOE). “Energy Sector-Specific Plan - 2015 | CISA.” Cisa.gov, 2015. https://www.cisa.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf. (accessed October 2019)

Department of Homeland Security (DHS) and the General Services Administration (GSA). “Government Facilities SSP - 2015 | CISA.” Cisa.gov, 2015. https://www.cisa.gov/sites/default/files/publications/nipp-ssp-government-facilities-2015-508.pdf. (accessed October 2019)

Healthcare and Public Health (HPH) Sector Coordinating Council (SCC) and Government Coordinating Council (GCC). “Healthcare Sector-Specific Plan - 2015 | CISA.” Cisa.gov, 2015. https://www.cisa.gov/sites/default/files/publications/nipp-ssp-healthcare-public-health-2015-508.pdf. (accessed October 2019)

Water Sector Coordinating Council and the Water Sector Government Coordinating Council. “Water Sector-Specific Plan - 2015 | CISA.” Cisa.gov, 2015. https://www.cisa.gov/sites/default/files/publications/nipp-ssp-water-2015-508.pdf. (accessed October 2019)

U.S. Department of Homeland Security (DHS)—with the Transportation Security Administration and the United States Coast Guard as executive agents for DHS—and the U.S. Department of Transportation. “Transportation Systems Sector | CISA.” Cisa.gov, 2015. https://www.cisa.gov/sites/default/files/publications/nipp-ssp-transportation-systems-2015-508.pdf. (accessed October 2019)

Election Infrastructure Subsector. “Election Security.” Department of Homeland Security, March 27, 2018. https://www.dhs.gov/topic/election-security. (accessed October 2019)

Wikipedia contributors, "Voice over IP," Wikipedia, The Free Encyclopedia, https://en.wikipedia.org/w/index.php?title=Voice_over_IP&oldid=921717372 (accessed October 2019).

Wikipedia contributors, "Plain old telephone service," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=Plain_old_telephone_service&oldid=920489716 (accessed October 2019).

Wikipedia contributors, "Satellite phone," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=Satellite_phone&oldid=918760438 (accessed October 2019).

Wikipedia contributors, "Professional mobile radio," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=Professional_mobile_radio&oldid=899043563 (accessed October 2019).

Wikipedia contributors, "Radio over IP," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=Radio_over_IP&oldid=918341989 (accessed October 2019).

DotGov Program. “Domain Requirements | DotGov.” Dotgov.gov, 2018. https://home.dotgov.gov/registration/requirements/. (accessed October 2019)

Parker, Melly. "Differences Between Personal and Corporate-Based Email" accessed October 2019. http://smallbusiness.chron.com/differences-between-personal-corporatebased-email-60187.html

Wikipedia contributors, "Local area network," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=Local_area_network&oldid=919579589 (accessed October 2019).

Wikipedia contributors, "Wireless LAN," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=Wireless_LAN&oldid=919969383 (accessed October 2019).

Wikipedia contributors, "Internet service provider," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=Internet_service_provider&oldid=920723956 (accessed October 2019).

Margaret Rouse and Ivy Wigmore, “mobile hotspot”, *WHatIs.com,* https://whatis.techtarget.com/definition/mobile-hotspot (accessed October 2019)

Wikipedia contributors, "Intranet," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=Intranet&oldid=919727563 (accessed October 2019).

Wikipedia contributors, "Website," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=Website&oldid=921401825 (accessed October 2019).

Wikipedia contributors, "Extranet," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=Extranet&oldid=911699334 (accessed October 2019).

