State of Michigan

CYBER DISRUPTION RESPONSE PLAN

October 2015

DTMB
Technology, Management & Budget

MICHIGAN STATE POLICE

DEPARTMENT OF MILITARY AND VETERANS AFFAIRS
MICHIGAN

State of Michigan
EXECUTIVE OFFICE
LANSING

RICK SNYDER
GOVERNOR

BRIAN CALLEY
LT. GOVERNOR

October 25, 2015

Dear Michigan Critical Infrastructure Partners:

Michigan government works diligently to block millions of unauthorized attempts to probe, scan, and access or disrupt its computer networks on a daily basis. These computer networks safeguard important information about Michigan's residents, control critical state agency operating systems, and provide customers with convenient access to state services. While the vast majority of these cyber anomalies are blocked by defensive systems, evolving threats represent a significant risk to the continuity of state government. Similar challenges are faced by Michigan's local government and private sector partners; organizations who also work diligently to safeguard their systems.

In 2011, Governor Rick Snyder introduced the Michigan Cyber Initiative to encourage a statewide effort among public and private partners to defend Michigan's critical networks. In support of this initiative, a team of state and local government representatives, alongside public safety and private sector critical infrastructure partners, developed the Michigan Cyber Disruption Response Strategy in 2013. To keep pace with the ever-evolving threats, we are proud to present the Michigan Cyber Disruption Response Plan.

The Plan provides guidelines to partner organizations to best protect Michigan's critical cyber infrastructure. The Plan includes strategies for information sharing, criminal investigation, cyber-attack response and recovery from a significant cyber-disruption to Michigan's critical infrastructure. Utilizing the Plan's strategies, participating organizations can collaborate in response to cyber threats as they are detected; often before the unthinkable happens.

It is our intent that by continuing to unify state government cyber security efforts, and working closely with our private sector and local government partners, we will continue Michigan's role as a national model of innovation, success and security.

David Behen
DTMB Director and
State Chief Information Officer

Colonel Kriste Kibbey Etue
Director, Michigan State Police

Major General Gregory J. Vadnais
Adjutant General, Michigan National Guard

State of Michigan

CYBER DISRUPTION RESPONSE PLAN

Prepared by:
Department of Technology Management & Budget

10/25/2015

Table of Contents

This page intentionally left blank.

1.0 Executive Summary

The Michigan Cyber Disruption Response Plan (CDRP) was created to protect the health, safety, and economic interests of Michigan's residents and businesses by reducing the impacts of disruptive cyber related events through response and mitigation planning, awareness, and implementation. Cyber disruption events have the ability to severely impact the social, economic and physical welfare of state citizens and businesses through escalated or multiple simultaneously executed attacks on the state's most critical sectors. The plan provides a framework that enables state emergency management and information technology to work seamlessly with public and private partners to rapidly respond to and minimize the impact of cyber disruption events in Michigan.

This plan provides a common framework for identifying and responding to technological threats, that mirror the federal government model, with corresponding responses to address threats of increasing scope and severity. These cyber disruption threats range from minor malware incidents; through specific attacks on targeted state networks and services; to severe attacks capable of catastrophic impact to services and facilities of single or multiple sectors providing critical support to citizens, government, public and private entities. The plan enables closely integrated planning by providing for critical infrastructure entities and partnership use. It leverages technical training for core team members, well-planned and executed exercises, and risk based metrics to identify, implement and track continuous improvement initiatives.

2.0 Introduction

The Michigan Cyber Disruption Response Plan (CDRP) provides the primary emergency management (EM) and information technology (IT) agencies in Michigan with a broad framework to coordinate response and recovery operations in the event of disruption to state government critical cyber infrastructure. Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience, signed June 2013, identified 16 critical infrastructure sectors:

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials and Waste
- Transportation Systems

- Water and Waste Water Systems

3.0 Purpose

The CDRP provides EM, IT, and other potential stakeholders, within Michigan, a management framework to coordinate preparedness, response, and recovery activities related to a large-scale or long-duration cyber disruption. It incorporates IT personnel into the Michigan-wide Incident Command System (MI-ICS) structure.

4.0 Scope

The CDRP uses a framework to coordinate intra-Michigan cyber preparedness, response, and recovery activities. The CDRP coordinates closely with local security policies and procedures. It provides an expanded description of the plans and activities the Michigan Department of Technology, Management and Budget (DTMB), the Michigan National Guard (MING) and Michigan State Police, Emergency Management and Homeland Security Division (MSP/EMHSD), will implement to prepare for, respond to, and recover from large-scale cyber disruptions. The CDRP defines the Michigan Cyber Disruption Response Team (CDRT) as the active coordinating structure for cyber disruption incidents.

Cyber disruptions may be a single yet pertinent element of a larger incident that threatens lives, property, and continued operation of critical business functions. Activities conducted pursuant to this CDRP work within state and local planning and incident command structures, complement existing plans and procedures, and are compliant with the National Incident Management System (NIMS).

5.0 Cyber Disruption Response Plan Roles and Responsibilities

The State of Michigan government works with federal, state, and local agencies and organizations; education; and private industry to respond to, resolve, and address secondary effects of cybersecurity disruptions, manmade disaster or natural disasters. The state promotes collaboration between the respective cyber disruption response functions and emergency management functions of these various entities. Given the integration of information technology with virtually any other discipline or line of business, these two functions will have to be engaged in almost any type of disruption or emergency. Specific roles and responsibilities for each entity are defined in Annex D: CDRP Roles and Responsibilities.

6.0 Michigan Cyber Disruption Response Team (CDRT)

The CDRT is comprised of subject matter experts responsible for preparation, response to, and recovery from large-scale or long-duration cyber disruptions impacting Michigan's critical infrastructure or other major assets. These disruptions could result from:

- Intentional threats (e.g., terrorism, internal or external)
- Accidental or unintended threats (e.g., disruption of power, shutdown of equipment, system patching without adequate testing)

- Process failures (e.g., institutionalized but untested processes)
- Natural phenomena (e.g., severe weather)

6.1 CDRT Membership and Organization

Department of Technology, Management and Budget (DTMB) and Michigan State Police (MSP) representatives will provide Cyber Disruption Response Team leadership. The Chief Security Officer (CSO) will be appointed Chairman and the Deputy State Director of Emergency Management and Homeland Security will serve as Vice Chairman. During State Emergency Operations Center (SEOC) activation, the Incident Commander directs CDRT operations.

6.1.1 CDRT Membership

The CDRT is composed of, at a minimum, representatives from the EM and IT communities from within Michigan. Other key federal, state, regional, local and private organizations, as necessary, may play a role in Michigan's CDRT or may be enjoined as necessary (and to the extent possible) to assist in the operations of a CDRT.

The Michigan CDRT consists of two primary groups; a core entity and an extended group. The core entity provides the leadership, day-to-day operational management and emergency operations directions. This group is composed primarily of DTMB, MSP and MING leadership and staff. The extended group supports key planning, operational and technological expertise and support for their specific cyber systems, operations and facilities. The Michigan Cyber Civilian Corps (MiC3), consisting of volunteers from government, education and business sectors; provides a rapid response capability to Governor declared state of emergency cyber events. When activated, the MiC3 supports both the CDRT core and extended groups.

