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 (DAS/OIT)

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)

I. INTRODUCTION

A. Cyber-related incidents are capable of causing extensive damage to critical infrastructure and key assets.

B. Voluntary sharing of incident information between state, local, tribal, and territorial (SLTT) law enforcement and the federal government is important to ensuring a safe and secure cyberspace.

C. The Ohio Department of Administrative Services – Office of Information Technology (DAS/OIT) must be immediately notified in the event of a cyber-related incident at 614.466.6930 or state.cio@das.ohio.gov.

II. SITUATION

A. Large scale cyber-related incidents will overwhelm the government and private sector, and disrupt the internet/critical information systems.

B. Critical systems include interlinked computer networks regulating power, water, financial services, medical care, public safety, telecommunication networks, and transportation systems.

C. Cascading effects of electronic infrastructure disruptions will threaten health/lives, property, the economy, and state/national security.

D. Rapid threat identification/investigation, systematized information exchange, and coordinated response/remediation are critical.

III. CONCEPT OF OPERATIONS

A. The facilitating agency and support agencies will execute preparedness, assessment, response, and recovery activities; in order to meet the following common cyber-hygienic objectives:

1. Increase cyber risk awareness.

2. Identify cyber intelligence and information sharing mechanisms.

3. Identify cyber incident escalation criteria and related notifications.

4. Identify cyber incident management structures.

5. Validate cyber incident response roles and responsibilities.

6. Review cyber resource request and management processes.

7. Discuss public information roles and responsibilities for cyber incidents.

B. Operational areas addressed during assessment, response, and recovery activities will include:

1. Planning, direction, control, communications, and coordination.

2. Resource/risk management, hazard mitigation, and mutual aid.

3. Information security and threat/vulnerability identification.

4. Continuity of Operations (COOP)/Continuity of Government (COG).

IV. ORGANIZATION AND ASSIGNMENT OF RESPONSIBILITY

A. Facilitating Agency

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 (SEOC) activations.

c. Request and manage support agency assistance.

d. Provide resources and guidance to state/local/non-governmental organizations (NGO's), and private sector stakeholders and partners.

e. Plan strategies to meet preparedness, response, and recovery objectives.

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

g. Develop reporting mechanisms/information flow charts to communicate cyber-related information to all state, local, tribal, and territorial agencies; cyber partners, tab contacts, stakeholders; and the private sector.

h. Report cyber-related incidents to federal law enforcement agencies, 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.

B. Support Agencies

1. 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.

2. All Support Agencies

a. Provide staff for SEOC 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.

3. Ohio Emergency Management Agency (Ohio EMA)

a. Coordinate information flow between County EMA's and DAS/OIT.

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

c. Provide information of interest from their local partners to OHS for intelligence coordination.

d. Provide logistical support and SEOC management.

4. Ohio State Highway Patrol (OSHP)

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

    b. Lead efforts to gather evidence, and advise local agencies regarding criminal prosecution, with assistance of DAS/OIT.

5. Ohio Homeland Security (OHS)

    a. Provide intelligence support to DAS/OIT during the incident.

    b. Coordinate tracking down information from divergent sources.

    c. Provide a clear picture of the incident, attackers, and second-order effects, in support of the response effort.

    d. Handle tips that come in through their suspicious activity reporting line.

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

    a. Provide cyber incident response, as directed by the governor, regardless of scope or customer type.

    b. Provide on-site assistance to critical infrastructure providers.

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

    d. Support OHS in the intelligence mission.