# STATE OF OHIO
# EMERGENCY OPERATIONS PLAN

# EMERGENCY SUPPORT FUNCTION #2
# COMMUNICATIONS AND INFORMATION TECHNOLOGY

# TAB B – CYBER INCIDENT RESPONSE PLAN

**FACILITATING AGENCY**

Ohio Department of Administrative Services –
Office of Information Technology

# OHIO EMERGENCY OPERATIONS PLAN
# EMERGENCY SUPPORT FUNCTION # 2

## COMMUNICATIONS AND INFORMATION TECHNOLOGY

## TAB B - CYBER INCIDENT RESPONSE PLAN

**FACILITATING AGENCY:** Ohio Department of Administrative Services – Office of Information Technology (DAS/OIT)

**SUPPORT AGENCIES:**
Ohio Emergency Management Agency (Ohio EMA)
Ohio State Highway Patrol (OSHP)
Ohio Homeland Security (OHS)
Adjutant General's Department, Ohio National Guard (OHNG)
Secretary of State’s Office (SOS)

## A. PURPOSE

1. The purpose of this plan is to identify organizations involved during a mass cyber incident, and to identify their roles and responsibilities.

2. This document describes when and how the Cyber Incident Response Plan will be activated.

3. This plan facilitates efficient threat identification, purposeful information exchange, and coordinated cyber incident response.

## B. DEFINITIONS

1. Security Event – An imminent threat to, or the attempted compromise of the Confidentiality, Integrity or Availability of a computer system.

2. Security Incident – A compromise of the Confidentiality, Integrity or Availability of a computer system.

3. Mass Security Incident – A security incident that results in broad significant impact to an entity within the territory of the State of Ohio.

4. Functional Impact – A measure of the actual, ongoing impact to the organization. In many cases (e.g., scans and probes or a successfully defended attack), little or no impact may be experienced due to the incident.

5. Information Impact – The type of information lost, compromised, or corrupted.

6. Potential Impact – The overall statewide impact resulting from a total loss of service from the impacted entity.

7. Significant Impact – The substantial and widespread degradation of Information Technology services.

8. Cyber Work Group – Any combination of members of Tab B to ESF-2.

## C. SITUATION

1. Cyber-related incidents are capable of causing extensive damage to critical infrastructure and key assets. Voluntary sharing of incident information between state and local agencies, law enforcement and the federal government will be important to ensuring a safe and secure cyberspace.

2. Senate Bill 52-Defined Operations

    a. Establishes Ohio Cyber Reserve Corps

    b. During activation of this Corps, non-traditional guardsmen (not in uniform) will deploy with traditional guardsmen.

## D. ASSUMPTIONS

1. Cyber incidents will have cascading effects (i.e. power outage, dam failure, transportation accident, etc.).

2. A cyber-related incident will follow as a secondary impact to a non-cyber incident.

3. During a multiple-incident response, all responding agencies will adhere to their normal communication procedures.

4. Each responding agency will follow their normal response plans for response to cascading impacts.

5. Multiple agencies will become aware of a cyber incident simultaneously through their daily-operations communications channels.

6. Cyber insurance coverage held by an impacted entity will impact response activities.

## E. CONCEPT OF OPERATIONS

1. Cyber System Failure/Incident Response

   a. Governmental jurisdictions, corporations, educational institutions, utilities, chemical companies, transportation systems, dams, and other critical infrastructure points in Ohio could all be vulnerable to damages and/or system failures due to a cyber incident.

   b. The support agencies to this plan have varying levels of capabilities and capacities to detect and respond to attacks/failures to computer-based systems that:

      i. Create, store, and transmit data and information.
      ii. Control the operations of critical infrastructure, including power generation, and water purification and delivery.
      iii. Control and/or manage dams, transportation and traffic control systems, emergency responder dispatch, etc.

   c. When there is a request for state assistance, DAS must approve the activation of this plan – Cyber Incident Response Plan – prior to the involvement of the DAS Office of Information Security and Privacy (OISP).