Michigan's CDRT members should meet the following requirements:

- CDRT core membership consists of key representatives from the EM, IT, and law enforcement communities.
- Member organizations will provide the appropriate level of decision-making authority to their assigned CDRT primary and alternate members.
- The CDRT chairperson determines the extent of team involvement based on incident scope and nature. Extended group representatives may only be included for incidents deemed to be within their area of expertise or business operations.
- The chairperson represents the CDRT in coordination with the Incident/Unified Commander and/or Operations or Planning sections during an incident response.
- The CDRT will appoint a chairperson and a vice-chair to oversee CDRT activities and communications.

- Additional local, state, and federal agencies, along with healthcare, education, and private sector partner organization members, with critical cyber infrastructure knowledge and expertise, may be requested to participate in applicable CDRT operations.

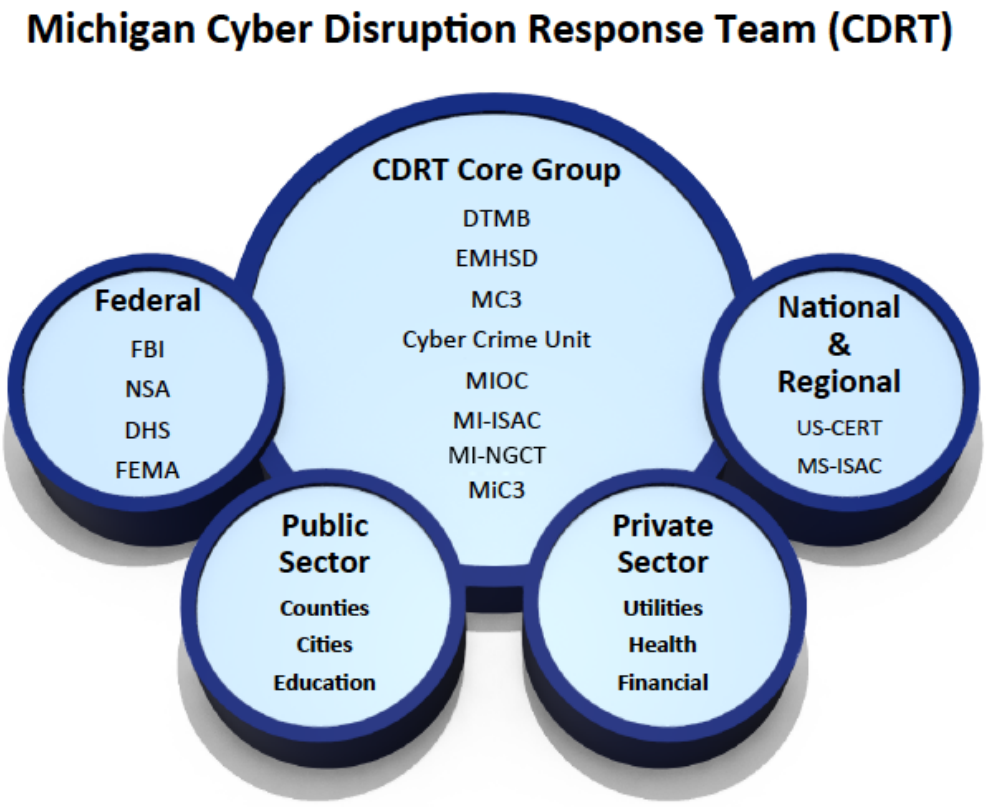

Figure 1: CDRT Membership

6.1.2 CDRT Organization

The CDRT internal structure follows Incident Command System (ICS) principles, with the Chair and Co-Chairs appointing a CDRT lead to act in the incident commander role. CDRT membership will fill Planning, Operations, Logistics, and Finance roles, as needed and as appointed by the CDRT lead.

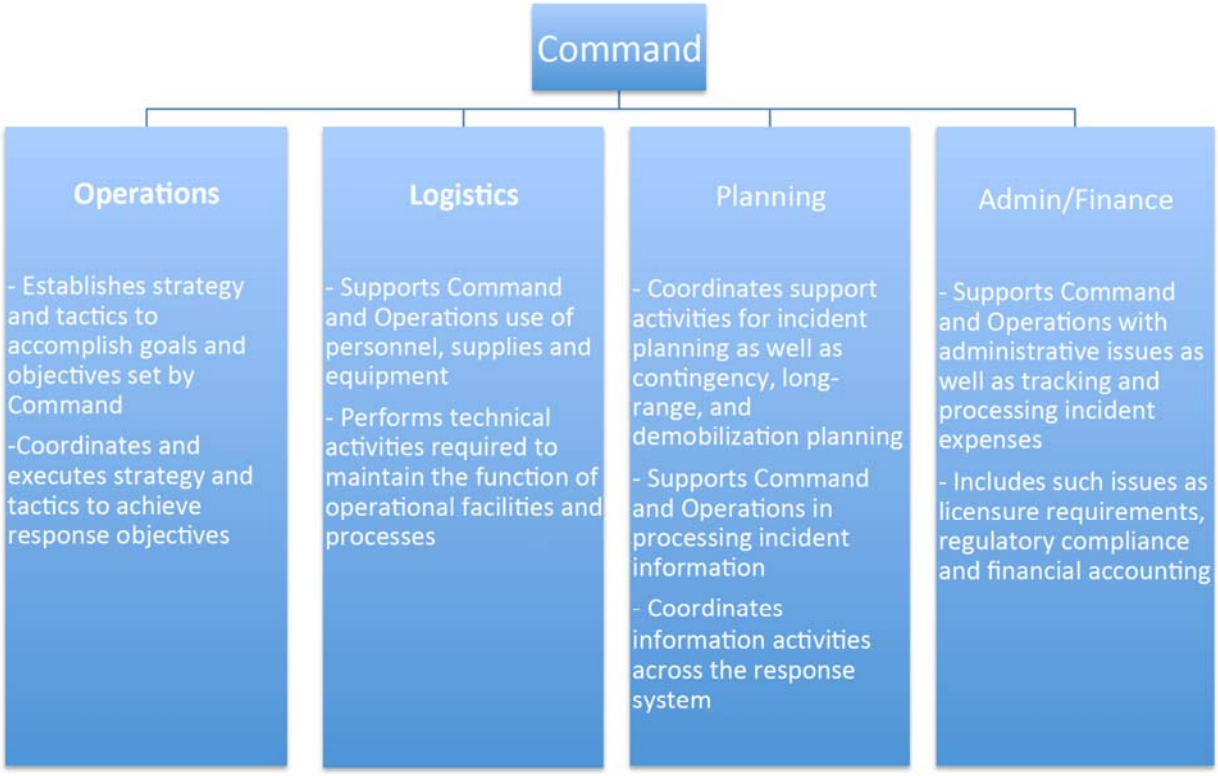

Image courtesy phe.gov

Figure 2: ICS Structure

As shown in Figure 3 on the following page, a CDRT may be established under the Planning or Operations Section. Under the Planning Section, it serves in a consultative role helping provide direction and expertise developing Incident Action Plan (IAP) objectives and related information. Under the Operations Section, the CDRT, or its members, may form a strike team or task force directing response/recovery actions or assisting in response/recovery actions in the field. The CDRT reports directly to the Incident/Unified Commander or other person responsible for directing response/recovery actions and providing specialized expertise to direct response efforts.

