Cyber-Incident Response Annex

Annex Approval and Implementation

Wisconsin Emergency Management has coordinated an update to this of the Wisconsin Emergency Response Plan. This annex will be reviewed in accordance with the timeline outlined in the states Integrated Preparedness Plan (IPP). If needed, modifications to this annex will be coordinated with appropriate stakeholders and routed through the Adjutant General for approval.

DocuSigned by:
Greg Engle
C25970AA863F435...

Greg Engle, Administrator
Wisconsin Emergency Management

Date: 7/31/2024 | 3:00 PM CDT

This incident annex is hereby adopted as written and supersedes all previous versions.

Signed by:
Brig Gen David May
8FBC546B20CF4AA...

DAVID W. MAY, Brigadier General
Interim Adjutant General of Wisconsin

Date: 8/6/2024 | 3:03 PM CDT

Table of Contents

List of Tables

List of Figures

Intentionally left blank

Table 1-1: Coordinating and Support Agencies

Lead Coordinating Agencies	Department of Administration/Division of Enterprise Technology (DOA/DET) Department of Military Affairs/Wisconsin Emergency Management (DMA/WEM)
Wisconsin Governmental Support Agencies	Department of Military Affairs/Wisconsin National Guard (DMA/WING) Wisconsin Department of Justice/Wisconsin Statewide Intelligence Center (WI DOJ/WSIC)
Federal Coordinating Agencies	Cybersecurity and Infrastructure Security Administration (CISA) Federal Bureau of Investigation (FBI) US DHS/Secret Service (US SS) US Department of Defense (DOD)

1. Introduction

1.1 General

1.1.1 The state's essential and emergency services, as well as its critical infrastructure, rely on the uninterrupted use of the internet and communications systems, including data, monitoring, and control systems.

1.1.2 Wisconsin faces an evolving array of intentional or unintentional cyber-based threats. Unintentional threats can be caused by software upgrades or defective equipment that inadvertently disrupts systems. Intentional threats can be both targeted and untargeted attacks by criminal groups, hackers, terrorists, organization insiders, and foreign nations engaged in crime, political activism, or espionage and information warfare.

1.1.3 Protecting against cyber-attacks is complicated by the fact that attackers do not need to be physically close to their targets and can easily remain anonymous, among other things. The magnitude of the threat is compounded by the ever-increasing sophistication of cyber-incident techniques, such as incidents that combine multiple techniques.

1.1.4 Given the interconnected nature of computer networks, responding to cyber threats is a shared responsibility by the whole community. Collaboration, communication, and engagement between the public and private sectors and across state, local, and tribal jurisdictions is essential to detect and identify, protect against, respond to, and recover from cyber-incidents.

1.1.5 Many elements of cyber-incident response are similar to other types of natural or technological emergencies. Wisconsin's approach to cyber-incident response is consistent with an all-hazards approach by integrating and building upon the all-hazards response capabilities already in place.

1.2 Purpose

1.2.1 This annex provides a scalable, flexible framework for responding to, and recovering from a cyber-incident by:

1.2.1.1 Identifying roles, responsibilities, and actions required to respond to a significant cyber incident.

1.2.1.2 Organizing cybersecurity efforts among public and private critical infrastructure sectors.

1.2.1.3 Describing the coordination structure that integrates the Homeland Security Council Cybersecurity Subcommittee (HSC/CY), and the Wisconsin Cyber Response Management Group (CRMG).

1.2.1.4 Establishing a framework for cybersecurity information sharing as well as effective and resilient communications systems and protocols to ensure continuity of communications during and after cybersecurity events.

1.2.1.5 Providing information to counties, tribes, and local units of government regarding available state assets and resources.

1.3 Scope

1.3.1 This annex describes the framework for coordination and execution within which state agencies:

1.3.1.1 Respond to incidents affecting state data systems and networks.

1.3.1.2 Assist local and tribal units of government in a cyber-related incident, as required by §323.01 of the Wisconsin Statutes.

1.3.1.3 Advise or assist public and private sector partners during cyber incidents including critical infrastructure.

1.3.2 The annex is not intended to supersede or replace state agency plans and procedures. Users are responsible for being familiar with and implementing their agency's standing plans and procedures.

1.3.3 The annex is a strategic plan for operational coordination and execution among state, local, and tribal (SLT) governments, the public/private sector, and other partners. It describes authorities, capabilities, and processes that can be utilized to enable response, and recovery in the cyber domains. Although steady-state activities and the development of a cyber common operational picture are key components of this annex, the plan focuses primarily on building the mechanisms needed to coordinate intra-Wisconsin resources.

1.3.4 This annex is intended to be scalable, ensuring a unified and coordinated response to any cyber-incident, including a significant cyber incident (SCI). A significant cyber-

incident as defined by Presidential Policy Directive 41 (PPD 41) "is one that either singularly or as part of a group of related incidents is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people." **For the purpose of this annex, a Cybersecurity Threat Level 3 – Medium (Yellow) or higher is an SCI within Wisconsin.** The incident may not meet the criteria of a federal definition but still meet the conditions requiring a state coordinated response.

1.3.5 This annex takes a whole-community approach. It encompasses both the state of Wisconsin, as a government enterprise (to include local units of government and tribes), and critical infrastructure partners critical to the protection of the health, safety, and economic vitality of the lives, organizations, and business in the state of Wisconsin. In all cases, cyber-incident response activities will be conducted in accordance with applicable laws, regulations, and policies. Nothing in this annex restricts, supersedes, or otherwise replaces the legal authorities or regulatory responsibilities of any government agency or organization. All information will be handled, transmitted, distributed, released, and stored in accordance with the standards, caveats, and procedures described by the originating agency, regulatory governance, and law.