Department of Homeland Security. “Safeguarding Sensitive but Unclassified (For Official Use Only).” Management Directive System. Department of Homeland Security, November 5, 2004. https://fas.org/sgp/othergov/dhs-sbu.html. (accessed October 2019)

U.S. Government Accountability Office, “Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information,” *Gao.Gov*, no. GAO-06-385 (2009), https://www.gao.gov/products/GAO-06-385. (accessed October 2019)

GovRegs, “6 CFR 29.8 - Disclosure of Protected Critical Infrastructure Information.,” Govregs.com, 2019, https://www.govregs.com/regulations/expand/title6_chapterI_part29_section29.8. (accessed October 2019)

Wikipedia Contributors, “Vital Record,” Wikipedia (Wikimedia Foundation, July 13, 2019), https://en.wikipedia.org/wiki/Vital_record. (accessed October 2019)

HIPAA Journal, “What Is Protected Health Information?,” HIPAA Journal, January 10, 2018, https://www.hipaajournal.com/what-is-protected-health-information/. (accessed October 2019)

Black's Law Dictionary, "What Is COURT RECORD? Definition of COURT RECORD (Black's Law Dictionary)," The Law Dictionary (The Law Dictionary, March 28, 2013), https://thelawdictionary.org/court-record/. (accessed October 2019)

Connor Reporting, "Court Records and Proceedings: What Is Public and Why? - Connor Reporting," Connor Reporting, April 18, 2017, https://connorreporting.com/court-records-proceedings-public/. (accessed October 2019)

*A Law Dictionary, Adapted to the Constitution and Laws of the United States. By John Bouvier.*. S.v. "contract." Retrieved October 2019 from https://legal-dictionary.thefreedictionary.com/contract. (accessed October 2019)

"Different Types of Contracts: Everything You Need to Know," UpCounsel, 2019, https://www.upcounsel.com/different-types-of-contracts. (accessed October 2019)

Payment Card Industry Security Standards Council, "Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards," Pcisecuritystandards.org, May 2018, https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf. (accessed October 2019)

Federal Trade Commission (FTC). "Identity Theft Recovery Steps | IdentityTheft.Gov." Identitytheft.gov. IdentityTheft.gov, 2019. https://www.identitytheft.gov/Info-Lost-or-Stolen. (accessed October 2019)

Orszag, Peter. "Executive Office of The President Office of Management And Budget M-10-23 Memorandum For The Heads Of Executive Departments And Agencies From." *Privacy Laws, Policies and Guidance*. Office of Management and Budget, June 25, 2010. http://www.osec.doc.gov/opog/privacy/Memorandums/OMB_M-10-23.pdf. (accessed October 2019)

Wikipedia contributors, "Data center," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=Data_center&oldid=920876767 (accessed October 2019).

Wen, Howard. "Cloud vs. Data Center: What to Consider." Business News Daily, December 27, 2018. https://www.businessnewsdaily.com/4982-cloud-vs-data-center.html. (accessed October 2019)

Techopedia. "What Is a Managed Data Center? - Definition from Techopedia." Techopedia.com, October 2019. https://www.techopedia.com/definition/30134/managed-data-center. (accessed October 2019)

Techopedia. “What Is Network Infrastructure? - Definition from Techopedia.” Techopedia.com, October 2019. https://www.techopedia.com/definition/16955/network-infrastructure. (accessed October 2019)

Wikipedia contributors, "Server (computing)," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=Server_(computing)&oldid=918793041 (accessed October 2019).

Wikipedia contributors, "Desktop computer," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=Desktop_computer&oldid=920206934 (accessed October 2019).

Wikipedia contributors, "Laptop," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=Laptop&oldid=921740639 (accessed October 2019).

Wikipedia contributors, "Tablet computer," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=Tablet_computer&oldid=920705015 (accessed October 2019).

Wikipedia contributors, "File server," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=File_server&oldid=920749909 (accessed October 2019).

WhatIs.com. “What Is Hard-Drive Encryption? Definition from WhatIs.Com.” Search Enterprise Desktop, 2019. https://searchenterprisedesktop.techtarget.com/definition/hard-drive-encryption. (accessed October 2019)

Wikipedia contributors, "Printer (computing)," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=Printer_(computing)&oldid=921263048 (accessed October 2019).

Techopedia, “What Is a Scanner? - Definition from Techopedia,” Techopedia.com, October 2019, https://www.techopedia.com/definition/30441/scanner. (accessed October 2019)

Wikipedia contributors, "Image scanner," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=Image_scanner&oldid=921115371 (accessed October 2019).