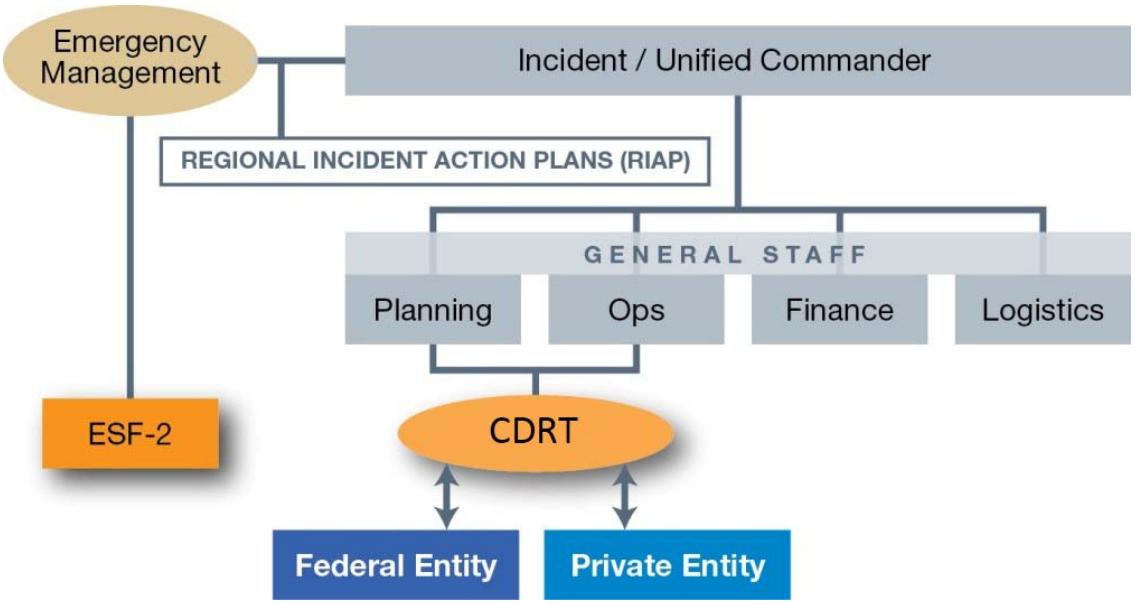

Figure 3: Organization Chart

6.2 Role of the CDRT

The CDRT is a specialized jurisdictional consultative group composed of representatives and subject matter experts from primarily the EM and IT domains. Representatives from other relevant domains are encouraged to participate. The CDRT serves the following roles in preparing for, responding to, and recovering from a cyber disruption:

- Helping executive management and Incident Command within the impacted systems and area understand the nature and potential duration of cyber disruptions.
- Helping EM staff determine the effects of cyber disruptions on critical life-safety systems, critical cyber assets, and other key response activities.
- Helping IT staff determine the potential resource needs of IT personnel and agencies to maintain, protect, and re-establish operations following a cyber disruption.

6.2.1 Preparation

The CDRT has a responsibility to be active in pre-event planning activities that increase the resilience of critical cyber assets across Michigan. The CDRT will:

- Identify threats and vulnerabilities to IT networks with respect to emergency management objectives and priorities.
- Identify mitigations (e.g., plans, procedures, hardening measures) for threats and vulnerabilities.
- Develop communications means and methodologies to enable intra- and extra-CDRT communication and transactions as prescribed in Annex A: Communication.

- Develop plans and procedures to address specific disruptions as described in Annex A: Response Plans.
- Train and exercise this CDRP, as well as other business continuity, continuity of operations, and continuity of government plans. Details on training and exercise program development and implementation are provided in Annex B: Training and Exercises.
- When necessary and possible, communicate with other CDRT representatives in the region to exchange best practices and information pertinent to preparing for cyber-related incidents.

6.2.2 Response

The core Cyber Disruption Response leadership team activates a virtual team of CDRTs as needed to support response activities. The CDRT incident response triage process seamlessly activates the SEOC during Severe and High Level incidents. The CDRT triage process is responsible for and manages the following activities:

- Monitor disruption events to determine scale and scope, and to determine if the event is stable, improving, or expanding.
- Share information within or between CDRTs that may indicate the development of a larger or more regional-level disruption event.
- Provide other CDRT representatives in the region with situational awareness and assistance during a catastrophic incident as necessary and possible.
- Help coordinate IT-related response activities pursuant to an Incident Action Plan (IAP)
- Coordinate with EM support staff to procure critical cyber-related resources.
- Provide situational awareness and subject matter expertise and solutions for an Incident/Unified Commander and his/her General Staff during a response, including:
    - Assisting Incident/Unified Commander's Operations Staff to understand technical and operational issues regarding cyber-related resources and networks.
    - Assisting Incident/Unified Commander's Planning Staff in the development of priorities and objectives of a long-term response to a large-scale cyber disruption incident. Developing objectives and activities become the key elements of an action plan for a determined operational period, set out by the Planning Chief and staff for the Incident/Unified Commander and contained in an IAP.

6.2.3 Recovery

CDRTs have a responsibility to be active throughout the recovery phase of an event, under the direction of the Deputy State Director of Emergency Management and

Homeland Security. It is possible that the recovery effort could exist over an extended period of time. CDRT responsibilities include:

- Working with affected system owners to determine resources needed to restore operations to a normal state.
- Tracking restoration efforts and providing information to the Incident/Unified Commander's Operations Staff regarding estimated and actual time to full restoration.
- Working with emergency management recovery leads over the extended life of the recovery effort.
- Communicating with Michigan National Guard Joint Operations Center (MING JOC); providing situational awareness and determining if MING resources can be of assistance.
- Conducting internal and external CDRT after-action reviews to obtain lessons learned following an incident.

6.3 CDRT Operation

The CDRT chairperson will be the primary decision-maker on behalf of the CDRT. The chairperson has the ability to appoint staff to provide support to a cyber disruption response effort, including staff responsible for Operations, Planning, Logistics, and Finance, according to ICS principles.

The CDRT chairperson and staff, as appropriate, will direct CDRT efforts by:

- Identifying and communicating the role of the CDRT within the larger response effort.
- Understanding and documenting the situation.
- Developing objectives, goals and mitigation strategies.
- Setting operational periods (OPs) to organize resources and measure effectiveness.
- Assigning staff to consultative, mitigation, or corrective response and recovery roles.
- Identifying and communicating potential health and safety hazards.
- Conducting other duties required to complete the response and recovery effort.

7.0 Plan Maintenance

The State of Michigan Chief Security Officer (CSO) and Department of Technology, Management and Budget (DTMB**)** are responsible for overall administration and maintenance of this plan and monitoring and reporting on its progress. This process includes periodic reviews as well as updates to incorporate changes achieved through the completion of planned initiatives and lessons learned from exercises and real-world situations.

