STATE OF MICHIGAN CYBER DISRUPTION RESPONSE PLAN

Prepared by:
Department of Technology, Management & Budget
November 2023

GRETCHEN WHITMER
GOVERNOR

STATE OF MICHIGAN
OFFICE OF THE GOVERNOR
LANSING

GARLIN GILCHRIST II
LT. GOVERNOR

November 12, 2023

Dear Michigan Cybersecurity Partners,

The Michigan government works diligently to block numerous unauthorized attempts to probe, scan, access, or disrupt its computer networks every day. 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 events are blocked by defensive systems, evolving cyber threats represent a significant risk to the continuity of state government.

Recognizing the critical nature of Michigan's cyber networks, the Michigan Cyber Initiative was launched in 2011. This initiative encouraged public and private partnerships among key stakeholders throughout Michigan to safeguard and defend Michigan's critical cyber networks. Through collaboration by state and local governments, and public and private partners, the Cyber Disruption Response Plan (CDRP) was created in 2015. The CDRP outlines and coordinates responses by cyber partners throughout Michigan as they respond to cyber incidents against Michigan's critical cyber infrastructure. It includes strategies for information sharing, criminal investigation, cyber-attack response, and recovery from significant cyber-disruptions to Michigan's critical infrastructure.

Since the CDRP was created, cyber threats continue to grow and evolve. The CDRP has been updated to address the changing threat environment and incorporate current protocols. The CDRP allows for more scalable and flexible responses to the dynamic cyber environment. This update ensures that Michigan cyber partners can respond proportionally to meet the threats that the State faces.

Today's evolving threat environment, combined with the interconnected cyber network, require close collaboration among cyber stakeholders more than ever before. By providing a unified framework to respond to cyber incidents, we enhance our preparedness for cyber threats that may affect the State. Regardless of how cyber threats persist or evolve, Michigan's cyber partners will continue to be at the forefront to safeguard our critical cyber infrastructure.

Michelle Lange
Director
Department of Technology, Management & Budget

Colonel James F. Grady II
Director
Michigan State Police

Major General Paul D. Rogers
Adjutant General
Michigan National Guard

Contents

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 can 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 by defining five threat levels 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 coordination by providing a standard incident response plan template 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 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 & Budget (DTMB), the Michigan National Guard (MING), the Michigan State Police, Emergency Management and Homeland Security Division (MSP/EMHSD), and MSP Intelligence Operations Division (MSP/IOD) 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).

3.0 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.

3.1 CDRT Membership Organization

DTMB and MSP representatives will provide Cyber Disruption Response Team leadership. The Chief Security Officer (CSO) will be appointed Chairperson and the Deputy State Director of Emergency Management will serve as Vice Chairperson. During State Emergency Operations Center (SEOC) activation, the CDRT will serve in a consultive role to incident/unified command.

3.1.1 Membership

The core CDRT is composed of representatives from the emergency management (EM), information technology (IT), and law enforcement communities within Michigan. Additional local, state, and federal agencies, along with healthcare, education, and private sector organizations, with critical cyber infrastructure knowledge and expertise may be requested to participate in applicable CDRT operations. 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.

3.1.2 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.

3.2 CDRT Function

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.

3.2.1 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 means and methodologies to enable CDRT communication and transactions as prescribed in Annex A: Communication Methods.
- Develop plans and procedures to address specific disruptions.
- Train and exercise this CDRP, as well as other business continuity, continuity of operations, and continuity of government plans. Details on exercise program development and implementation are provided in Annex C: 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.

3.2.2 Activation

CDRT activation can be authorized by the CDRT chairperson or vice chairperson upon request by CDRT member organization, local officials, law enforcement, or emergency managers. Activation decisions are made based upon the trigger criteria described below.

- Major disruptions of power grids in the region.
- Threat to or widespread loss of communications and data networks (e.g., internet, mobile/cellular).
- Imminent threats to critical government facilities.
- Significant cyber incidents.
- Physical damage to a critical cyber asset.
- Loss of access to a facility hosting a critical cyber asset.
- Loss of staff (e.g., injury, sickness, or death) with irreplaceable knowledge of critical cyber systems.
- Other events that have the potential to create significant cyber threats or incidents.

When the CDRT chair decides to initiate a CDRT meeting or teleconference, the initiator develops a brief message indicating the date, time, who is activated, communication method (e.g., teleconference, in-person), and summary of the reason for the activation:

"CDRT Activation in response to Detroit-area major power outage. CDRT Core and Associate Members. Teleconference scheduled for 7/10/2015 at 1300 on 888-555-1212 x123456. If communication systems fail, Core members will meet at Lansing JOC at 442 Roper Ave. at 1400."