Wilson, Sarah, Sonia Lelii, and Margaret Rouse. “What Is USB Flash Drive? - Definition from WhatIs.Com.” SearchStorage, October 2019. https://searchstorage.techtarget.com/definition/USB-drive. (accessed October 2019)

WhatIs.com. “What Is External Hard Drive? - Definition from WhatIs.Com.” WhatIs.com. WhatIs.com, October 2019. https://whatis.techtarget.com/definition/external-hard-drive. (accessed October 2019)

Wikipedia contributors, "CD-ROM," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=CD-ROM&oldid=921638376 (accessed October 2019).

Wikipedia contributors, "Mobile phone," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=Mobile_phone&oldid=921882355 (accessed October 2019).

# Indiana Cyber Emergency Resiliency Response State Guide

# CYBER EMERGENCY RESILIENCE AND RESPONSE STATE GUIDE

# CYBER EMERGENCY RESILIENCY AND RESPONSE STATE GUIDE

## Table of Contents

1.0 Introduction .......... 3

2.0 Purpose .......... 3

3.0 Scope .......... 3

4.0 Cyber Emergency Preparation and Response Plan Core Group .......... 4

5.0 Cyber Emergency Preparation Process .......... 7

6.0 Response Process .......... 8

7.0 Plan Maintenance .......... 9

## 1.0 Introduction and Definitions

The Indiana Cyber Emergency Resiliency and Response State Guide (State Guide) was created to communicate the roles of an effective emergency response to a cyber emergency from the Executive Branch of Indiana government and indicate what roles partners may have during a cyberattack.

Determining which organizations should be involved and the roles they will play has proven challenging at all levels of government for nontraditional catastrophic emergencies such as a cyber attack. Emergency managers often have a difficult time understanding the technical nature of a cyber attack and how that fits in an emergency response while still developing decision-making processes that are true to an all-hazards approach. Below are emergency management resources to assist in planning and responding to a cyber attack.

### Cyber Emergency VS Cyber Incident

The State of Indiana defines a **cyber emergency** as any actual, imminent, or potential incident that will adversely affect public health, safety, or security; the environment; or economic prosperity on a level materially significant to the State of Indiana or its operations that requires a coordinated state response.

The State of Indiana defines a **cyber incident** as it is described in the Presidential Policy Directive 41, which is "an event occurring on or conducted through a computer network that actually or imminently jeopardizes the confidentiality, integrity, or availability of computers, information or communications systems or networks, physical, or virtual infrastructure controlled by computers or information systems, or information resident thereon."

## 2.0 Purpose

The State Guide the roles, considerations, and process to effectively coordinate the proper resources to proactively protect and defend state-owned data systems and networks during a cyber emergency. This will also provide clarification to the state's role in assisting local units of government in a cyber-related incident as well as coordinating with private sector partners.

## 3.0 Scope

The State Guide will be utilized when the following criteria are met:

- A cyber emergency involving activation of state level continuity of operations (COOP), or continuity of government (COG) plans.
- A cyber event that has a material impact on public safety.
- A threat or incident involving state-level, cyber-critical infrastructure.
- When requested by:
  - A local government entity
  - Director of the Indiana Office of Technology
  - Director of the Department of Homeland Security
  - The Adjutant General of Indiana

- When directed by:
    - The Governor of Indiana

## 4.0 Cyber Emergency Resiliency and Response Partners

The State of Indiana relies on a core group of agencies to assess the circumstances, determine an emergency, and deliver the response needed from state government. Inclusion in the core group is driven by the essential expertise and capabilities needed from the Executive Branch to assess and potentially assist in a response to the cyber emergency situation. As with many other threats and hazards, the success of resiliency and response must rely on the state, federal, public, military, and private partners.

### STATE AGENCIES AND PARTNERS

#### OFFICE OF THE GOVERNOR

The Governor provides overall direction and control for the preparation and carrying out of all emergency actions, including development and execution of the State's Comprehensive Emergency Management Plan. State agencies will support emergency operations in accordance with Executive Order 17-02.