8.0 Authorities and References

- Presidential Policy Directive-21: Critical Infrastructure Security and Resilience
- Department of Homeland Security National Infrastructure Protection Plan 2013 (NIPP): Partnering for Critical Infrastructure Security and Resilience
- Homeland Security Presidential Directive-5 (HSPD-5): Management of Domestic Incidents
- Homeland Security Presidential Directive-7 (HSPD-7): Critical Infrastructure Identification, Prioritization and Protection
- Homeland Security Exercise and Evaluation Program (HSEEP)
- NIST Special Publication 800-55 Revision 1, Security Measurement
- NIST Special Publication 800-61, Revision 2, Computer Security Incident Handling Guide

This page intentionally left blank

Annex A: Response Plans

A.1 Introduction

This annex provides a template for the development of cyber response plans for Michigan's critical infrastructure, and a framework for response to cyber disruptions. These efforts are based on the cyber incident response cycle, which describes the "fundamental elements of prevention and protection activities" associated with a cyber-response.

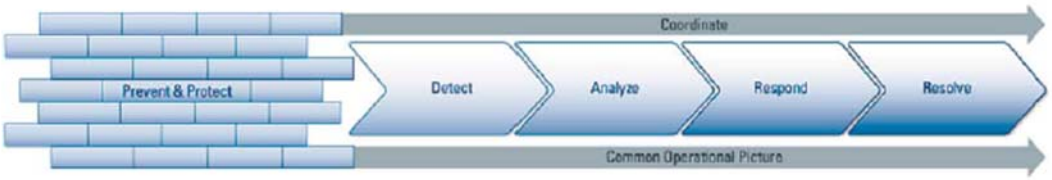

Figure A-1: Interim National Cyber Incident Response Plan Incident Response Cycle

A.2 Response Plan Template

A.2.1 Introduction

Incident response plans provides a set of instructions for critical infrastructure owner and operator cyber security incident response team execution in the event of a given security incident. Each response plan is effectively a Play Book used to prevent uncoordinated responses to potentially devastating security incidents.

A.2.2 Background

To ensure consistency of approach across all departments it is essential that they are use the same basic framework as outline in the proposed template. The benefit of this is that if a responder moves to a different team, there will be a very small learning curve to get up to full speed.

A2.3 Critical Systems Information

Critical systems, applications and services should be properly identified, included in the asset management system and recovery and restoration directions must be clearly defined. At a minimum, the following information should be maintained for each critical system:

- System Name
- Classification
- Location
- Owner
- Restoration Priority
- Configuration Information
    - Build

    - Patch
- Location of Backup
- Restoration Checklist
- Subject Matter Expert

A.2.4 Concept of Operations

Organizations should develop a Concept of Operation (ConOps), which is a user-oriented document that describes system characteristics for a proposed system from the users' viewpoint. The ConOps describes the user organization (mission(s) and organizational objectives from an integrated systems point of view. This section defines what the organizations Incident Response Plan is; how it affects the user; why it is vital and what users need to know/do.

a) Prevention and Protection

- Prevention
    - Incident Handler
        - Communications
        - Facility (e.g., In-House or Contract)
    - Incident Analysis Hardware & Software
    - Incident Analysis Resources
    - Incident Mitigation Software
- Protection
    - Risk Assessments
    - Host Security
    - Network Security
    - Malware Prevention
    - User Awareness & Training
    - Patch Management

b) Detection and Analysis

- Log Management and Alert Integration
- Security Event Triage Processing
- Security Event Validation
- Event Analysis and Possible Escalation to Security Incident

c) Response and Recovery

- Response Plan Activation
    - Security Event Escalation
    - Response Team Call-out Tree Activation
    - War Room Invocation
    - Extended Response Team Activation
- Response Activities
    - Communications Lockdown for Serious Events
    - Further Event Analysis and Response Selection from Response Play Book
    - Response Playbook Execution and Results Documentation

- Affected Systems Containment
- Known Threat Blockage
- Implementation of Additional Controls to Stop Threat
- Damage Identification
- Damage Eradication and Identification of Required Restoration

A.2.5 Specific Cyber Response Action Plans

a) Data Backup Action Plan

- Identification of Data to Be Backed Up
  - Network Servers
  - Desktop Computers
  - Laptop Computers
  - Wireless Devices
  - Network Devices
  - Security Devices
- Backup of Vital Hard Copy Records
- Backup Software & Hardware
- Backup Media
  - Location
  - Classification
- Storage
  - In-House
  - Cloud
- Restoration
  - Test/Validation

b) Disaster Recovery/Business Continuity Plan (DR/BCP)

This plan covers recovery strategies for Information Technology (IT) systems, applications and data, including networks, servers, desktops, laptops, wireless devices, data and connectivity. IT recovery priorities should be consistent with the priorities for recovery of business functions and processes developed during the Business Impact Assessment (BIA). IT resources required to support time-sensitive business functions and processes should also be identified. The recovery time for an IT resource should match the recovery time objective (RTO) for the business function or process that depends on the IT resource. The following are standalone plans referenced by the DR/BCP plan, which could place them as outlines in separate annexes:

c) Halt Key Processes Plan

- Identifies and documents key processes.
- Describes the order and any dependencies that affect how these processes should be safely and completely halted.

- Roles and responsibilities for achieving these shutdowns must also be documented.

d) Equipment Shutdown Plan

- Identifies and documents key items of equipment or plant that require specific and detailed shutdown processes.
- Describes the order and any dependencies that affect how these items of equipment should be safely and completely shut down and the processes needed to implement this.
- Roles and responsibilities for achieving these shutdowns must also be documented.

e) Log File Recovery Plan

- Defines processes to synchronized log file data from remote locations.
- Provides test plan to validate this process operates correctly.

f) Communication Plan (Include Media, Executives, etc.)

Include directions on:

- Secure Communications Channels
- Incident Communications
  - Team Notifications
  - Incident Updates
- Communications Types/Updates
  - Internal
    - Senior Management
    - Business Units
    - Staff
    - Crisis Management Team
    - Others
  - External
    - Media
    - Law Enforcement
    - Customers
    - Business Partners
    - Vendors
    - Others

g) Michigan Cyber Disruption Response Plan (CDRP) Activation

- Internal conditions and steps necessary to activate the Michigan Cyber Disruption Response Plan.
- Primarily based on organization triage process decision trees.
- Triage process should be fully auditable to ensure appropriate actions and decisions that are made by teams responsible for those actions or decisions.

Annex B: Training and Exercises

B.1 Introduction

This annex provides a training and exercise framework for cyber security professionals charged with the defense of Michigan's critical infrastructure.

B.2 Training Plan

Effective training & exercise plans address the following elements to support the various roles and functions of assigned members:

- Basic and advanced training, including refresher training requirements
  - External training
  - Internal training
  - Certifications gained/maintained
- Process testing training
  - Regular pre-scheduled process training/testing exercises including table-top exercises
  - Random unscheduled process training/testing exercises including table-top exercises

Michigan has defined a set of recommended capabilities associated with seven cyber security domains essential to the protection of critical systems. Critical infrastructure owners and operators must ensure expertise in these seven primary cyber security areas reside within their organization. Development of these capabilities within all partner organizations is the goal. The form those capabilities take, within the organizations, is up to the partners.

The Michigan Cyber Range offers a number of courses that provide training and certifications in the seven core Michigan Cyber Disruption Response Plan training domains. Table B-1 maps domains to course topics and certifications designed to support training plans. More information and a course listing are available at www.merit.edu/cyberrange.