3.2.3 Response

The CDRT incident response process considers activation of the SEOC during Severe and High Level incidents. The CDRT 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 the CDRT 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 Incident/Unified Command and General Staff during a response including:
    - Assisting Incident/Unified Command Operations Staff to understand technical and operational issues regarding cyber-related resources and networks.

- Assisting Incident/Unified Command 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 Command and contained in an IAP.

3.2.4 Recovery

CDRT members have a responsibility to be active throughout the recovery phase of an event, under the direction of the Deputy State Director of Emergency Management. It is possible that the recovery effort could exist over an extended period. CDRT responsibilities during the recovery phase 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 Command 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 in MING resources can be of assistance.
- Conducting internal and external CDRT after-action reviews to obtain lessons learned following an incident.

3.3 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 operation periods to organize resources and measure effectiveness.
- Assigning staff to consultive, 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.

4.0 Cyber Alert Escalation/De-escalation Procedures

The Michigan Cybersecurity Threat Matrix consists of five distinct threat levels, as illustrated in Figure 1, which are impacted by internal and external cybersecurity events. The matrix provides a high-level snapshot of anticipated response for each threat level.

Threat Level	Description	Potential Impact	Anticipated Response Activity
Low	*Unlikely to impact* public health, safety, or confidence.	Normal concern for known hacking activities known viruses or other malicious activity.	None expected.
Medium	*May impact* public health, safety, or confidence.	Potential for malicious cyber activities, malicious activity has been identified on SOM networks with minor impact, no known exploits identified, or known exploits identified but no significant impact has occurred.	Informational only. No follow-up activity required. No real-time collaboration. All information sharing is passive and asynchronous.
High	*Likely to result in a demonstrable* impact to public health, safety, or confidence.	Compromised systems or diminished services.	Real-time synchronous collaboration via phone and email as required. No financial considerations, no deployments, all activities conducted remotely.
Severe	*Likely to result in a significant* impact to public health or safety.	Core infrastructure targeted or compromised causing multiple service outages, multiple system compromises or critical infrastructure compromises.	Voluntary resource collaboration between members, technical information sharing & resource deployment based on mutual aid agreements. Could include financial considerations.
Emergency	*Poses an imminent* threat to the provision of wide-scale critical infrastructure services.	Widespread outages and/or significantly destructive compromise to systems with no known remedy or one or more critical infrastructure sectors debilitated.	State Emergency Operations Center activation. Statewide response coordination by Michigan State Police. Michigan Cyber Civilian Corps (MiC3) activation.

Figure 1: Michigan Cybersecurity Threat Matrix

The Cyber Disruption Response Escalation Path (Figure 2 below) depicts the state of Michigan decision-making process designed to drive rapid and effective responses to potential cyber disruption scenarios.

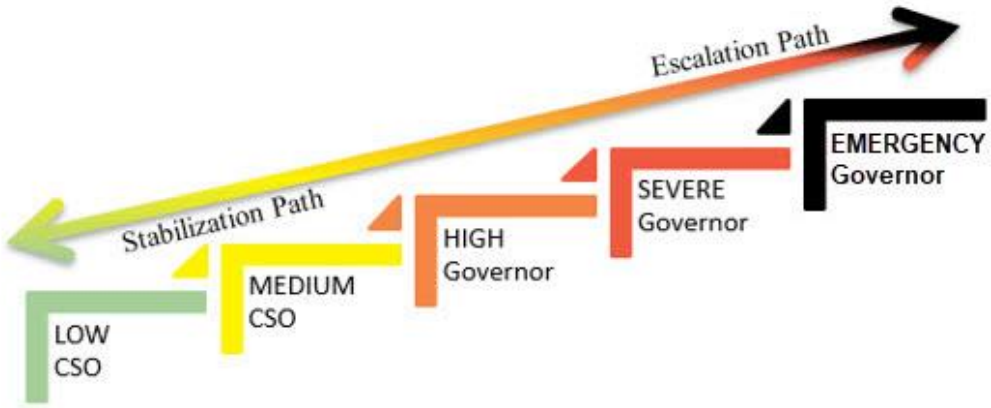

Figure 2: Cyber Disruption Response Escalation Path

It is important to note that threat levels in this document may not occur in a linear order and are dependent on the individual characteristics of the cyber incident or threat.

4.1 Cybersecurity Threat Level Low (Green)

Threat Level Low (Green) is the lowest operational level in the cybersecurity threat matrix.

Steady state – Insignificant or no malicious activity has been identified. Examples include but are not limited to:

- Credible warnings of increased probes or scans reported from authoritative sources and/or discovered in State of Michigan networks.
- Infected by known low risk malware.
- Other like incidents.
- Normal activity with low level of impact.

Actions:

- Continue routine preventative measures including application of vendor security patches and updates to anti-virus software signature files on a regular basis.
- Continue routine security monitoring.
- Determine baseline of activity for the state – it is important to know what "normal" looks like – and then continually be on alert for any changes to that baseline.
- Ensure all personnel receive proper training on cybersecurity policies and security best practices.