1.3.6 This annex describes thresholds between each level of the Cyber Severity Schema (see Table 3-1). Subsequently, the plan describes when the CRMG convenes and how their actions guide the remainder of the response. The CRMG does not take the place of Wisconsin Emergency Management (WEM) in response to natural disasters. They assist WEM with planning during cyber-incidents. The plan is applicable whether a physical event causes a cyber incident or the other way around.

1.3.7 The annex is intended to develop broad concepts focused on Wisconsin's interface with federal agencies including but not limited to:

1.3.7.1 The Cybersecurity and Infrastructure Security Administration's (CISA) National Cybersecurity and Communications Integration Center's (NCCIC).

1.3.7.2 Department of Defense (DOD) Cyber Crime Center (DC3) and US Cyber Command.

1.3.7.3 Federal Bureau of Investigation (FBI)

1.3.7.4 US DHS/Secret Service (USSS).

1.3.8 For the purposes of this annex, see the following definitions.

1.3.8.1 'Cyber' refers to the relationship between computer hardware and software including electronic tablets, smartphones, and other similar devices as well as the interconnections between them for the collection, electronic storage, and dissemination of information.

1.3.8.2 'Cyberspace' means the electronic environment for information transfer including public and private local and wide area networks and the internet.

1.3.8.3 'Cyber-incident' means an occurrence related to computers, servers, controls, electronic files, email systems, software, networks, or the internet requiring a response to protect life, property, the environment, or the economy.

1.3.8.4 The 'Cyber-environment' includes all physical and virtual assets in cyberspace.

1.3.8.5 'Cyber-threat' means the intent to, or possibility of, a malicious attempt to damage or disrupt computer equipment or networks, or exfiltrate electronic information at rest or in transit for nefarious purposes.

1.3.8.6 'Cyber-critical infrastructure' means physical or virtual systems and assets vital to Wisconsin which, if incapacitated or destroyed, would have a debilitating impact on Wisconsin's safety, security, economy, public health, or any combination of those matters.

2. Assumptions

2.1 Vulnerability and Risk

2.1.1 The cause of a cyber-related threat or incident may be natural, technological, or human-caused or evolve from an ongoing physical-world incident.

2.1.2 Cyber-assets in both the public and private sectors in Wisconsin are vulnerable to a range of threats - from hardware and software failures, to attacks by criminals, terrorists, or nation state actors as an act of war. For a better understanding of vulnerability and its relationship to the range of cyber threats and potential impacts in Wisconsin, refer to the discussion on the Cyber Incident Severity Schema (Section 3.4).

2.1.3 Cyber incidents may be a single element of a larger incident. Activities conducted pursuant to this annex 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). Detailed tribal, state, and local operational and strategic plans will support this annex.

2.1.4 Each vulnerability imposes a degree of organizational risk. Managing these risks is the responsibility of government, non-government, and private sector organizations, all of which must understand the likelihood of an identified risk leading to an incident and the likely impacts of that incident. With that knowledge, organizations can establish their level of risk tolerance.

2.1.5 Tools and operations in the effort to establish a secure cyber-environment include:

2.1.5.1 Equipment: including network protection, intrusion detection, and encryption technologies.

2.1.5.2 Planning: including developing and implementing a written and socialized comprehensive cyber-security approach. Plans should be reviewed and updated periodically to address new technologies and vulnerabilities.

2.1.5.3 Training: including programs that expand the whole community's knowledge of cyber-threats and security measures.

2.1.5.4 Process Documentation for:

(1) Incident reporting

(2) Incident assessment and escalation

(3) Incident response

(4) Documentation and metrics

2.1.6 Network risk tolerance, mitigation, and defense include:

2.1.6.1 Identification by State Agencies and organizations of critical operations and systems.

2.1.6.2 At the executive level, IT system owners evaluate vulnerabilities within their systems; determine the level of risk each imposes, and the organization's level of risk tolerance.

2.1.6.3 Information technology managers evaluate and assign financial and other available resources to mitigate and protect against system risks in accordance with the organization's established risk tolerance.

2.1.6.4 Operations level personnel implement mitigation and protective actions to defend the network against intrusion and disruption.

2.2 Authorities

2.2.1 *Lead agency in a cyber-incident:* In accordance with Section §323.12(3) of the Wisconsin Statutes, WEM serves as the lead coordinating agency during a state of emergency declared by the Governor. However, in a cyber or telecommunications-related incident, the Governor may designate the Department of Administration (DOA) as the lead agency in accordance with §323.10 of the Wisconsin Statutes.

2.2.2 In accordance with 2019 Executive Order #6, the Wisconsin Homeland Security Council advises the Governor and coordinates the efforts of state and local officials with regard to prevention of, and response to, potential threats to the homeland security of Wisconsin. The Chair of the Wisconsin Homeland Security Council serves as lead advisor for cybersecurity matters throughout the state of Wisconsin.

2.3 Policies

2.3.1 Incident Command System (ICS): Section §323.13(1)(b) of the Wisconsin Statutes requires that ICS training be implemented to manage emergency incidents. Therefore, the

Incident Command System shall be included in training for the management of any cyber related incident.

2.3.2 Public (and private sectors) should incorporate cybersecurity into all aspects of emergency management and continuity of operations (COOP) and continuity of government (COG) plans.