#### INDIANA DEPARTMENT OF HOMELAND SECURITY

IDHS is tasked to coordinate the state's emergency plans, and serve as the coordinating agency for state efforts for preparedness for, response to, mitigation of, and recovery from emergencies and disasters. As with other hazard-related emergencies, IDHS manages the operations of the State Emergency Operations Center.

#### INDIANA OFFICE OF TECHNOLOGY

IOT oversees and manages the IN-ISAC. IOT is responsible for the security of state government information networks and all domains and is responsible for protecting the State's IT infrastructure from internal and external cybersecurity threats. IOT will assist IDHS during an cyber emergency activation with situational awareness, identifying external decision-makers, and accessing the necessary mitigation resources and lead remediation efforts if the event affected state government infrastructure.

#### INDIANA STATE POLICE

The ISP Office of Intelligence and Investigative Technologies (OIIT) focuses on cybersecurity incidents with a criminal nexus. The Cybersecurity Crime and Investigative Technologies Section and the Crime Analysis Section conduct activities related to cybersecurity forensics, cybersecurity crime investigations including those involving network intrusion and exploitation, electronic surveillance, and crimes against children.

The Indiana Intelligence Fusion Center (IIFC) collaborates with the IN-ISAC to conduct criminal intelligence analysis and incident reporting involving cybersecurity crimes. In the event that a criminal nexus is suspected in a cybersecurity emergency, law enforcement will investigate. Post-recovery, the IIFC may work with the IN-ISAC to help generate analytical after-action reports for external partners.

### INDIANA NATIONAL GUARD

The INNG has a Cybersecurity Mission comprised of experts in both preparedness and response efforts. As with other state emergencies, IDHS Executive Director may request deployment of cybersecurity force packages to support incident response.

### INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY

Signed by Governor Eric. J Holcomb on January 9, 2017, the Indiana Executive Council on Cybersecurity (IECC or Council) was continued through Executive Order 17-11 with the recognition that a cross-sector body of subject-matter experts is required to form an understanding of Indiana's cyber risk profile, identify priorities, establish a strategic framework of Indiana's cybersecurity initiatives, and leverage the body of talent to stay on the forefront of the cyber risk environment.

Led by the Indiana Department of Homeland Security, Indiana Office of Technology, Indiana State Police, and the Indiana National Guard, the Council is made up of government (local, state, and federal), private-sector, military, research, and academic stakeholders to collaboratively move Indiana's cybersecurity to the Next Level. With 35 Council members and more than 250 advisory members, the Council delivered a comprehensive strategy plan to Governor Holcomb September 2018.

Moreover, the experts of the Council are charged with providing best practices, resources, and information to increase the state resiliency against cyberattacks. In addition to the private and public partners, state agencies and elected officials such as the Indiana Economic Development Corporation, Indiana Secretary of State, Indiana Attorney General, and many more have come together to increase the resiliency.

In a cyber emergency, experts from the Council may be included as a part of the Cybersecurity Advisory Group.

### CYBERSECURITY ADVISORY GROUP

The Indiana Cybersecurity Advisory Group (CAG) provides operational guidance and subject-matter expertise in support of a coordinated state cybersecurity incident response. The CAG will assess the incident and organize the strategic response to give to IDHS's Emergency Operations Center. The CAG also develops, coordinates and recommends courses of action and response strategies. Designated agency representatives include the IOT Chief Information

Security Officer, or designee, ISP Commander, Intelligence and Investigative Technologies or designee, INNG Defensive Cybersecurity Programs Lead, or designee, Indiana Cybersecurity Program Director, IDHS Division Director, Response and Recovery, or designee and selected subject-matter experts.

## FEDERAL AGENCIES

### U.S. DEPARTMENT OF HOMELAND SECURITY

The Department of Homeland Security (DHS) is the designated lead agency during a cybersecurity incident requiring a federal response. Their primary functions are to identify the source of disruption and help remove it, determine how they gained access, assess the damage, and provide guidance to the organization on how to make their system more secure.