4.1.1 Responsibilities

The **Chief Security Officer (CSO)** is responsible for the following function:

- Threat Monitoring – The CSO will monitor national and international cybersecurity threat levels and cybersecurity informational resources to identify and report on potential threats that could impact the state.

State of Michigan Information Technology (SOM IT) is composed of various State information technology units including agency Information Security Officers, Agency Services IT liaisons, Technology Services, DTMB IT, Michigan Security Operations Center (Mi-SOC), among others. Individually and collectively, SOM IT is responsible for the following functions:

- Threat Monitoring – Monitoring national and international cybersecurity threat levels and cybersecurity informational resources.
- Resource Management – Ensuring operating systems, antivirus security agents and firewalls are up to date.
- Reporting Cybersecurity Incidents – Reporting agency specific cybersecurity incident(s) to the CSO. Incidents can range from data breaches to unexplained network issues/traffic.
- Agency Cybersecurity Alert Level – Monitoring agency cybersecurity readiness and internal threat levels. Increase the level when a confirmed cybersecurity incident occurs or during times the respective agency could be greater risks of attack, such as tax season and elections.
- Antivirus – SOM IT will ensure that all servers have the most current antivirus agents and files installed and working correctly.

MSP Michigan Cyber Command Center (MC3) will**:**

- Support the mission of the CDRP by gathering and sharing intelligence related to cybersecurity threats.
- Will determine if any events are criminal in nature and will work with partners to initiate a criminal investigation and prosecute malicious actors identified during the criminal investigation.
- May refer impacted parties to resources available to assist with remediation.

MSP EMHSD will support the cyber mission by monitoring the national and international cybersecurity threat levels and cybersecurity informational resources.

MSP Michigan Intelligence Operations Center (MIOC) will work with the MC3, CSO, and Federal Bureau of Investigation (FBI) to identify potential threats that could impact the state and its business partners.

4.2 Cybersecurity Threat Level Medium (Yellow)

Threat Level Medium (Yellow) is the first active threat level in the cybersecurity threat matrix. Malicious activity has been identified on State of Michigan networks with minor impact. Examples include but are not limited to:

- Changes in normal activity with minor impact to IT operations.
- A vulnerability being exploited with minor impact.
- Infected by malware with the potential to spread quickly.
- Compromise of non-critical system(s) that did not result in loss of sensitive data.
- A distributed denial of service attack with minor impact.

Actions:

- Continue recommended actions from previous level.
- Identify vulnerable systems and implement appropriate countermeasures.
- Identify malware on system(s) and remediate accordingly.
- Document data exposure with minor impact.
- When available, test and implement patches, install anti-virus updates, and other security measures in the next regular cycle.

4.2.1 Potential Impact

At a Medium Threat Level, the following conditions are in place:

- There is no threat to mission critical applications or resources. The issue has been properly identified and can easily be remediated without risk of a data breach or theft of services.
- The issue can be remediated within normal business hours.
- The threat can be easily remediated by installing software patches, updating the antivirus files, or denying network access to specific Internet Protocols (IPs) or IP ranges.
- A special event or circumstance incites hackers interested in trying to disrupt the agency's IT services or cause political embarrassment such as website defacements, and application hacking.

4.2.2 Responsibilities

The **Michigan Chief Information Officer (CIO)** will work with agencies to ensure they comply with remediation recommendations provided by the CSO and CTO.

The **Michigan Chief Technology Officer (CTO)** will be responsible for communicating with the CIO. Additionally, the CTO will ensure all executive branch agencies assist with remediation effort.

The **CSO** is responsible for notifying all stakeholders when the alert level changes from Low (Green) to Medium (Yellow), will work with the CIO and CTO to assist with communication and remediation efforts and will coordinate communications between state agencies, the Multi-State Information Sharing and Analysis Center (MS-ISAC), and the Michigan-wide Information Sharing and Analysis Center (MI-ISAC). The CSO is also responsible for:

- Incident Reports – The CSO will investigate incidents reported to them by SOM IT, state employees, State Security Operations Center (SOC), state agencies and functions or state government service providers.
- MI-ISAC Advisories – The CSO will work with the MI-ISAC to create advisories for distribution to members.
- MS-ISAC Coordination – The CSO will contact MS-ISAC as needed for more information about potential attacks or to request clarification on remediation efforts.

SOM IT will work with the CSO to identify actions necessary to remediate the threat. Additionally, SOM IT will be responsible for:

- Security Monitoring Tools – Reporting any anomalies detected by security monitoring tools to the CSO.
- Communication – Working with the CSO and their customers to identify and communicate information about the incident and remediation efforts.
- Agency Alert Level – Monitoring the incident and adjusting agency alert levels to properly match their readiness and remediation efforts.