2.3.3 The ReadyWisconsin website will serve as the state's public-facing outlet, providing information on cyber security and threats to that security.

2.3.4 State network administrators are responsible for ensuring the cyber-hygiene in the wisconsin.gov and other state agency domains. Cyber-hygiene involves five key processes:

2.3.4.1 **Count:** Knowledge of the cyber-environment. Conduct an inventory of network-connected hardware and software to better assess vulnerabilities.

2.3.4.2 **Configure:** Secure the cyber-environment. Assure all network-connected computers have common security settings that protect the state's cyber-domains.

2.3.4.3 **Control:** Manage administrative privileges. Limit authority to add software, modify configurations, and add devices to the state network.

2.3.4.4 **Patch:** Protect the cyber-environment. Provide routine and verifiable security settings that are kept current.

2.3.4.5 **Repeat:** Monitor the cyber-environment and assure policies and procedures are enforced.

2.3.5 Consistent with the National Response Framework, a response to a cyber-threat or incident should be scalable, flexible, and adaptable. In general, each threat or incident should be addressed at the lowest jurisdictional level possible consistent with an effective response. However, unlike most incidents, the cyber-incident may originate at the state level, or may simultaneously occur at multiple levels of government. This requires additional flexibility to the initial response to the incident.

2.3.6 State and local government agencies (as well as private sector entities) should collaborate and share existing cyber-response capability for potential use in a declared state of emergency by the Governor.

3. Concept of Operations

3.1 Cyber Watch and Warning Organizations – Incident Reporting and Detection

3.1.1 Due to the pervasive nature of a cyber threat, initial identification of the threat may be through a variety of channels. Wisconsin maintains five primary watch and warning centers that monitor and share information in the event of a cyber-threat or attack.

Incident information will be shared with the Adjutant General and other agency senior leadership as necessary.

3.1.2 Wisconsin National Guard Joint Operation Center (WI-JOC): The WI-JOC serves as the focal point for Wisconsin National Guard (WING) domestic operations by maintaining a 24-hour DO system to receive reports from individuals, state agencies, local units of government, tribal, and the private sector through a public facing toll-free telephone number. The JOC provides situational awareness via a common operational picture (COP), serving as a centralized communications and coordination node, and providing a command-and-control platform for contingency response operations. The WI-JOC is manned 24/7, 365 days a year.

3.1.2.1 The WI-JOC gathers and shares information through Situational Reports to WING, WEM, and Public/Private Partners to ensure their situational awareness and facilitate effective decision-making. When notified of a cyber-threat or incident, the JOC notifies the WEM Administrator and follows established Cyber Response Team Request SOG.

3.1.3 Wisconsin Department of Justice (WI DOJ)/Wisconsin Statewide Intelligence Center (WSIC): As Wisconsin's primary fusion center, WSIC works in partnership with the US Department of Homeland Security (US DHS) and the Federal Bureau of Investigation (FBI), as well as partners from other federal, state, local, tribal agencies, and the private sector to gather information and produce intelligence products for federal, state, local, tribal government agencies, the private sector, and the public. The WSIC is available at 608.242.5393 and wsic@doj.state.wi.us.

3.1.3.1 In response to the emerging threats from cyber intrusions and associated disruptions, the WSIC has taken on roles and responsibilities in gathering, receiving, analyzing, and disseminating cyber threat information. The WSIC gathers cyber threat information through partnerships with the private sector as well as state, tribal, and local agencies.

3.1.3.2 The WSIC Cyber, Fusion, and Threat Liaison Officer programs are statewide initiatives to work with federal, state, tribal, local agencies, and the private sector to provide training and serve as a mechanism for the liaison officers to submit suspicious activity reports (SARs) to WSIC in order to detect, prevent, and respond to both criminal and terrorism-related activities.

3.1.3.3 WSIC disseminates cyber threat information through its robust distribution network. Intelligence is disseminated both for situational awareness and for specific threats to critical infrastructure. Through the implementation of the governance authority of this strategy, WSIC will utilize the subject matter experts or "authorized agents" identified for each of the critical infrastructure sectors to disseminate cyber threat intelligence.

3.1.4 Department of Administration, Division of Enterprise Technology - Enterprise Service Desk (DET ESD): The DET ESD monitors the state cyber-domain on a 24-hour basis for threats or incidents using a variety of automated systems. DET ESD notifies the state Chief Information Security Officer (CISO) of any detected or suspected threat or attack against state information technology assets. DET ESD is available at 608-264-9383 and at esdhelp@wisconsin.gov.

3.1.5 Department of Military Affairs (DMA) Cybersecurity Operations: The Directorate has two full-time cyber intelligence analysts, who work directly with National Guard cyber operational elements, WSIC, and the Cyber Response Team Program (CRT) to assist in monitoring threat reports, providing situational awareness to the command group, information sharing across entities, and maintaining the COP during a cyber event.

3.2 Wisconsin Cyber-Incident Annex Triggers

3.2.1 Cyber-related mitigation and preparedness activities are ongoing functions that routinely occur as part of the steady-state operations. See the Wisconsin Prevention and Protection Plan for additional details.

3.2.2 Conditions that may trigger the incident response functions of this annex include:

3.2.2.1 An incident involving activation of state level continuity of operations (COOP) or continuity of government (COG) plans.

3.2.2.2 When requested by:

(1) A local or tribal unit of government.

(2) DOA management (CIO/CISO).

(3) DMA management.