   d. State EOC-based response to an incident caused by an attack/failure to an entity's computer system will be similar to a non-cyber-based incident response. Depending on the nature of an impacted entity, a cyber-generated State EOC-based response could be to a transportation system incident, a communication system incident, a dam failure incident, a hazmat incident, a power outage incident, etc.

   e. Additional State EOC-based facilitation and coordination activities in response to a cyber-system attack and/or failure could include facilitating communications between an impacted entity and the U.S. Computer Emergency Response Team (US-CERT), or another organization that could assist impacted entities in recovering from cyber-related impacts.

   f. US-CERT is charged with providing response support and defense against cyber-attacks to the Federal Civil Executive Branch, and with information sharing and collaboration with state and local governmental jurisdictions, industry, and international partners. US-CERT interacts with federal agencies, industry, the research community, state and local governments, and others to disseminate information and assistance.

   g. A cyber incident that impacts a State-level agency, infrastructure, or system will be managed through the State Incident Response Plan that is maintained by DAS.

   h. The Secretary of State's (SOS) Office may take the role of the lead agency during a cyber incident that impacts elections.

i. The Roles and Responsibilities of lead and support agencies may vary depending on the level of an impacted entity (e.g. state vs. local).

2. Plan Activation Triggers

a. This plan will only be activated for mass cyber incidents which are defined in the Definitions section of this document (above), or for IT-related incidents that could pose a risk to the health, safety and welfare of the citizens of Ohio.

3. Security Concerns

a. Cyber Incident Response includes confidential information that will be safeguarded during incident response. System platforms for information sharing and common operating picture development will be used with respect to safeguarding information.

b. The Communication and Information Management System (CIMS) will be used for information sharing. Traffic Light Protocol (TLP) will be used when sharing incident information. The TLP is a set of designations used to ensure that sensitive information is only shared with appropriate audiences. (https://www.us-cert.gov/tlp)

c. The Cyber Work Group will maintain a contact list to identify authenticated individuals to be contacted for incident response.

4. Preparedness Objectives

a. To meet the following common objectives, the facilitating agency and support agencies will execute the following preparedness, assessment, response, and recovery activities:

i. Increase cyber risk awareness.
ii. Identify cyber information sharing mechanisms.
iii. Identify cyber incident escalation criteria and related notifications.
iv. Identify cyber incident management structures.
v. Validate and exercise cyber incident response roles and responsibilities.
vi. Review cyber resource request and management processes.
vii. Discuss public information roles and responsibilities for cyber incidents.

b. Preparation – On an annual basis, the facilitating agency and support agencies will review their preparedness and ability to execute this plan. Areas of focus of this review will include, but will not be limited to assessing their:

i. Contact lists and communication plans.
ii. Incident reporting mechanism.
iii. Exercise incident activation process.

c. Detection and Analysis – Facilitating agency and support agencies will be prepared to facilitate a response to a variety of cyber incident types. They will be prepared to collaborate with involved parties to detect possible attack vectors and to analyze available evidence.

d. Containment, Eradication, and Recovery – Facilitating agency and support agencies will be prepared to work with involved parties to develop and implement containment, eradication and recovery strategies, including recovery activities that are the responsibility of the impacted entity.

5. Post-Incident Activity – Facilitating agency and support agencies will facilitate a "lessons learned" activity with all involved parties to assess:

a. What happened, and at what times?

b. How well did the involved parties perform in dealing with the incident?

c. Were documented procedures followed?

d. Were documented procedures adequate?

e. What information was needed sooner?

f. Were any steps or actions taken that might have inhibited the recovery?

g. What could be done differently the next time a similar incident occurs?

h. How could information sharing with other organizations have been improved?

i. What corrective actions could be recommended to prevent similar incidents in the future?

j. What precursors or indicators could be watched for in the future to detect similar incidents?