Agencies will work with SOM IT to address any concerns or issues and to coordinate remediation efforts that may requires assistance from the CSO or other agencies. Agencies will also communicate with **State Government Service Providers (SPs)** and other **Business Partners (BPs)** to ensure they are aware of security (or threat) level changes and to take additional proactive measures to secure their IT infrastructure.

MSP MC3 will continue monitoring, information sharing, support, and investigative actions previously described in Section 4.1.

MSP EMHSD will:

- Continue to monitor national and international cybersecurity threat levels and cybersecurity information resources.
- Monitor Michigan Critical Incident Management System (MI CIMS) and resource requests.
- Collect, communicate, and provide situational awareness of local emergency management information with the CDRT and MSP leadership.
- Monitor incidents for potential cascading effects.
- Determine the need for SEOC activation.

MSP MIOC will continue monitoring and information sharing as previously described in Section 4.1.

The **MING** will work with the MC3 and other partners to assist with the assessment of potential threats and information sharing when allowed by statute. The MING may be called upon to assist the CSO with the event if additional resources are required.

4.3 Cybersecurity Threat Level High (Orange)

Threat Level High (Orange) is the third threat level in the cybersecurity threat matrix. Malicious activity has been identified in state networks with a moderate level of damage or disruption. Examples include but are not limited to:

- An exploit for a vulnerability that has a moderate level of damage.
- Compromise of secure or critical system(s).
- Compromise of systems containing sensitive information or non-sensitive information.
- More than one agency affected in the state network with moderate level of impact.
- Infected by malware spreading quickly through the Internet with moderate impact.
- A distributed denial of service attack with moderate impact.

Actions:

- Continue recommended actions from previous levels.

- Identify vulnerable systems.
- Increase monitoring of critical systems.
- Immediately implement appropriate countermeasures to protect vulnerable critical systems.
- When available, test and implements patches, install anti-virus updates and other system security measures as soon as possible.
- Contact the MC3 for awareness and information sharing regarding potential threats and outreach to other entities for prevention purposes.

4.3.1 Potential Impact

At a High Threat Level, the following conditions are in place:

- A critical vulnerability, with the potential to cause significant damage if exploited, has been detected.
- Multiple web defacements
- A critical vulnerability is being exploited and there has been moderate impact.
- Attackers have gained administrative privileges on compromised systems.
- Critical applications or resources have been impacted.
- Compromise of secure or critical system(s) containing sensitive information.
- Compromise of critical system(s) containing non-sensitive information if appropriate.
- IT Services may be interrupted by denial-of-service attacks.
- The issue can be remediated within one to three business days and may require critical applications or services be taken offline until the issue can be remediated.
- The State Continuity of Operations Plan/Continuity of Government (COOP/COG) may have to be initiated to address damages from the cyber-attack.
- The threat can be remediated by state agencies installing software patches, updating the antivirus files, or denying network access to specific IPs or IP ranges.

4.3.2 Responsibilities

The **CIO** will contact the Governor's Office to provide status updates and will work with the Governor's Office and Attorney General to address any political or legal ramifications that may arise from the incident. Additionally, the CIO will contact agencies to discuss potential contingency plans.

The **CTO** will work with the CIO and agencies providing technical assistance in remediating issues caused by the incident(s).

The **CSO** will work with the CTO and assist with communications identifying issues and remediation efforts. The CSO is also responsible for the following:

- Incident Reports - The CSO will continue documenting and investigating incidents reported by SOM IT staff or other state employees.
- MS-ISAC Notifications – The CSO will contact the MS-ISAC as needed.
- Critical Systems Monitoring – The CSO will increase monitoring of the state's critical systems to ensure the cybersecurity event is not affecting their operational status.
- Coordinate an incident response within SOM IT agencies and other stakeholders.

- MSP MC3, MIOC, and EMHSD Notifications – If this is a new event, the CSO will notify MSP MC3, MIOC, and EMHSD appraising them of the situation and requesting assistance if needed.

SP SOCs will work with the CSO to identify and address potential cybersecurity incidents discovered by their security monitoring tools or reported to them by agencies, users, and citizens. SPs may also need to block IPs, DNS, and other potential attack vectors.

SOM IT will work with the CSO to identify the appropriate actions necessary to remediate the threat. Additionally, SOM IT will address:

- Security Monitoring Tools – SOM IT will report any anomalies to the CSO.
- Block IPs – SOM IT will identify and block Ips from which attacks are originating and work with BPs to identify and remediate the issue(s).
- Agency Alert Level – SOM IT will monitor the incident and adjust agency alert levels to properly match their readiness and remediation efforts.
- Communication – SOM IT will work with agencies, the CSO, the CIO, Provider Security Operations and Support (SOS), and their customers to identify and communicate information about the incident and remediation efforts.