(4) A critical infrastructure provider.

3.2.2.3 When directed by:

(1) The DET CISO up to cybersecurity threat level 2 – Low (Green).

(2) The Adjutant General at cybersecurity threat level 3 – Medium (Yellow).

3.3 Organization

3.3.1 Agency and entity roles and responsibilities in a cyber-incident:

3.3.1.1 End Use (Client): Individual system owners are responsible for training their users in proper and appropriate uses of equipment, software, and networks. In a cyber-attack, system owners bear ultimate responsibility for equipment and network incident and loss or exfiltration of data involving their computers, servers, and networks.

3.3.1.2 Service Provider: Internet service providers and other vendors of computer and network services are responsible for securing the domains and services they host or provide.

3.3.1.3 Local, State, and Federal Law Enforcement Agencies:

(1) Law enforcement: Police and sheriffs' departments, along with WI DOJ and federal law enforcement agencies, investigate cyber-crime and refer cases for prosecution. These agencies also pass on information on the mechanisms used to disrupt or infiltrate victim networks to assist owners with securing their systems.

3.3.1.4 State agencies:

(1) DOA/WEM: At the state level, WEM operates the SEOC and coordinates state agency incident response. During a state of emergency declared by the Governor involving a cyber-incident, DMA is the lead agency unless the Governor appoints DOA as the lead agency under Wisconsin Statutes §323.10.

(2) DMA/WEM directs and manages deployment of Cyber Response Teams to support affected entities. The Cybersecurity Preparedness Coordinator serves as the CRT Lead.

(3) WI DOJ/WSIC: The Wisconsin Statewide Intelligence Center (WI DOJ/WSIC) coordinates information sharing among federal, state, local, and tribal government agencies, the private sector, and the US Intelligence Community.

(4) DMA/WING: The J6 is part of the Joint Staff and provides direct support to the Defensive Cyber Operations Element (DCO-E) for administrative, training, and readiness.

3.3.1.5 Federal agencies:

(1) U.S. DHS and CISA: The Department of Homeland Security is the principal federal agency for domestic incident management. Through the National Cybersecurity and Communications Integration Center (NCCIC), CISA coordinates cyber response to national level significant cyber-incidents and integrates information sharing between federal, state, tribal, local governments, and the private sector.

(2) US DOJ/FBI: The DOJ, through the FBI & National Cyber Investigative Joint Task Force (NCIJTF) serves as the lead federal agency for threat response activities during significant cyber incidents IAW PPD-41.

(3) DOD: The Department of Defense is the lead federal agency for responding to acts of war. Table 3-2: Cyber-Incident Roles and Responsibilities illustrates agency roles and responsibilities across a range of cyber-incidents.

3.3.1.6 MS-ISAC: The mission of the MS-ISAC is to improve the overall cybersecurity posture of the nation's state, local, tribal, and territorial governments through focused cyber threat prevention, protection, response, and recovery.

3.3.1.7 Further organizational responsibilities are outlined in Section 3.5 "Management and Operations."

3.4 Cyber Incident Severity Determination

3.4.1 Per Presidential Policy Directive 41 (PPD-41), the US federal cybersecurity centers, in coordination with departments and agencies with a cybersecurity or cyber operations mission, adopted a common schema for describing the severity of cyber-incidents affecting the homeland, US capabilities, or US interests. The schema (see Table 3-1) establishes a common framework to evaluate and assess cyber-incidents to ensure that departments and agencies have a common view of the:

3.4.1.1 Severity of a given incident

3.4.1.2 Urgency required for responding to a given incident

3.4.1.3 Seniority level necessary for coordinating response efforts

3.4.1.4 Level of investment required of response efforts

3.4.2 State threat level considerations:

3.4.2.1 Whenever the federal government increases or decreases the cyber security threat level for the nation, it is expected that Wisconsin will align its response posture to match the federal government.

3.4.2.2 However, Wisconsin will also conduct its own assessment of the cybersecurity threat posed within the state and may increase or decrease the state's cybersecurity threat level independent of the federal government's assessment.

3.4.2.3 Increasing the cyber security threat level up to level 2 is at the direction of the DET Administrator.

3.4.2.4 Increasing the cyber security threat level above level 2 is at the direction of the Chair of the Homeland Security Council.

3.4.2.5 Decreasing the cyber security threat level is conducted at the discretion of the elevation authority for that level. Note: The Chair of the Homeland Security Council may lower the cybersecurity threat level to level 1 at his or her discretion.

Table 3-1: Key Elements of the Cyber Severity Schema

Level	General Definition	Observed Actions	Intended Consequence	Primary Operational Coordination
Level 6 Emergency (Black)	Poses an imminent threat to the provision of wide-scale critical infrastructure services, national government stability, or the lives of US persons.	Effect	Cause physical consequence Damage computer and networking hardware Corrupt or destroy data	SEOC
Level 5 Severe (Red)	Likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties.	Effect	Deny availability to a key system or service Steal sensitive information Commit a financial crime Nuisance Denial of Service (DoS) or defacement	SEOC
Level 4 High (Orange)	Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.			CRMG or SEOC (if SEOC is elevated)
Level 3 Medium (Yellow)	May impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence	Presence		CRMG or SEOC (if SEOC is elevated)
Level 2 Low (Green)	Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	Engagement Preparation		CRMG

Level	General Definition	Observed Actions	Intended Consequence	Primary Operational Coordination
Level 1 Baseline (Minor) (Blue)	Highly unlikely to affect public health or safety, State security, economic security, civil liberties, or public confidence.	Observation		CRMG
Level 0 Baseline (White)	Unsubstantiated or inconsequential event.	Observation		CRMG

3.5 Management and Operations – Cybersecurity Incident Response

3.5.1 Cyber Response Management Group (CRMG) –The CRMG is an incident response element. Depending on the characteristics of the cyber event, the team may consist of personnel from HSC/CY, DET, WSIC, WEM, WING, federal agencies, other state, local, and tribal personnel, and owners of impacted systems. Members of the team are cyber security subject matter experts responsible for incident response and analysis, knowledge sharing, and providing intelligence assessments to senior leaders. The team will conduct ongoing assessments of the incident and complete the Severity Schema. In addition, the CRMG makes recommendations in response to significant cyber-incidents.