k. What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

6. Request for State Assistance from a Local Entity.

   a. Requests for state assistance will be made from the County EMA to Ohio EMA. This will be done by a call into the Ohio EMA Watch Office. The requester will relay the following information:

      i. Incident Reporter's Name
      ii. Impacted Organization
      iii. Reporter and Impacted Agency's Contact Information
      iv. A standard incident reporting message could be: "I would like to report a cybersecurity incident and request activation of the Cyber Incident Response Plan – Tab B to ESF-2 of the Ohio Emergency Operations Plan"
      v. Incident-specific situational overview

   b. DAS/OIT will be made aware of the situation. Ohio EMA will support with coordination and contact to the impacted entity to determine the necessary level of response, and if activation of this plan is appropriate.

   c. If this plan is activated, Ohio EMA will coordinate a call with the appropriate state partners.

   d. The Ohio Department of Administrative Services - Office of Information Technology (DAS/OIT) will be the lead agency on the call unless it is an election related cyber issue, where the Secretary of State will be the lead. The call will be for government employees and will not be open to third parties.

7. Request for State Assistance from State Partner

   a. DAS will be the lead agency.

   b. If any of the ESF2 Tab B partners are made aware of an incident that could activate this plan, they will share information with Ohio EMA Watch Office or DAS directly. If DAS determines the need to activate the plan, this decision will be communicated to all partners.

## F. RELATIONSHIPS BETWEEN LEVELS OF GOVERNMENT

1. Federal

   a. The Federal Government has multiple cyber incident response resources available to the state of Ohio.

   b. These resources include, but are not limited to:

      i. US Department of Homeland Security – Cybersecurity and Infrastructure Security Agency (CISA)
      ii. U.S. Department of Defense
      iii. U.S. Computer Emergency Readiness Team (CERT)
      iv. Multi-State Information Sharing and Analysis Center (MS-ISAC)
      v. Federal Bureau of Investigation (FBI) (If requesting FBI resources, specifically ask for the FBI Cyber Supervisor)

2. State

   a. In accordance with the Ohio Revised Code 5502, the Ohio Emergency Management Agency is in charge of coordinating state-level emergency communications support between the agencies of state, federal and local government from activation of the EOC to recovery.

   b. In accordance with the Ohio Revised Code 125.18 the Ohio Department of Administrative Services is charged with establishing policies and procedures to protect personal information which is maintained by State agencies.

   c. In accordance with the Ohio revised Code 5502.03,  Ohio Homeland Security is charged with intelligence and information sharing to support local, state, and federal law enforcement, other government agencies, and private organizations to enhance security and protection of critical infrastructure and key assets in Ohio.

3. Local

   a. Support Agencies to this plan will coordinate and facilitate cyber-related emergency response activities with impacted areas' local EOCs.

The chart, below, shows the relationship between federal, state and local communications organizations.

**Comparison Chart - Organizations by Level of Government**

| **Local Organizations** | **State Organizations** | **Federal Organizations** |
|---|---|---|
| Local EMAs | Ohio EMA | Department of Homeland Security, Cybersecurity and Infrastructure Security Agency<br>Federal Communications Commission |
| Local Law Enforcement | Ohio State Highway Patrol | Federal Bureau of Investigation |
| * | Department of Administrative Services | * |
| * | Adjutant General's Department, Ohio National Guard | U.S. Department of Defense |
| Ohio Amateur Radio | * | * |
| * | Ohio Homeland Security | * |

* There is no comparable designated organization at this level of government.

## G. ORGANIZATION AND ASSIGNMENT OF RESPONSIBILITIES

Organization

1. The Ohio Department of Administrative Services Office of Information Technology is the facilitating agency for all non-election related events under Tab B to ESF-2.

2. All Support Agencies – Each agency listed in this section may have statutory authority or requirements outside the context of ESF-2 Tab B. Nothing in this section is to be construed as restricting them from performing these additional duties as required.

   a. Provide staff for State EOC activations.

b. Assist with planning strategies to meet preparedness, response, and recovery objectives.

c. Develop agency-specific resource manuals; inclusive of checklists, procedures, roles and responsibilities, and other job aids.

d. Report cyber-related incidents to the facilitating agency.