Agencies should coordinate with **SPs and BPs** if assistance is needed in the remediation effort.

MSP MC3 will continue monitoring, information sharing, support, and investigative actions previously described in Section 4.1.

MSP EMHSD will continue previous actions, communications, and monitoring previously described in Section 4.2.

MSP MIOC, in conjunction with the MC3, will reach out to federal and local contacts to apprise them of the situation and to determine if the event is isolated or part of a larger attack. The MIOC will share intelligence related to the incident with the CDRT**.**

MING will work with the MSP MC3 and other partners to assist, as necessary. Michigan National Guard Cyber Teams (MI-NGCT) may be called upon to help with remediation efforts.

4.4 Cybersecurity Threat Level Severe (Red)

Threat Level Severe (Red) signifies confirmed cyber-attacks are disrupting federal, state, and local government communications; and/or unknown exploits have compromised state IT resources and are using them to propagate the attack or to spread misinformation. Malicious activity has been identified in state networks with a major level of damage or disruption. Examples include but are not limited to:

- Malicious activity impacting core infrastructure.
- A vulnerability is being exploited and there has been major impact.
- Data exposed with major impact.
- Multiple system compromises or compromises of critical infrastructure.
- Attackers have gained administrative privileges on compromised systems in multiple locations.

- Multiple damaging or disruptive malware infections.
- Mission critical application failures but no imminent impact on the health, safety, or economic security of the state.
- A distributed denial of service attack with major impact.

Actions:

- Continue recommended actions from previous levels.
- Contact the MSP MC3 for awareness and information sharing regarding potential threats and outreach to other entities for prevention purposes. The MC3 will take enforcement actions through investigation and criminal prosecution.
- Closely monitor security mechanisms including firewalls, web log files, antivirus gateways, and system log files for unusual activity.
- Consider limiting or shutting down less critical connections to external networks such as the Internet.
- Consider isolating less mission critical internal networks to contain or limit the potential of an incident.
- Consider use of alternate methods of communication per the CDRP Communication Methods (Annex A).
- When available, test and implement patches, antivirus updates, and other measures immediately.
- SEOC activation based on conditions. Voluntary resource collaboration between members, technical information sharing, and resource deployment based on mutual aid agreements. Could include financial considerations.

4.4.1 Potential Impact

- A critical vulnerability is being exploited and there has been significant impact.
- Telecommunications may be interrupted causing agencies to use alternate forms on communication.
- E-mail communications may be disrupted or untrusted making it necessary for agencies impacted by the event to use alternate forms of communication.
- Normal grid supplied power may become unreliable/unavailable for extended periods of time.
- Multiple damaging or disruptive virus attacks; and/or multiple denial of service attacks against critical infrastructure services.
- The issue can be remediated within five – ten business days and may require critical applications or services be taken offline until the issue can be remediated.
- The COOP/COG may need to be initiated to address the damages from the cyber-attack.
- The threat can only be remediated by restoring the applications and systems to an operational state by rebuilding equipment, restoring critical systems, or applications to a previous date before the attacks occurred.

4.4.2 Responsibilities

The **CIO** will contact the Office of the Governor to report on the severity of the situation. Additionally, the CIO will:

- Determine if COOP should be activated.
- Determine if the CIO should relocate staff to report to the SEOC for command, control, and communication purposes.
- Review contingency plans.
- Assist the Governor and cabinet members with:
    - Crafting sensitive communications to politicians, media, and other parties as required.
    - Contacting the State Budget Office (SBO) to obtain emergency funding to replace equipment and resources damaged or destroyed by the event.
- Designate team members to work with the CSO to remediate the issue(s).

The **CTO** will work with the CIO and SOM IT staff to coordinate the recovery process and to provide technical assistance in remediating issues caused by the incident(s). Additionally, the CTO will:

- Identify critical assets that have been damaged or destroyed by the incident and forward the information to the CIO to request emergency purchase.
- Ensure agency directors are briefed and begin preparing to assist with remediation efforts as necessary.

The **CSO** will assist the CIO and CTO with communications that identify the issues and remediation efforts. Additionally, the CSO will:

- Assist agencies with remediating the issues that are impacting their IT resources.
- Assist MSP EMHSD is establishing alternate forms of communications.
- Closely monitor security mechanisms, including firewalls, web log files, antivirus gateways and system log files, for unusual activity.
- Consider limiting or shutting down less critical connections to external networks such as the Internet.
- Consider isolating less mission critical internal networks to contain or limit the potential of an incident.
- Identify and address potential cybersecurity incidents discovered by security monitoring tools or reported to them by agencies, users, and citizens.
- Incident Response – Forward any cybersecurity related incidents reported to the SOC 24/7 Hotline (517-335-1722 or DTMB-MiSOC@michigan.gov).
- Enterprise Firewall Management – Identify and block IPs that are the origin of attacks.