3.5.1.1 When a cybersecurity incident occurs which affects either state, local, tribal (SLT) systems or public/private critical infrastructure in Wisconsin beyond the capabilities or scope of the CRT, the CRMG will convene with DOA as the lead agency. The cybersecurity response effort will be led by the State CISO and DMA Cybersecurity Operations Lead.

3.5.1.2 Cybersecurity Incident Severity Level Determination: The State CISO and DMA Cybersecurity Operations Lead assess the severity of reported cybersecurity incidents using the Cyber-Incident Severity Schema. If the incident may affect public safety or continuity of government, the State CISO and DMA Cybersecurity Operations Lead will brief the HSC/CY, which includes the DET CIO / CISO and TAG. TAG and the DET Administrator may adjust the Cybersecurity Threat Level in accordance with Section 3.4.2.

3.5.1.3 During cybersecurity incidents that may impact public safety, the CRMG may expand to include senior level executives that manage and coordinate both a unified command group for cybersecurity incident response and the SEOC manager. The CRMG typically includes members of the HSC/CY, CRT, DOA, and DMA. It may also include senior leaders and personnel from other State Agencies as required.

3.5.1.4 The CRMG communicates with the Governor's office and the HSC-CY. As necessary, TAG may delegate coordination of briefings to the Wisconsin Homeland Security Council to CRMG members as necessary.

3.5.2 TAG: TAG is the Governors' senior state official for cybersecurity matters and coordinates cybersecurity response efforts with CISA and other federal agencies when required. TAG is the state's primary point-of-contact (POC) for the NCICC. The DET Administrator is the state's alternate POC for the NCICC. Additional POCs have also been identified to ensure continuous contact with the NCICC.

3.5.3 Wisconsin Homeland Security Council Cybersecurity Subcommittee (HSC/CY) – This subcommittee is made up of 10 members from state education, emergency

management, elections commission, tribal, and business representation. It is responsible for:

- Identifying, prioritizing, and mitigating the state's cyber risk
- Developing plans to better identify, respond to, and recover from cyber attacks
- Making cybersecurity recommendations
- Sharing information among stakeholders
- Recommending education and training programs to bolster the cybersecurity workforce

3.5.4 Wisconsin Cyber Strategy and Planning Working Group (WCSPWG) – This working group is comprised of subject matter experts from the public and private sector responsible for advising on preparation, response to, and recovery from large-scale or long-duration cyber incidents impacting Wisconsin's critical infrastructure or other major assets. This working group conducts routine, monthly sessions. They are responsible for continuing broad analysis of existing cyber response plans, risk assessments, and knowledge sharing between and among members. During an incident, members of this group may be included in the CRMG.

3.5.5 Cyber Response Team Program (CRT) - The State of Wisconsin has facilitated the establishment of a CRT. The DMA Cybersecurity Preparedness Coordinator is responsible for training, certification, proficiency standards, validation criteria, and preparedness activities to maintain readiness. The CRT incorporates FEMA standards for team membership.

3.5.5.1 The team is comprised of cyber experts from the SLTT governments, critical infrastructure (public and private) organizations and managed by the DMA/WEM.

3.5.5.2 Table 3-2 outlines the US Department of Homeland Security critical infrastructure sectors and aligns them with State of Wisconsin government agencies. These agencies, along with public/private sector partners, participate in the CRT. They focus most of their efforts on pre-incident planning. The critical infrastructure sectors in bold are referred to as the Lifeline Sectors. These sectors will help to: 1) establish decision points mapped to the lifecycle of an event; and 2) determine the threat level, action plan, and resource allocation from a large-scale or long-duration cyber incident that affects the state.

3.5.6 Wisconsin National Guard (WING) Defensive Cyber Operations Element (DCO-E) - The WING trains and certifies a DCO-E. This team is comprised of approximately 10 Guardsmen that can provide support to mission partner networks in State Active Duty (SAD), under applicable laws and regulatory parameters.

The Wisconsin National Guard also fields three 7-person teams as members of the Wisconsin-Illinois National Guard Cyber Protection Teams (CPT). The teams are able to provide support to civil authorities in accordance with the existing Defense Support of Civil Authorities (DSCA) policy and practice.