Assignment of Responsibilities

1. Ohio Department of Administrative Services – Office of Information Technology (DAS/OIT)

   a. Maintain communication with the ESF-2 Primary Agency (Ohio EMA) regarding overall planning, communication, and coordination.

   b. Provide staff for State Emergency Operations Center (State EOC) activations.

   c. Request and coordinate support agency assistance.

   d. Provide guidance to state/local/non-governmental organizations, and private sector stakeholders and partners. This includes guidance on PII that may be impacted by a cyber event.

   e. Develop and maintain a cyber-related resource manual, inclusive of key contacts for local and state law enforcement cyber incident reporting, checklists, procedures, roles and responsibilities, and other job aids.

   f. Develop reporting mechanisms/information flow charts to communicate cyber-related information to local and state agencies, cyber partners, plan contacts, stakeholders, and the private sector.

   g. Where applicable report cyber-related incidents to OSHP and OHS

2. Ohio Emergency Management Agency (Ohio EMA)

   a. Coordinate information flow between County EMA's and DAS/OIT, including other plan partner agencies.

   b. Assist in mitigating physical-world effects of cyber incidents.

   c. Provide information coordination for local partners to the Statewide Terrorism Analysis & Crime Center (STACC) / Strategic Analysis and Information Center (SAIC).

3. Ohio State Highway Patrol (OSHP)

    a. Serve as a liaison to law enforcement agencies at all levels.

    b. Provide law enforcement situational awareness regarding response from the OSHP Watch Desk Commander.

    c. Provide analytical support for the STACC/SAIC through Computer Crimes Unit, as requested.

    d. With assistance from the DAS/OIT, lead efforts to gather evidence, and advise local agencies regarding criminal prosecution.

    e. Assess and respond to information that comes in through the OHS suspicious activity reporting line (877-OHS-INTEL).

    f. Utilizing the *Law Enforcement Cyber Incident Reporting – A Unified Message for State, Local, Tribal, and Territorial Law Enforcement* document (https://www.fbi.gov/file-repository/law-enforcement-cyber-incident-reporting.pdf/view), coordinate the reporting of cyber-related incidents to federal law enforcement agencies with OHS.

4. Ohio Homeland Security (OHS)

    a. Provide information and support to DAS/OIT during a cyber response incident.

    b. Coordinate gathering information from divergent sources.

    c. Provide situational awareness regarding the incident, attackers, and second-order effects.

    d. Coordinate reporting of cyber-related incidents to federal law enforcement agencies with OSHP, utilizing the Law Enforcement Cyber Incident Reporting – A Unified Message for State, Local, Tribal, and Territorial Law Enforcement document at https://www.fbi.gov/file-repository/law-enforcement-cyber-incident-reporting.pdf/view.

    e. Distribute cyber incident response products.

5. Adjutant General's Department, Ohio National Guard (OHNG)

    a. Provide cyber incident response services, as directed (through proclamation) by the Governor.

b. Provide on-site assistance to critical infrastructure providers, as directed by the Governor.

c. Provide supplemental incident response personnel to DAS/OIT to help manage the incident and relieve personnel/reduce staff fatigue, as directed by the Governor.

d. Provide on-site liaising services.