Domains	Course Topics	Cyber Range Certifications
Application Level Security	a. Known Software/Database Vulnerabilities (Java, SQL) b. Web Application Security c. Application Based Attacks (Buffer Overflow, SQL Injection)	Certified Information Systems Security Officer Certified Penetration Testing Consultant Certified Penetration Testing Engineer
Hardware and Device Level Security	a. Vulnerabilities of Routers, Switches, Servers b. Cryptography c. Firewalls	Certified Information Systems Security Officer Certified Penetration Testing Consultant Certified Penetration Testing Engineer
Network Level Security	a. OSI Model and Protocols b. Network Architecture (LAN, Wireless) c. Network Based Attacks (wireless intercept, IP spoofing)	Certified Information Systems Security Officer Certified Penetration Testing Consultant Certified Penetration Testing Engineer
Disaster Recovery and Business Continuity	a. Business Impact Analysis b. Business Continuity Planning c. Interdependency	Certified Disaster Recovery Engineer
Computer Forensics	a. Seizure Concepts b. Incident Investigation c. Digital Evidence and Electronic Discovery	Certified Network Forensics Engineer Certified Digital Forensics Examiner
Physical Security	a. Risks, Threats and Countermeasures b. Physical Intrusion Protection c. Access Control	Certified Information Systems Security Officer
Incident Management	a. Incident Command System b. Roles and Responsibilities c. Incident Reporting	Certified Incident Handling Engineer

Table B-1: Michigan Cyber Disruption Response Training Domains

B.3 Additional Training Resources

In addition to the Michigan Cyber Range, a variety of public and private organizations provide training in the designated training domains in Table B-1, above. Examples of such organizations and training offered include, but are not limited to:

- *Federal Emergency Management Agency (DHS/FEMA) Emergency Management Institute (EMI)* offers a variety of in-residence and online courses in incident management and security and emergency management, including several on continuity and disaster recovery (www.training.DHS/FEMA.gov).

- The *SANS Institute* provides specialized information technology training resources delivered in a variety of formats (www.sans.org).

- The *International Information Systems Security Certification Consortium (ISC2)* offers a number of training and certification (with concentrations) options including the industry leading Certified Information Systems Security

Professional (CISSP) designation (www.isc2.org).

- *ISACA* provides guidance, benchmarks, education and certifications for information systems governance, security, audit, and assurance professionals. ISACA security focused certifications include the Certified Information Systems Auditor (CISA) and Certified Information Systems Manager (CISM) designations (www.isaca.org).

B.4 Exercises

DTMB and MSP/EMHSD work in close collaboration to leverage MSP/EMHSD exercise planning and implementation expertise and methodology using the Homeland Security Exercise and Evaluation Program (HSEEP) framework (Figure B-1). HSEEP ensures exercises are conducted according to a standard risk-based methodology applicable to all mission areas: prevention, protection, mitigation, response and recovery.

Figure B-1: HSEEP Exercise Cycle

DTMB, MSP/EMHSD and subject matter experts will plan, develop, schedule and execute cyber disruption scenarios for the following types of exercise (as detailed in Appendix B: Exercise Types of the State of Michigan/UASI Training and Exercise Plan). HSEEP exercises are organized in a progressive manner.

- Discussion-Based Exercises
    - Seminars – Generally used to orient participants to or provide an overview of authorities, strategies, plans, policies, procedures, protocols, response resources, or concepts and ideas.
    - Workshops – Similar to seminars with increased interaction and focus on achieving or building a product (such as plan or policy).

- Tabletop Exercises (TTXs) – Intended to stimulate discussion of various issues regarding a hypothetical situation. Can be used to assess plans, policies, and procedures or to assess types of systems needed to guide the prevention of, response to, and recovery from a defined incident.

- Operations-Based Exercises

  - Drills – A coordinated, supervised activity usually used to test a single, specific operation or function in a single agency. Commonly used to provide training on new equipment, develop or test new policies or procedures, or practice and maintain current skills.

  - Functional Exercises (FEs) – Also known as a Command Post Exercise (CPX). Focused on exercising the plans, policies, procedures and staffs of the direction and control nodes of the ICS or Unified Command System (UCS).

  - Full-Scale Exercises (FSEs) – Multi-agency, multi-jurisdictional exercises that test many facets of emergency response and recovery. Simulates the reality of operations in multiple functional areas by presenting complex and realistic problems requiring critical thinking, rapid problem solving, and effective responses by trained personnel in a highly stressful environment.

B.5 Exercise Planning Process

MSP (MC3, EMHSD) and DTMB will:

- Determine exercise type/schedule.
- Develop exercise scenarios in collaboration with required subject matter experts.
- Define and coordinate logistics (location, facility, supplies, etc.).
- Coordinate details with the applicable person and/or entity.
- Conduct and evaluate exercise.
- Document findings and recommendations in an after action report and program improvement plan.

Annex C: Risk Assessment

C.1 Risk Management Framework

The adopted risk management framework for the Michigan Cyber Disruption Response Plan is represented in the following graphic:

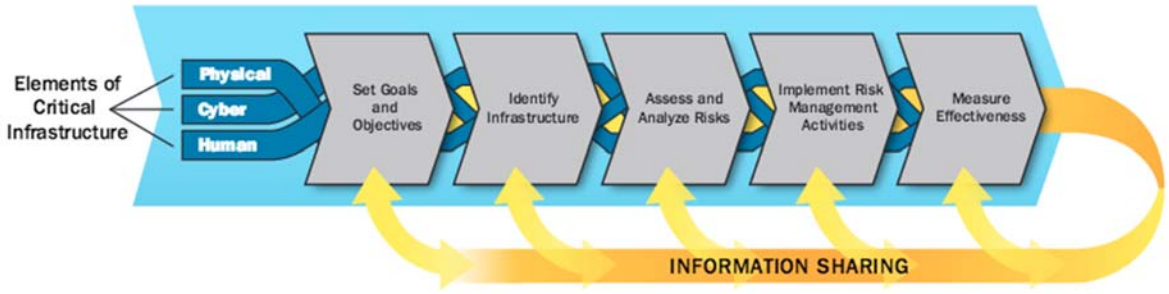

Figure C-1: Risk Management Framework

U.S. Department of Homeland Security, National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience, p. 15. (Available at http://www.dhs.gov/sites/default/files/publications/National-Infrastructure-Protection-Plan-2013-508.pdf)

The Michigan Cyber Disruption Response Plan sets goals and objectives for the management of cyber disruptions affecting critical systems. The remaining areas of the risk management framework are equally important to the effective management of cyber disruption risk.

C.2 Identification of Critical Network Assets

BIA results for each asset in your asset management system (AMS) should be reviewed to identify and prioritize your organizations most valuable and important (critical) assets. The BIA methodology used should encompass the risk assessment methodology outlined below.

C.3 Risk Assessment Methodology

Risk assessment involves the development of a measure of risk based on the evaluation of the threat, vulnerability and consequences associated with an attack on a target, such as critical infrastructure. Risk assessment is necessary for risk management and typically involves the following steps:

1. Identify critical infrastructure and key resources;
2. Identify and assess threats to the subject infrastructure;
3. Identify the vulnerabilities of the target infrastructure associated with the identified threats;
4. Evaluate the consequences of a successful attack on the subject infrastructure;
5. Determine the risk to the subject infrastructure based on the aforementioned factors;
6. Identify means of reducing risk to subject infrastructure;
7. Evaluate the resources available to mitigate risk; and,
8. Develop a risk management strategy taking into account the risk priorities and resources available.