Telecommunications Service Provider SOCs will work with the CSO to help identify issues, block firewall ports, and assist with remediation efforts. The Telecommunications Service Provider may also be called upon to work with the CSO to reroute network traffic to systems that are not impacted by the cyber-attack.

SOM IT will work with the CSO to identify and coordinate the appropriate actions necessary to remediate the threat. Additionally, SOM IT will:

- Security Monitoring Tools – SOM IT will report any anomalies to the CSO.

- Patch Management – SOM IT will work with the CSO to identify the proper application patches and ensure they are installed on servers that would be impacted by the threat.
- Agency Alert Level – SOM IT will monitor that incident and adjust their agency alert level to properly match their readiness and remediation efforts.
- Incident Reporting – SOM IT is responsible for reporting any incident that may come about during the remediation efforts or that may have caused the agency to raise its alert level.
- Communication – SOM IT will work with the CSO, CIO and their customers to identify and communicate information about the incident and remediation efforts.

Agencies should coordinate with **SPs and BPs** if assistance is needed in the remediation effort.

MSP EMHSD will continue previous actions, communications, and monitoring previously described in Section 4.2.

MSP MC3 will continue monitoring, information sharing, support, and investigative actions previously described in Section 4.1.

MSP MIOC will continue to communicate and share intelligence as previously described in Section 4.3.

MING will work with MSP MC3 and other state and federal partners to assist as necessary. MING may also:

- MING JOC may begin recall of Cyber Mission Forces as directed by the Adjutant General or other designated MING official.
- MI-NGCT may be called upon to assist with remediation efforts.

4.5 Cybersecurity Threat Level Emergency (Black)

Threat Level Emergency (Black) occurs when unknown vulnerabilities are being exploited causing widespread damage and disrupting critical IT infrastructure and assets. These attacks have an impact at the national, state, and local level. Malicious activity has been identified with a catastrophic level of damage or disruption. Examples include but are not limited to:

- Malicious activity resulting in widespread outages and/or complete network failures.
- Data exposure with severe impact.
- Significantly destructive compromises to systems, or disruptive activity with no known remedy.
- Mission critical application failures with imminent or demonstrated impact on the health, safety, or economic security of the state.
- Compromise or loss of administrative controls of critical system.
- Loss of critical Supervisory Control and Data Acquisition (SCADA) systems.

Actions:

- Continue recommended actions from previous levels.
- Activate the Michigan Cyber Civilian Corps (MiC3) to support response activities.

- Contact the MSP MC3 for awareness and information sharing regarding potential threats and outreach to other entities for prevention purposes. The MSP MC3 will take enforcement actions through investigation and criminal prosecution.
- Shutdown connections to the Internet and external business partners until appropriate corrective actions are taken.
- Isolate internal networks to contain or limit the damage or disruption.
- Use alternate methods of communication as needed.

4.5.1 Potential Impact

- Telecommunications may be unavailable making it necessary to use alternate forms of communication.
- The power grid may be unreliable causing agencies to rely on backup generators or uninterrupted power supply (UPS).
- Buildings may have been damaged or destroyed rendering IT resources inoperable.
- COOP may be implemented to restore IT operations.
- Datacenters have to be restored or relocated to alternate facilities.
- The issues will take over six business days to remediate and critical applications and services will be offline until the issues can be remediated.
- The threat can only be remediated by restoring the applications, systems, and facilities to an operational state by rebuilding equipment or restoring critical systems or applications to a previous date before the attacks occurred.

4.5.2 Responsibilities

The **CIO** will contact the Governor's Office to report of the severity of the situation. Additionally, the CIO will:

- Work with the Governor's Office and Attorney General to address any political or legal ramifications that may arise from the incident.
- Activate the COOP.
- Recommend relocation of appropriate Governor's Office staff to the SEOC for command, control, and communication purposes.
- Review contingency plans.
- Assist the Governor's Office and MSP EMHSD with crafting sensitive communications to politicians, media, etc.
- Assist the Governor's Office with contacting SBO to coordinate emergency funding to replace equipment and resources damaged or destroyed by the event.

The **CTO** will work with the CIO, SOM IT, and the Deputy State Director of MSP EMHSD to coordinate the recovery process and to provide technical assistance in remediating the issues caused by the incident(s). Additionally, the CTO will:

- Identify critical assets that have been damaged or destroyed by the incident and forward the information onto the CIO to request emergency purchase.
- Ensure that Agency Directors are briefed, and they prepare to assist remediation efforts.
- Establish networks and telecommunications to Governor's Office and state agency alternate facilities.

The **CSO** will activate the MiC3 and work with the CTO to assist with communications, identifying issues and remediation efforts. The CSO is also responsible for the following:

- Incident Reports – The CSO is responsible for documenting what occurred and providing the CTO with a post-mortem report.
- Assisting agencies with remediating the issues that are impacting IT resources.
- Shutting down connections to the Internet and external business partners until appropriate corrective actions are taken.
- Isolate internal networks to contain or limit damage or disruption.