Table 3-2: Agencies Representing the US DHS Critical Infrastructure Sectors

Critical Infrastructure Sector	WI State Agency	Federal
Agriculture and Food	DATCP	USDA/HHS
Financial Services	**DFI**	**Treasury**
Chemical	DATCP/DMA	US DHS
Commercial Facilities	DATCP/DMA	US DHS
Communications	**DOA/DMA**	**US DHS**
Critical Manufacturing	DATCP	US DHS
Dams	DNR	US DHS
Defense Industrial Base	DATCP/DMA	DOD
Emergency Services	DMA	US DHS
Energy	**PSC**	**Energy**
Government Facilities (including elections)	DOA, WEC, DPI	ICE/FPS
Healthcare and Public Health	DHS	HHS
Information Technology	DOA	US DHS
Nuclear Reactors, Materials and Waste	PSC	US DHS
Transportation Systems	**DOT**	**USCG**
Water and Wastewater Systems	**DNR**	**EPA**

Note: Sectors in **Bold** are key sectors in a cyber incident and include the lifeline sectors.

3.5.7 Whole Community Information Sharing – Cybersecurity incident information is shared using appropriate pathways to protect sensitive information and ensure actionable information reaches appropriate partners.

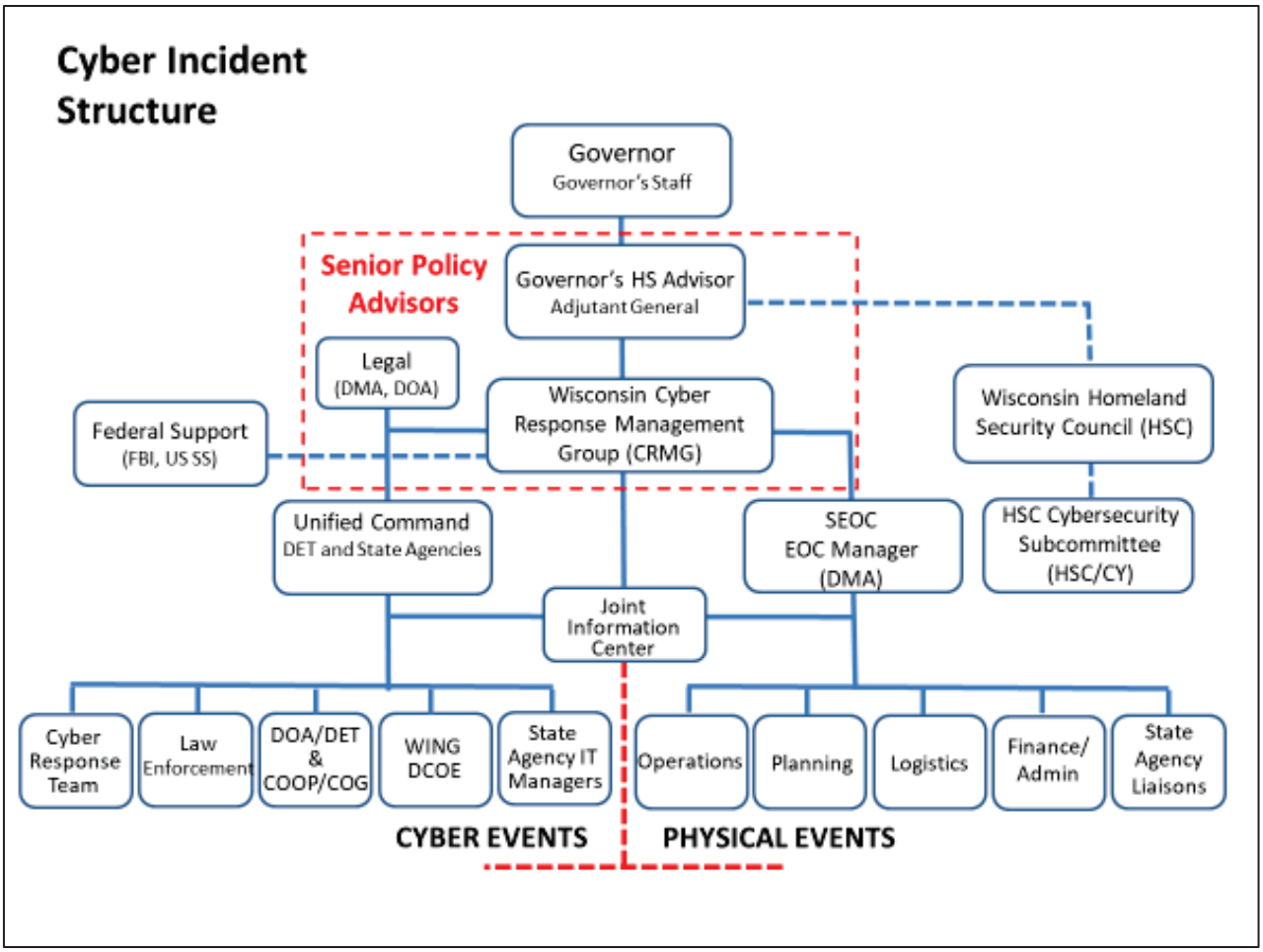
3.5.7.1 The WSIC, as the state intelligence coordinating and analysis center, shares incident information with affected state level agencies and with US DHS and federal law enforcement. WSIC acts as the clearinghouse and analysis center for cyber-intelligence products in Wisconsin, with input from DOA, private sector cyber-intelligence and defense assets, law enforcement, and other intelligence sources, including the public.

3.5.7.2 DOA and WEM public information officers form a Joint Information Center (JIC) in accordance with Emergency Support Function (ESF)-15 Attachment 1 for sharing incident-related information with the public. The Lead PIO function will be fulfilled by the lead agency in the incident.