### FEDERAL BUREAU OF INVESTIGATIONS

The FBI is the lead federal agency for investigating cybersecurity-attacks by criminals, overseas adversaries, and terrorists. Specially trained FBI agents and analysts based at the FBI Indianapolis Field Office investigate computer intrusions, theft of intellectual property and personal information, child pornography and exploitation, and online fraud.

### U.S. SECRET SERVICE

The Secret Service maintains Electronic Crimes Task Forces, which focus on identifying and locating international cybersecurity criminals connected to cybersecurity intrusions, bank fraud, data breaches, and other computer-related crimes. The Secret Service also runs the National Computer Forensic Institute, which provides law enforcement officers, prosecutors, and judges with cybersecurity training and information to combat cybersecurity crime.

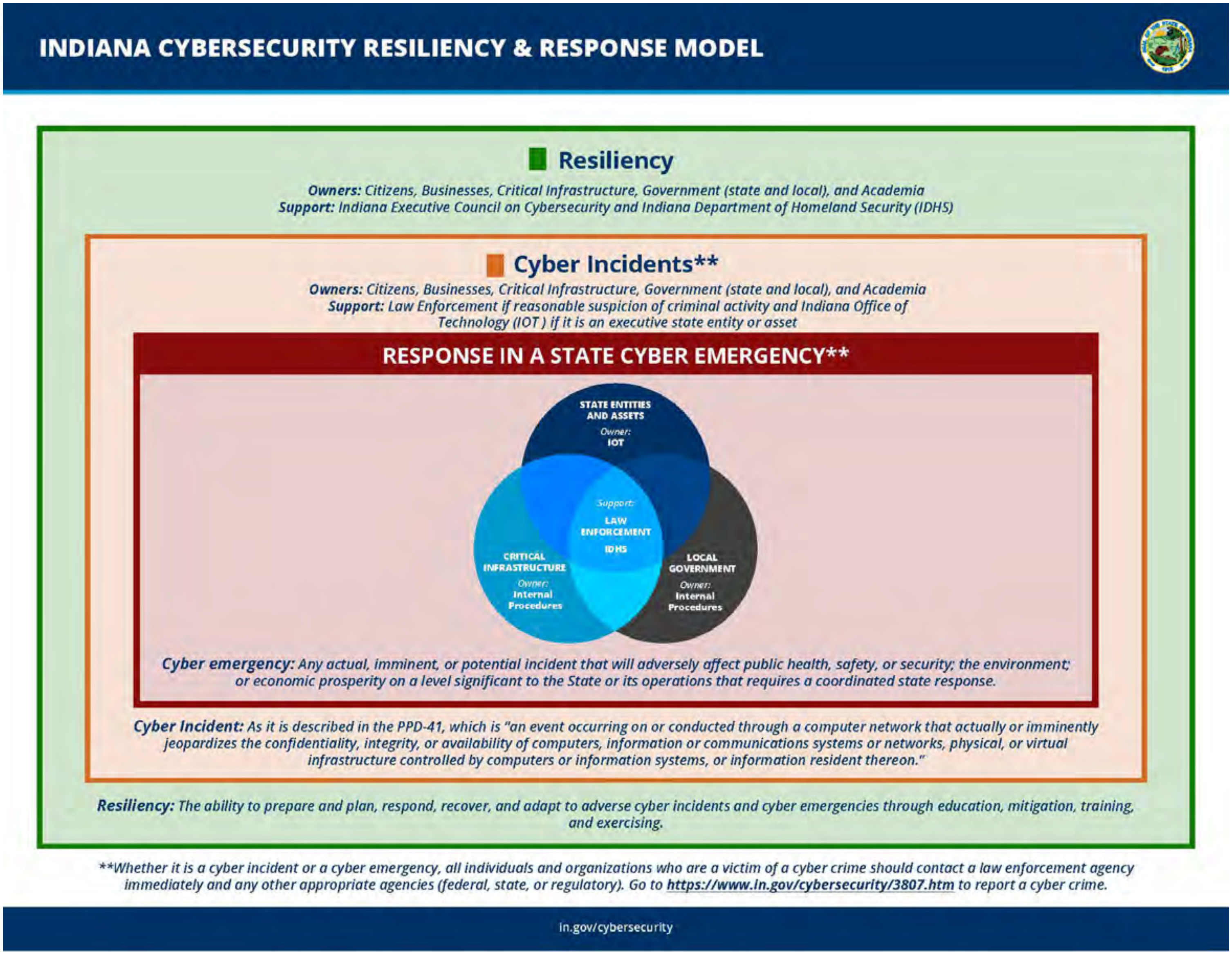
### U.S. DEPARTMENT OF JUSTICE

DOJ’s Offices of U.S. Attorneys and its’ Criminal and National Security Divisions, working with federal law enforcement agencies, use criminal and national security authorities to investigate, prosecute, and disrupt cyber threats and to apprehend cyber threat actors. Information and evidence obtained pursuant to appropriate legal process are used to identify the source of cyber incidents and to gather pertinent cyber threat information.

## 5.0 Cyber Emergency Resiliency Efforts

The State of Indiana core agency group include the Indiana Department of Homeland Security, Indiana Office of Technology, Indiana National Guard, and Indiana State Police.

This core agency group assists and leads in the overseeing of the cybersecurity resiliency efforts of the Indiana Executive Council on Cybersecurity and the ability for the state to be prepared to enable the rapid and effective response needed by state government constituents during a cyber emergency or cyber incident as appropriate. The following Indiana Cybersecurity Resiliency and Response Model further identifies the owners and support organizations during the resiliency phase, a cyber incident, and a cyber emergency.