Service Provider SOCs will participate on any conference calls that the CSO sets up. Additionally, they will advise the CSO of any information from its business partners that could help restore the state's infrastructure.

SOM IT will work with the CSO to identify necessary actions needed to remediate the threat. SOM IT will also help remediations efforts and report any incidents that may occur during remediation efforts or that may cause an agency to raise its alert level.

Agency representatives should coordinate with **BPs** if assistance is needed with remediation efforts.

MSP EMHSD, during SEOC activation, will maintain communications and coordination with federal and local contacts and continue previous actions, communications, and monitoring previously described in Section 4.2.

- The Director of MSP EMHSD will join the CIO and CTO at the SEOC or a designated recovery site.

MSP MC3 will continue monitoring, information sharing, support, and investigative actions previously described in Section 4.1.

MSP MIOC will continue to communicate and share intelligence as previously described in Section 4.3.

- The MIOC Director will join the CSO staff at the SEOC or designated recovery site.

The **MING** Cyber Operations Officer or Senior Cyber representative will join the staff at the SEOC or designated recovery site to help restore the state's critical infrastructure as directed by the Governor.

- MI-NGCT members will be activated as required to support operations.

MiC3 volunteers will report to CSO designated IT and EM functions to support response and remediation efforts.

5.0 Plan Maintenance

The State of Michigan Department of Technology, Management & Budget is 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.

6.0 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

Annex A: Communication Methods

<table>
<tr><th colspan="2">Primary Communication Methods</th></tr>
<tr><td>Cellular</td><td rowspan="3">This is day to day operational.</td></tr>
<tr><td>Landline / Voice Over Internet Protocol (VOIP)</td></tr>
<tr><td>Microsoft Teams</td></tr>
<tr><td colspan="2">Note: If the primary method of communications is not functioning move to the alternate methods.</td></tr>
<tr><th colspan="2">Alternate Communication Methods</th></tr>
<tr><td>GETS / WPS</td><td>Try using your GETS (landline) / WPS (cellular) cards by contacting your CDRT command structure, or MSP Operations (517-241-8000), or any other phone that is maintained 24/7 such as DTMB's Central Control (517-241-0191) located at the Joint Operation Center in Lansing. Ask if they are experiencing or are aware of any ongoing network communication outages.</td></tr>
<tr><td>Satellite Phone</td><td>If you have a satellite phone, try contacting your CDRT command structure or any other phone that is maintained 24/7 such as DTMB's Central Control (517-241-0191) located at the Joint Operation Center in Lansing. Ask if they are experiencing or are aware of any ongoing network communication outages.</td></tr>
<tr><td>Email</td><td>Try emailing supervision or peers. If unsuccessful, email DTMB-CentralControl@michigan.gov. Use "Status Check" as the subject header and annotate that you are only attempting to validate that email still works. Central Control is a 24/7 operation center, and you will receive a response.</td></tr>
<tr><td>HSIN</td><td>If you have a HSIN (Homeland Security Information Network) log-in ID, try logging in and validate if a room has been created. If one has, attempt to check in.</td></tr>
<tr><td>MI CIMS</td><td>If you have a MI CIMS log- in ID, try logging in and validate if an event has been created. If one has, attempt to view the SEOC activity log for updates.</td></tr>
<tr><td colspan="2">Note: If any of these means of communication are operational, notify your CDRT command structure and report your current limitations while advising what means you are currently operating on. If none of the primary and alternate methods are operational, move to the contingency methods of communication.</td></tr>
<tr><th colspan="2">Contingency Communication Method</th></tr>
<tr><td>In Person (Local)</td><td>Attempt to utilize communications through a local business that operates various communication pathways, such as a gas station. Notify your CDRT command structure and advise of your current location and outage limitations.</td></tr>
<tr><td colspan="2">Note: Before traveling and to gain situational awareness, check TV/Radio/Internet News/Weather Radio. If contingency communications are out, this may be a local issue to you. Move to the Emergency Communication Method.</td></tr>
</table>

Emergency Communication Methods	
In Person (MSP-HQ / SEOC)	Report to your designated workstation at MSP-HQ or the SEOC. Once the CDRT is onsite and gathered, a full communication assessment will take place and the emergency methods intended to be utilized will be determined, mobilized, and deployed.
Runners/Approved portable storage	The Emergency Support Function 2 (Communication Branch) will coordinate at the direction of CDRT Leadership.
800 MHz – See ICS 205 for talk groups	
AUXCOMM	
Private Partners (Verizon, ATT/FirstNet)	
Deployable (communication trailers, hotspots, etc.)	