3.5.7.3 Since a cyber-incident may cause significant effects to physical assets, the organizational structure may include resources involved in response to and recovery from those effects. Wisconsin Statutes Chapter 323 tasks local units of government with the responsibility to respond to incidents in their jurisdictions. The SEOC may elevate to coordinate state agency support to local and tribal government in accordance with ESF-5 'Emergency Management' as directed by TAG. The SEOC will share relevant response information with tribal and local units of government so they can maintain situational awareness and scale their own response efforts if needed.

3.5.8 Cybersecurity Information Sharing: Organizations that specialize in cybersecurity incident response utilize a variety of platforms to share sensitive incident information. All stakeholders must ensure information is safeguarded in accordance with applicable laws and agreements. Specific information about platforms utilized to share information by state agencies may be found in the Cyber Response Team Operations Plan.

Figure 3-1: Cybersecurity-Incident Response Structure



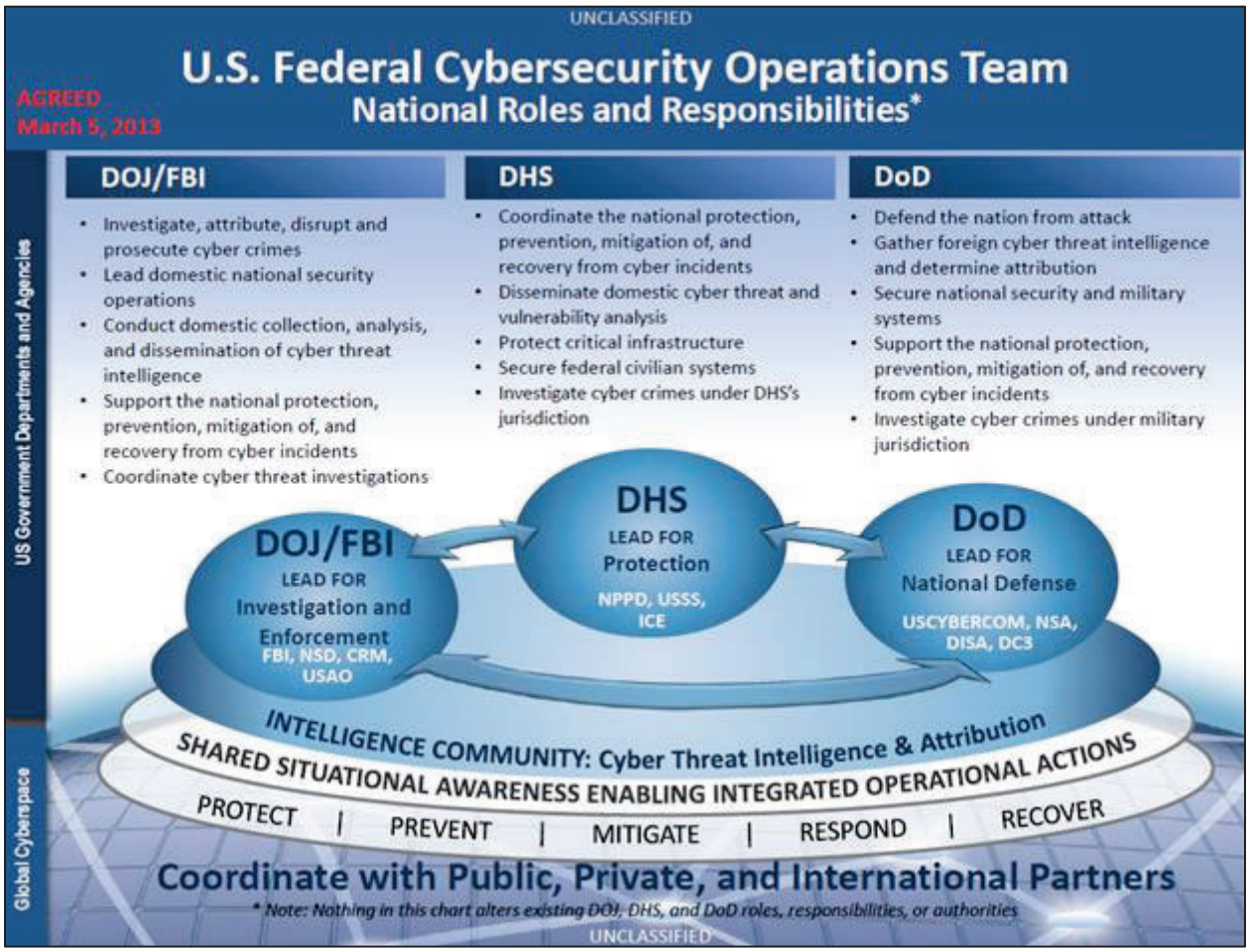
3.5.9 Incorporating Federal Response Assets – Various federal government entities possess different roles, responsibilities, authorities, and capabilities (Figure 3-2) that can be brought to bear on cyber-incidents. These entities coordinate with state and local governments as well as private-sector entities to generate optimal results.

3.5.9.1 The State's Fusion Centers (Southeastern Wisconsin Threat Analysis Center and WSIC) regularly collaborate with federal law enforcement agencies to share information and, when necessary, respond to cyber-incidents.

3.5.9.2 All lead coordinating agencies and governmental support agencies included in this plan coordinate with the U.S. Department of Homeland Security and its subordinate agencies, FBI and other federal entities. These agencies often participate in protection, mitigation, and recovery activities with federal partners as well.

3.5.9.3 Requests for federal assistance during a cyber-incident are coordinated through the CRMG, TAG, or the Governor's Authorized Representative.

Figure 3-2: Coordination of Cyber-Incident Management at Federal Level



3.5.10 Tables 3-3 to 3-9 (on the following pages) shows the Cybersecurity Threat Levels and the involvement of supporting agencies at each level.