**INDIANA CYBERSECURITY RESILIENCY & RESPONSE MODEL**

🟩 **Resiliency**

***Owners:*** *Citizens, Businesses, Critical Infrastructure, Government (state and local), and Academia*
***Support:*** *Indiana Executive Council on Cybersecurity and Indiana Department of Homeland Security (IDHS)*

🟧 **Cyber Incidents****

***Owners:*** *Citizens, Businesses, Critical Infrastructure, Government (state and local), and Academia*
***Support:*** *Law Enforcement if reasonable suspicion of criminal activity and Indiana Office of Technology (IOT ) if it is an executive state entity or asset*

**RESPONSE IN A STATE CYBER EMERGENCY****

***Cyber emergency:*** *Any actual, imminent, or potential incident that will adversely affect public health, safety, or security; the environment; or economic prosperity on a level significant to the State or its operations that requires a coordinated state response.*

***Cyber Incident:*** *As it is described in the PPD-41, which is "an event occurring on or conducted through a computer network that actually or imminently jeopardizes the confidentiality, integrity, or availability of computers, information or communications systems or networks, physical, or virtual infrastructure controlled by computers or information systems, or information resident thereon."*

***Resiliency:*** *The ability to prepare and plan, respond, recover, and adapt to adverse cyber incidents and cyber emergencies through education, mitigation, training, and exercising.*

***Whether it is a cyber incident or a cyber emergency, all individuals and organizations who are a victim of a cyber crime should contact a law enforcement agency immediately and any other appropriate agencies (federal, state, or regulatory). Go to* ***https://www.in.gov/cybersecurity/3807.htm*** *to report a cyber crime.*

in.gov/cybersecurity

## 6.0 Response Process

### Report a Cyber Crime

When an organization's experiencing a cyber attack, the following these steps should be taken.

Step 1: Contact Law Enforcement

- FBI Internet Crime Complaint Center (IC3)
- Indiana State Police (ISP) Cybercrime and Investigative Technologies
- If there is an immediate threat to public health or safety, call 911.