Common methods for risk assessment include the use of subject matter experts and the scoring of risk characteristics based on relativistic scales. Additionally, penetration testing or "red team" techniques may be used to uncover vulnerabilities and test security of potential targets, yielding data that may be used to develop risk assessments and mitigation priorities.

A common method of risk evaluation is the use of relativistic methodologies. In this approach, various scales are used commonly across all evaluated targets and targets are given a score based on the assessor's determination. Often, individuals conduct these risk assessments with expertise in the given sector in order to support the evaluation's integrity. These scales are typically represented in one of two ways, either by a scoring scale, which applies points to different vulnerabilities, which are later totaled, or by percentage. In the case of percentage the decision factor is often represented as (0,1), meaning the factor should be rated as 0% probably (0) to 100% probable (1). For example, the threat of a vehicle borne improvised explosive device at a particular target site may be assessed by an expert to be 85% likely (.85). The factor can then be applied in a formula upon which the method is based.

R = TxVxC
Where:
- R= Risk (Expected Loss)
- T = Threat
  - (0,1)
  - Likelihood of a potential type of attack
    Intent and capability of the adversary
- V = Vulnerability
  - (0,1)
  - Likelihood or probability of successful attack
- C = Consequence
  - Replacement cost, could be in dollars
  - Direct economic impact
  - Indirect economic impact

The Michigan Cyber Disruption Plan recommends that any risk assessment used by partners is documented, reproducible, and defensible and based on the risk factors indicated above. The results of such risk assessment results can be discussed and shared with partners, as appropriate, to assist in the identification of critical network nodes and their associated interdependencies.

C.4 Prioritized Remediation

Ultimately, the goal of the risk assessment process is to provide a prioritization of the critical assets of Michigan's networks, and a plan to safeguard them. The highest priority assets should be those that are most vulnerable and would have the greatest impact if disrupted. As such, these critical nodes should receive the greatest amount of resource support. Members will develop remediation plans based on their risk assessment

activities using a state-wide pre-defined remediation plan format, the key fields include:

Member Name:
Location:
Function:
Risk Identified:
Asset(s) Impacted and their Criticality:
Recommended Remediation Activity:
Date Remediation Activity Approved:
Date Remediation Activity Approved by:
Residual Risk(s) following Remediation Activities:
Date Remedial Recommendation(s) Implemented:
Implementation Team:

These plans will be reported to the CDRP partnership at a level of detail deemed appropriate by the reporting member.

C.5 Measuring Effectiveness

An effective protective program should yield measurable progress. Regular meetings of the Michigan Cyber Disruption Response Plan Partners will include a structured report of the effectiveness of remediation.

Annex D: CDRP Roles and Responsibilities

D.1 Michigan Chief Information Officer (CIO)

When a cybersecurity event escalates to be classified as a cyber-disruption the CIO works with MSP/EMHSD, the SBO, the Chief Technology Officer (CTO) and the Chief Security Officer (CSO) to identify related issues and effects, and assist in the remediation efforts. The CIO is also responsible for communications with high-level political officials and the media.

D.2 Michigan Chief Technology Officer (CTO)

The CTO reports to the CIO and is responsible for state IT infrastructure day-to-day operations. During a cyber-disruption, the CTO works with the CIO, CSO, and MSP/EMHSD to ensure cybersecurity issues and effects are properly identified and remediated. The CTO also collaborates with MSP/EMHSD to establish the SEOC and coordinate mitigation and recovery activities where man-made or natural disasters intersect with a parallel cyber-attack or cyber disruption effort.

D.3 Michigan Chief Security Officer (CSO)

The CSO reports to the CIO and is responsible for protecting the State's IT infrastructure from internal and external cybersecurity threats. The CSO is also responsible for the state's cybersecurity readiness, threat analysis, and remediation efforts. This responsibility includes:

- Working with agency IT staff to address local and statewide cybersecurity events.
- Working with MS-ISAC to assist in statewide, regional and national cybersecurity events and to communicate potential remediation procedures to agencies, counties, boroughs, and cities impacted by a cyber-disruption.
- Acting as the MI-ISAC chairman:
    - Ensuring the state or regional ISAC communicates cybersecurity threat levels and provides local readiness and response within the state.
    - Providing a central resource for gathering information on cyber threats to critical infrastructure throughout the state.
    - Facilitating information sharing between local governments and other states encompassed by the event.
- Leading response efforts for cybersecurity events that have statewide implications. During a concurrent cyber-event and emergency event, the CSO and MSP/EMHSD or the Incident Commander will share this role.
- State Emergency Operations Center (SEOC) Cybersecurity Emergency Preparedness Liaison Officer (EPLO) – The CSO is the CIO's representative at the SEOC during cyber events that reach High or Severe threat level.
- Michigan Emergency Management Plan/Emergency Support Function (MEMP/ESF) #2 (Warning and Communications) – The CSO will ensure the Office for Information Security fulfills the responsibilities identified in the Cyber

Attacks section of the MEMP Technological Disaster Procedures section, maintained by MSP/EMHSD.

- Federal Emergency Management Agency (FEMA) – The CSO, in conjunction with MSP/EMHSD, will work with FEMA to address cybersecurity incidents and disruptions that impact or are precipitated by national disaster recovery efforts.
- U.S. Computer Emergency Readiness Team (US-CERT) – The CSO will ensure the Office for Information Security works with US-CERT to gather and disseminate cybersecurity information and warnings to the state.
- Michigan State Police, Emergency Management and Homeland Security Division (MSP/EMHSD) – The CSO will assist MSP/EMHSD with their mission of enhancing the state's information and intelligence sharing capabilities with law enforcement on a local, state, and national level, focusing on prevention, protection and mitigation.
- Michigan Intelligence Operations Center (MIOC) and Michigan Cyber Command Center (MC3) – The CSO will work with the MIOC and the MC3 to support their mission of assisting local, state, and federal law enforcement agencies with cyber terrorism and cyber-criminal activity. This assistance may range from providing subject matter experts (SMEs) to assist in the analysis of cyber threat information to providing cybersecurity training for the MIOC and MC3 analysts.
- Service Providers (SP) – The CSO will work with the service providers listed in the state enterprise services portfolio to ensure they perform proper reporting and management of cybersecurity disruptions in order to secure and protect the state's critical IT business processes and assets from cyber threats.
- Proactive Cybersecurity Event Monitoring – The CSO will use the MS-ISAC, Microsoft Bulletins, and other media outlets to proactively identify potential cybersecurity threats and take precautions before they can cause harm to the state's IT infrastructure.
- State Security Threat Level – The CSO is responsible for setting and alerting the state regarding the current cybersecurity threat posture.
- Cybersecurity Alerts – The CSO, in partnership with the MC3, disseminates cyber threat warnings and information to state government agencies, local government agencies, private citizens, and business entities.
- Coordinating Recovery From Cybersecurity Attack/Event – During a cyber-event the CSO coordinates the recovery of state network operations, telecommunications, and IT applications and databases.
- Remediation Efforts – The CSO coordinates with local government IT representatives, through the MI-ISAC and ISOs, to exchange policy and operational information required to respond to and recover from cybersecurity incidents.
- Agency Support – The CSO provides assistance to agencies remediating issues caused by cybersecurity incidents.