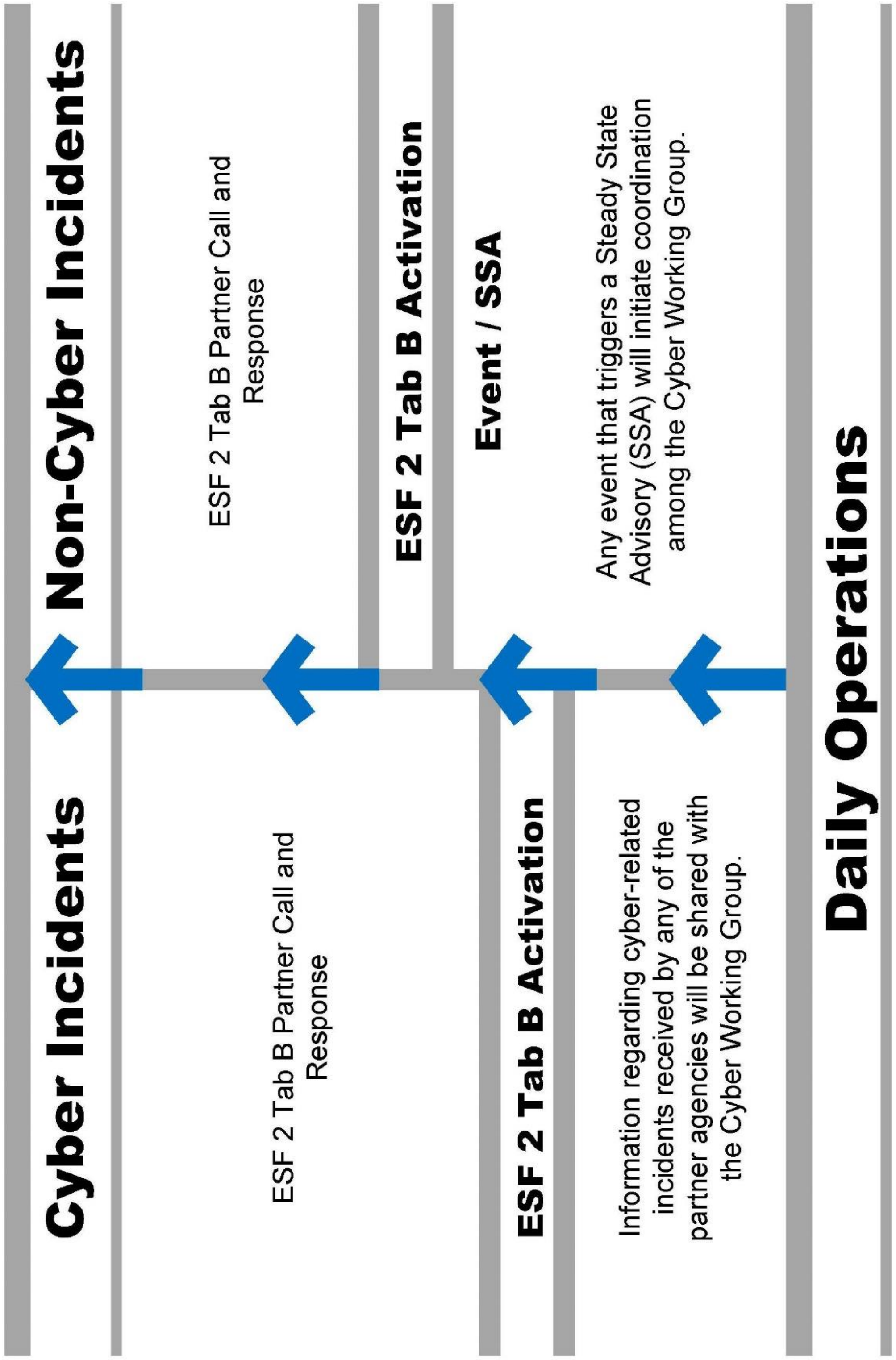
e. As required by an incident, and as directed by the Governor, provide the following services: cyber leadership/coordination, vulnerability assessments, NIST SCAP (National Institute of Standards and Technology Security Content Automation Protocol) scans, web site penetration testing/analysis, firewall compliance/analysis review, network mapping/analysis, and forensics.

6. Ohio Secretary of State (SOS)

   a. During an election-related incident, coordinate cyber response efforts.

   b. During an election-related incident, provide cyber incident response services.

## Attachment 1. COMMUNICATION FLOWCHART AND DECISION TREE



Cyber Incidents

Non-Cyber Incidents

ESF 2 Tab B Partner Call and Response

ESF 2 Tab B Partner Call and Response

ESF 2 Tab B Activation

ESF 2 Tab B Activation

Event / SSA

Information regarding cyber-related incidents received by any of the partner agencies will be shared with the Cyber Working Group.

Any event that triggers a Steady State Advisory (SSA) will initiate coordination among the Cyber Working Group.

Daily Operations