Step 2: Additional Reporting

In addition to reporting the cyber attack, an organization should consider contacting other agencies to report the attack, which include:

- **Indiana Attorney General** requires organizations report any security breach resulted in exposure of personal information. For more information, click here.
- **Regulators:** Regulated organizations may need to report cyber crimes to other state or federal agencies.
- **Secretary of State:** If necessary, contact the SOS offices regarding any related cyber incidents at electionsecurity@sos.in.gov
- **Federal Government:** This fact sheet explains how to report cyber crimes to many federal agencies.
- **Indiana Department of Homeland Security** at WatchDesk@dhs.IN.gov.

Step 3: Utilize additional resources

For additional tips regarding avoiding ransomware and information from the National Governors Association Response Planning Memo, National Emergency Readiness Team information, Department of Homeland Security's National Cybersecurity and Communications Integration Center, and more visit www.in.gov/cybersecurity/3807.htm.

Step 4: Information Sharing

It's important to share cyber crime information with other organizations to protect critical infrastructure, the State of Indiana, and our nation. Learn more at www.in.gov/cybersecurity/3819.htm.

It is important to note that once the State of Indiana is notified, the following process was created with a single objective: Get the emergency into the hands of capable, representative, and empowered individuals to bring Indiana government resources and relationships quickly to the aid of those suffering from a cyber emergency.

Once a request for assistance is received by one or more state agencies, the core agency group will convene and assess the traits and impacts of the cyber incident or emergency and the value of their resources as they apply to an effective response to the emergency, whether it is with state resources or working with other key public and private partners. Cyberattacks shared with the State of Indiana will stay at the highest level of leadership and only shared with need-to-know parties. After each cyber event reported to one or more of the core agency group, a post-emergency evaluation will be completed by the state’s Cybersecurity Program Director to rate response effectiveness, identify additional needs, and process adjustments.

## 7.0 Plan Maintenance

The State of Indiana Department of Homeland Security Executive Director, Indiana Office of Technology Chief Information Officer (CIO), and Indiana Cybersecurity Program Director are responsible for overall administration and maintenance of this State Guide.

# Integrated Preparedness Information Handout

# INTEGRATED PREPAREDNESS CYCLE

The Integrated Preparedness Cycle of planning, organizing/equipping, training, exercising (POETE), and evaluating/improving is a continuous process that ensures the regular examination of ever-changing threats, hazards, and risks, as shown in Figure 2.1.

The Cycle involves the assessment of threats, hazards, and risks; new and updated plans; and improvements implemented from previously identified shortfalls or gaps.

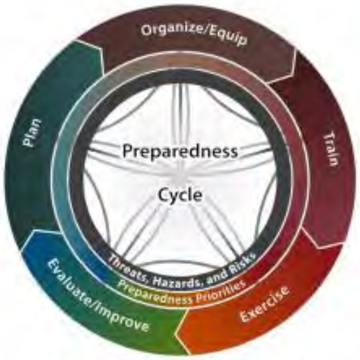


Figure 2.1: The Integrated Preparedness Cycle

Effective program management is comprised of the following components: •Engaging senior leaders; •Establishing multi-year preparedness priorities; •Conducting an Integrated Preparedness Planning Workshop (IPPW); •Developing a multi-year Integrated Preparedness Plan (IPP) and Integrated Preparedness Schedule (IPS); •Maintaining program reporting of exercise outcomes; and •Managing exercise program resources.

# INTEGRATED PREPAREDNESS PLANNING WORKSHOP (IPPW)

## PURPOSE

Use guidance provided by senior leaders to identify and set preparedness priorities and develop a multi-year schedule of preparedness activities.

The process confirms: •Coordination of whole community initiatives; •Prevention of duplication of efforts; •Assurance of the efficient use of resources and funding; and •Avoidance of overextending key agencies and personnel.

During the IPPW, participation from the whole community ensures preparedness activities are included in the program's priorities.

CONTACT INFORMATION •Exercise@dhs.IN.gov•

## WORKS CITED

Homeland Security. "Homeland Security Exercise and Evaluation Program (HSEEP) January 2020." www.fema.gov/sites/default/files/2020-04/Homeland-Security-Exercise-and-Evaluation-Program-Doctrine-2020-Revision-2-2-25.pdf.