- Cybersecurity Preparedness and Education – The CSO is responsible for preparing and educating state agencies, and employees to the dangers of cybersecurity threats and how to reduce risk exposure.
- Collaboration – The CSO, in partnership with the MC3, facilitates interaction and collaboration among state agencies, state and local governments, national organizations, business partners, private sector entities, and international organizations related to cybersecurity and cyber incidents.
- Cybersecurity Advanced Analytics – The CSO develops and exercises cybersecurity related predictive analytics capabilities.
- Cybersecurity Forensic Analysis – The CSO supports the Department of Justice, Federal Bureau of Investigations, Michigan State Police and other law enforcement agencies in investigating and gathering information related to cyber threats and attacks.
- Statewide Cybersecurity Emergency Response – The CSO work with MSP/EMHSD to coordinate remediation efforts from a cybersecurity event that jeopardize the health and safety of the citizens of the state. The CSO disseminates cyber threat warning information in conjunction with the SEOC.

D.4 Enterprise Data Center (EDC)

The EDC is responsible for ensuring state servers are patched properly and have the most current antivirus and intrusion detection software installed. During a cybersecurity event, the EDC will work with the CSO to resolve issues that may require initiation of the Disaster Recovery Plan.

D.5 Continuity of Operations Plan Incident Command Team

In the event of activation or partial activation of the Continuity of Operations Plan (COOP), the COOP Incident Command Team has been identified and organized according to federal NIMS/ICS guidelines. To staff the COOP teams, MSP/EMHSD has identified key positions to provide management and technical expertise necessary to establish critical functions within 12 hours after the emergency event.

D.6 Agency Cybersecurity Emergency Preparedness Liaison Officer (Agency Cybersecurity EPLO)

The Agency Cybersecurity EPLO is assigned and authorized, by the respective agency heads, to act as the agency's cybersecurity representative at the SEOC. During a cybersecurity event, this individual:

- Represents the Agency – The Agency Cybersecurity EPLO represents the agency, from an IT perspective, and has authority to redirect IT personnel, assets, and other resources to the remediation effort.
- Emergency Purchase Orders – The Agency Cybersecurity EPLO completes emergency purchase orders to procure equipment, staff augmentations, backup facilities, services and supplies.

- Enacts the Agency COOP - The Agency Cybersecurity EPLO has the authority to enact the agency's COOP.

D.7 Agency Information Security Officers (ISOs)

ISOs are responsible for the day-to-day IT security administration of their respective agencies. During a cybersecurity event, ISOs report cybersecurity incidents to the CSO. ISOs:

- Monitor their agency's internal cybersecurity level and report increases/decreases to the CSO.
- Report cybersecurity incidents to their agency IT staff and the CSO.
- Communicate security related information to the CSO, agency IT staff, business partners, and users.
- Assist in agency remediation efforts.

D.8 State Government Service Providers

State government service providers support the CSO with the state's cybersecurity mission and perform proper reporting and management of cybersecurity incidents in order to secure and protect the state's critical Information Technology (IT) business processes and assets from cyber-threats. As part of these responsibilities, service providers provide:

- Technical and operational support for the CSO when a cybersecurity incident involves enterprise assets, multiple agencies, or outside entities such as business partners or citizens that are utilizing a service provider's controlled assets (e.g., appliances, servers, firewalls, routers, and other systems), Incident handling processes are outlined in Section 6.4 and 6.5 for service providers and service provider/Level 3 respectively
- Points of contact to be responsible for ensuring that cybersecurity incident reporting and handling is addressed within the timeframes identified by the state's incident response Service Level Agreements (SLAs).
- Notification to DTMB, within thirty (30) minutes of detection, that incident reports need to be filed within four (4) hours of detection.
- Prompt investigation of incidents involving the unauthorized or accidental modification, destruction, disclosure, loss, damage, misuse, or access to information technology resources such as systems, files, and databases.
- Alerts to CSO of potential cybersecurity incidents discovered via their automated incident response, intrusion detection, and security event and incident management systems.
- Names, work phone numbers, mobile phone numbers, home phone numbers, and work and home e-mail addresses for cybersecurity incident responders who can work with CSO to remediate cybersecurity incidents
- Cooperation with CSO cyber incident investigation and remediation efforts.

- Processes for ensuring all service provider security operations and support employees are aware of the state's cybersecurity policies and procedures.
- Guidance to ensure the service provider security operations and support Service Desk personnel are aware of the internal/external cybersecurity incident response processes and how to differentiate between network, telecom, and cybersecurity incidents.

D.9 State Government Business Partners

State Government Business Partners (BPs) are defined as companies and non-profit organizations that provide support to the state IT infrastructure or require access to provide services to citizens. During a cybersecurity incident, BPs work with the, CIO CTO, and CSO to remediate issues associated with the attack.

D.10 Michigan State Police, Emergency Management and Homeland Security Division (MSP/EMHSD)

The mission of MSP/EMHSD is to coordinate state agency response, including the to support county and local governments in the areas of civil defense, disaster mitigation and preparedness, planning, and response to and recovery from man-made or natural disasters.

MSP/EMHSD manages the overall protection framework and oversees the implementation and continual evaluation of the state's Critical Infrastructure Protection Program. This program is comprised of five objectives that include: identifying assets; assessing risks; prioritizing disaster recovery; implementing protective programs; and measuring effectiveness.

During a cybersecurity event, MSP/EMHSD monitors the situation to determine if an event is tied to a terrorist attack. If it is, MSP/EMHSD will act as a liaison to the Federal Department of Homeland Security (DHS) to help coordinate federal resources and assist in the recovery process.

From a cybersecurity perspective MSP/EMHSD:

- Works with the county emergency management agencies and communication centers to ensure that MSP/EMHSD's IT based resources are not impacted by a cyber-security event.
- Coordinates statewide response of the counties and municipalities and collect, report, and remediate any cybersecurity threat that could impact disaster recovery efforts.
- Acts as the state's backup cybersecurity operations center providing the CIO and agencies, impacted by cybersecurity events, with meeting facilities and back-up communications (satellite feeds, wireless radios, etc.).

D.11 Michigan Information Sharing and Analysis Center (MI-ISAC)

The MI-ISAC is responsible for addressing cybersecurity readiness and critical infrastructure coordination. It is led by the CSO who is responsible for leading the state's

efforts for cyber-readiness and resilience. It provides a common mechanism for raising the level of cybersecurity readiness and response within state government by providing a central resource for gathering information on cyber threats to critical infrastructure throughout the state and providing two-way sharing of information between and among local governments.

D.12 Michigan Intelligence Operations Center (MIOC)

The MIOC, operated by the Michigan State police, is the statewide intelligence operations fusion center that provides law enforcement agencies a central point of contact for their information needs. MIOC analysts provide state police members and federal, state, and municipal law enforcement officers with access to intelligence information, investigative data, and public source information 24 hours a day, seven days per week. Analysts also provide investigative support by analyzing complex information and collating it into intelligence summaries, organization charts, link analysis, time event analysis, and other manageable, professional products.