Annex B: Training Resources

A variety of public and private organizations provide training pertaining to responding to a cyber event/disruption. 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, disaster recovery, NIMS, and ICS (www.training.DHS/FEMA.gov).
- *Cybersecurity and Infrastructure Security Agency (CISA)* offers a variety of in-person and online training courses on cybersecurity, cyber threats and advisories, information and communications security, and critical infrastructure security and resilience (www.cisa.gov)
- *National Institute of Standards and Technology (NIST)* offers guidance, sets benchmarks, and publishes documents related to information security, cyber security, and risk analysis (www.nist.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 (ICS2)* offers a number of training and certification (with concentrations) options including the industry leading Certified Information Systems Security Professional (CISSP) designation (www.isc2.org).
- *The Information Systems Audit and Control Association (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).

Annex C: Exercises

DTMB and MSP EMHSD work in close collaboration to leverage exercise planning and implementation expertise and methodology using the Homeland Security Exercise and Evaluation Program (HSEEP) framework. HSEEP ensures exercises and conducted according to a standard risk-based methodology applicable to all mission areas: prevention, protection, mitigation, response, and recovery. DTMB, MSP EMHSD, and subject matter experts will plan, develop, schedule, and execute cyber disruption scenarios.

Annex D: SEOC Activation Levels

STATE OF MICHIGAN

STATE EMERGENCY OPERATIONS CENTER

ACTIVATION LEVELS

	Level		Description	SEOC Staffing	Activities
	4	**Steady State Operations**	Routine operations	• None	• MSP/EMHSD Duty Officer monitoring all incidents • District Coordinators engaged locally
Activated	3	**Monitoring and Assessment**	Monitor ongoing incidents which could potentially result in local declarations and/or require state support	• SEOC Command & General Staff	• Operations takes over incident coordination • Monitoring MI CIMS for local incident details • District Coordinators engaged local EOC activities • Complete Situation Reports
Activated	2	**Partial Activation**	Support incidents where one or more jurisdictions request state support	• SEOC Command & General Staff • Specific state agencies, as determined by the incident	Same as Level 3, plus: • Monitor local requests for state resources • Provide state resources as requested and available • Develop an Incident Action Plan • Report agency activities
Activated	1	**Full Activation**	Support complex or large-scale incidents involving multiple jurisdictions requesting state support	• SEOC Command & General Staff • All or most state agencies	Same as Level 2, plus: • All or most state agencies activated
Activated	**	**Virtual**	Activation levels 1-3 may be done virtually or physically in the SEOC. This determination will be made by the SEOC Director.		

The State Emergency Operations Center's (SEOC) activation protocols and criteria are situation dependent and are influenced by multiple criteria. SEOC activation may also be in-person or virtual. During a CDRP incident, the SEOC may be activated to support coordination, response, and recovery efforts. The SEOC activation level will depend on multiple factors such as the size, scale, complexity and/or cascading impacts of an incident, and may not always mirror the CDRP Threat Level. The following CDRP Threat Levels may correspond to an SEOC activation:

- CDRP Threat Level Low: SEOC Activation Not Likely
- CDRP Threat Level Medium: SEOC Activation Depending on Conditions
- CDRP Threat Level High: SEOC Activation Depending on Conditions
- CDRP Threat Level Severe: SEOC Activation Probable
- CDRP Threat Level Emergency: SEOC Activation Probable

Annex E: Acronyms

BP	Business Partner
CDRP	Cyber Disruption Response Plan
CDRT	Cyber Disruption Response Team
CIO	Chief Information Officer
COG	Continuity of Government
COOP	Continuity of Operations Plan
CSO	Chief Security Officer
CTO	Chief Technology Officer
DNS	Domain Name System
DTMB	Department of Technology, Management & Budget
EM	Emergency Management
EMHSD	Emergency Management and Homeland Security Division
FBI	Federal Bureau of Investigation
HSEEP	Homeland Security Exercise and Evaluation Program
IAP	Incident Action Plan
ICS	Incident Command System
IOD	Intelligence Operations Division
IP	Internet Protocol
IT	Information Technology
JOC	Joint Operations Center
MI CIMS	Michigan Critical Incident Management System
MI-ISAC	Michigan-wide Information Sharing and Analysis Center
MING	Michigan National Guard
MI-NGCT	Michigan National Guard Cyber Teams
MIOC	Michigan Intelligence Operations Center
MC3	Michigan Cyber Command Center
MiC3	Michigan Cyber Civilian Corps
MS-ISAC	Multi-State Information Sharing and Analysis Center
MSP	Michigan State Police
NIMS	National Incident Management System
SBO	State Budget Office
SCADA	Supervisory Control and Data Acquisition
SEOC	State Emergency Operations Center
SOC	Security Operations Center
SOM	State of Michigan
SOS	Security Operations and Support
SP	Service Providers
UPS	Uninterrupted Power Supply