During a cyber event, the MIOC works in conjunction with MC3 and the CSO to help identify, document, and collect forensic evidence for potential prosecution. In addition to this, the MIOC helps coordinate investigations that involve the Department of Homeland Security and the Federal Bureau of Investigation's cyber law enforcement agencies to prosecute cyber criminals that may reside in other states and nation states.

D.13 Michigan Cyber Command Center (MC3)

The MC3 is a specialized group of MSP enlisted and civilian analysts who are highly trained and have legal authority to investigate technology facilitated crimes in partnership with skilled public and private professionals in emergency response to cyber events. The MC3 emphasizes Cyber Crime prevention through information sharing, training, partnerships, and outreach. It functions as the central command and control center during cyber disruption situations having a potential crime nexus. During a Cybersecurity event, the MC3 is responsible for the coordination of Cyber First Responders focusing on minimizing damage, identification of electronic evidence, forensic data recovery and analysis, as well as developing strategies for criminal prosecution while operating under the authority of the SEOC.

D.14 Michigan National Guard Cyber Teams (MI-NGCT)

The Michigan National Guard (NG) is comprised of the Air National Guard (ANG) and Army National Guard (ARNG). In peacetime, the governor serves as commander in chief of the NG, exercising control through the adjutant general. In the event of natural disaster or civil emergency, the governor can order NG personnel and equipment into service to assist state and local authorities. As part of this mission, the NG has created teams of part-time soldiers and airmen who work as cybersecurity experts in the private and public sectors.

During a large scale cyber event, the Governor will activate NG cyber teams to assist state and local governments with combating cyber-attacks and restoring critical physical infrastructure (including dams, power plants, mass transit) and services lost or damaged resulting from cyber-attacks. In addition to recovery, the NG will work with MSP/EMHSD and service providers to establish alternate forms of telecommunications

(satellite, cellular, shortwave, etc.) and assist with physical security at critical infrastructure and alternate recovery sites.

D.15 Michigan Cyber Civilian Corps (MiC3)

The Michigan Cyber Civilian Corps (MiC3) provides rapid response to Governor-declared state of emergency cyber events. It consists of volunteer cyber experts, from government, education and business sectors, who work with DTMB, MSP, NG and other public and private sector entities providing mutual aid to government, education and business organizations in the state of Michigan.

D.16 Multi-State Information Sharing and Analysis Center (MS-ISAC)

The MS-ISAC is a collaborative organization with participation from all 50 states, the District of Columbia, local governments and U.S. Territories. The mission of the MS-ISAC is to provide a common mechanism for raising the level of cybersecurity readiness and response in each state and with local governments.

D.17 DHS/Federal Emergency Management Agency (DHS/FEMA)

DHS/FEMA provides communications and IT support to Joint Field Office operations, and coordinates the restoration of Public Safety Communications systems and first-responder networks. During a cybersecurity event, DHS/FEMA works with the National Communications System (NCS) to provide communications support to the impacted area and assists in the remediation efforts.

D.18 U.S. Computer Emergency Readiness Team (US-CERT)

US-CERT is a 24/7 operations center with connectivity to all major federal cyber operations centers, private sector Internet service providers, information sharing mechanisms, and vendors. During a cyber-event, US-CERT acts as a focal point to collect and disseminate cybersecurity information received from public and private sector sources.

Annex E: Glossary

Abbreviation Definition

A

ANG	Air National Guard
AMS	Asset Management System
APT	Advanced Persistent Threat
ARNG	Army National Guard
ASEOC	Alternate State Emergency Operations Center

B

BCP	Business Continuity Plan
BIA	Business Impact Assessment
BP	Business Partner

C

CDRP	Cyber Disruption Response Plan
CDRT	Cyber Disruption Response Team
CIO	Chief Information Officer
CISA	Certified Information Systems Auditor
CISM	Certified Information Systems Manager
CISSP	Certified Information Systems Security Professional
COG	Continuance of Government
ConOps	Concept of Operations
COOP	Continuity of Operations Plan
CPX	Command Post Exercise
CSO	Chief Security Officer
CTO	Chief Technology Officer

D

DHS	Department of Homeland Security
DR	Disaster Recovery
DTMB	Department of Technology, Management and Budget

E

EDC	Enterprise Data Center
EM	Emergency Management
EMI	Emergency Management Institute
EPLO	Emergency Preparedness Liaison Officer
ESF-2	Emergency Support Functions – Communications

F

FBI	Federal Bureau of Investigation
FE	Functional Exercise
FEMA	Federal Emergency Management Agency
FOIA	Freedom of Information Act
FSE	Full-Scale Exercise

G

H

HSEEP	Homeland Security Exercise and Evaluation Program
HSIN	Homeland Security Information Network

I

IAP	Incident Action Plan
ICS	Incident Command System
IIS	Internet Information Services
IOC	Indicators of Compromise
IP	Internet Protocol
ISAC	Information Sharing and Analysis Center
(ISC)2	International Information Systems Security Certification Consortium
ISO	Information Security Officer
IT	Information Technology

J

K

L

M

MC3	Michigan Cyber Command Center
MEMP/ESF	Michigan Emergency Management Plan/Emergency Support Function
MiC3	Michigan Cyber Civilian Corps
MI-ICS	Michigan-wide Incident Command System
MI-ISAC	Michigan Information Sharing and Analysis Center
MING	Michigan National Guard
MI-NGCT	Michigan National Guard Cyber Teams
MIOC	Michigan Intelligence Operations Center
MOM	Microsoft Operations Manager

MS-ISAC	Multi-State Information Sharing and Analysis Center
MSP	Michigan State Police
MSP/EMHSD	Michigan State Police, Emergency Management and Homeland Security Division

N

NCS	National Communications System
NG	National Guard
NGO	Non-Governmental Organization
NIMS	National Incident Management System
NIPP	National Infrastructure Protection Plan
NSA	National Security Agency

O

OP	Operational Period

P

Q

R

RTO	Recovery Time Objective

S

SBO	State Budget Office
SCADA	Supervisory Control and Data Acquisition
SEOC	State Emergency Operations Center
SLA	Service Level Agreement
SME	Subject Matter Expert
SOC	Security Operations Center
SOS	Security Operations and Support
SP	Service Provider

T

TTX	Tabletop Exercise

U

UASI	Urban Areas Security Initiative
UPS	Uninterrupted Power Supply
US-CERT	United State Computer Emergency Response Team

V

VOIP Voice Over Internet Protocol

W, X, Y, Z

SPECIAL THANKS TO THE CIO AND CSO KITCHEN CABINETS FOR THEIR PARTNERSHIP

Amerisure
Beaumont Health Systems
Blue Cross Blue Shield
Board of Water & Light
BorgWarner
CGS Advisors
Chrysler
City of Detroit
City of Detroit Water & Sewage
CMS Energy
Dow
DTE Energy
Education Achievement Authority of Michigan
Federal Mogul
Flagstar Bank
Homedics
Kent County
Meridian Health Plan
MGM Grand Detroit
Michigan Health Cybersecurity Council
Michigan State University
Nexteer Automotive
Oakland County
Penske
Plante Moran
Quicken Loans
Sparrow
University of Michigan
ZF Group


THE STATE OF MICHIGAN
E PLURIBUS UNUM
TUEBOR
SI QUÆRIS PENINSULAM AMŒNAM
CIRCUMSPICE
A.D.MDCCCXXXV.