Table 3-3: Cybersecurity Threat Level 0 and Corresponding Command and Control Actions

Cybersecurity Threat Level 0 – Baseline (White)		
Definition: Standard IT defensive measures are in place and active measures such as scanning, patching, and hygiene activities are conducted as a matter of standard operations. Regular or low levels of scanning, probes, etc. activity are occurring. Warnings, alerts, and indicators received and processed as a matter of routine. **Resulting affects:** No risks are expected. No special events mandating the rise to a higher level. **Communications Procedures:** Standard day-to-day coordination.		
Phase	**Action Item**	**Agency**
Cybersecurity Threat Level 0 – Baseline (White)	• Not convened at this level.	Cyber Response Management Group (CRMG)
	• Conduct routine, monthly sessions. • Continue broad analysis of existing cyber preparedness and response plans, risk assessments, and knowledge sharing between and among members. • A portion of a team may conduct training and advise or assist in assessing an agency's security program.	Cyber Response Team Program (CRT)
	• Provide direction and priorities to the State of Wisconsin IT enterprise; may select special focus on specific malicious threats or request the WCSPWG convene to discuss impacts of the emerging threats. • Continue to provide direction and priorities to the State of Wisconsin IT security enterprise and agency CISOs • Notify appropriate agencies of significant identified vulnerabilities.	State CISO
	• Coordinate and manage the volunteer, administrative, and program functions of the CRT. • Integrate cybersecurity preparedness activities as an All-Hazards preparedness line of effort to SLTT partners.	WEM
	• Continue broad surveillance of cyber threat spectrum and receive updates or information from deployed WI Cyber Response Team assets. • Explore significant or potential indicators of compromise that may indicate a broadening of the threat and provide analysis of potential future targets. • Notify WEM, WING, and DET of any potential for cybersecurity threat level increase. • Pass requests for CRT assistance to the JOC.	WSIC
	• Provide regular and recurring updates about homeland security-related events. • The JOC routinely monitors emails and calls. • The JOC reports any cyber-incident activity to the CRMG, per established Standard Operating Guidelines (SOG). • Log requests for CRT Assistance per established SOG.	DMA/WI-JOC
	• Pass requests for CRT assistance to CRT Preparedness	DMA Cybersecurity

	Coordinator (or designee). • Convene CRMG as necessary to assess and respond to reported cybersecurity incidents.	Operations

Table 3-4: Cybersecurity Threat Level 1 and Corresponding Command and Control Actions

Cybersecurity Threat Level 1 – Baseline-Minor (Blue)

Definition: An unsubstantiated event/malicious activity with an unknown impact that is occurring or has occurred. The incident is highly unlikely to affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence. The potential for impact, however, exists and warrants additional scrutiny.

Resulting effects: Unknown to minimal risks are expected. Minor special events mandating the rise to a higher level.

- Unknown to minor changes to normal activity occurred or are occurring.
- Warnings, alerts, and indicators received.
- Services impacted by slow down or unresponsiveness
- Potential malware compromise of a non-critical system, but no further noticed action occurred.

Communications Procedures: An affected entity, county EM, or WEM Regional Director notifies the JOC DO or respective agency intake officer. The intake officer or JOC will notify DMA Cybersecurity Operations and provide affected entity's callback information. DMA Cybersecurity Operations will notify appropriate CRMG personnel and the CRMG will contact the affected entity to assess incident severity and determine initial response actions. If email is down, alternate means will be used to notify the appropriate personnel. All communications procedures follow established protocols on existing systems

Note: *All Level 0 procedures are continued at Level 1. Items listed below are additional activities relevant to Cybersecurity Threat Level 1 (Baseline-Minor)*

Phase	Action Item	Agency
Cybersecurity Threat Level 1 –Baseline-Minor (Blue)	• Convene to assess incident severity and determine initial response. • Contact affected entity to remediate.	CRMG
	• Continue all Level 0 activities. • CRT Lead may direct the deployment of a WI Cyber Response Team to the affected entity. • A portion of a team may activate to conduct initial liaison to investigate an incident. • Assist affected entities with remediation of cybersecurity incidents. • Pass forensic evidence to WI DOJ. If there is any criminal activity suspected, notification of WSIC is mandatory.	CRT
	• Continue all Level 0 activities. • Notify Multi-State Information Sharing and Analysis Center (MS-ISAC) of the event. • Update National Cybersecurity and Communications Integration Center (US NCCIC) status map.	State CISO
	• Continue all Level 0 activities. • May notify WEM regional directors and affected tribal or	WEM

	county emergency managers if appropriate.	
	• Continue all Level 0 activities. • Participate in CRMG calls as necessary. • Pass relevant information about the incident to mission partners as applicable (example: indicators of compromise).	WSIC
	• Continue all Level 0 activities. • Monitor deployment of WI Cyber Response Team assets in state.	DMA/WI-JOC
	• Continue all Level 0 activities. • Work with CISO to determine appropriate response to the cybersecurity incident (technical assistance, monitor, remediation, etc.) • Convene CRMG. • May assist CRT for LNO duties or initial outreach. • DCO-E may provide support to mission partner networks.	DMA Cybersecurity Operations

Table 3-5: Cybersecurity Threat Level 2 and Corresponding Command and Control Actions

Cybersecurity Threat Level 2 – Low (Green)

Definition: A substantiated event/malicious activity with minor impact that is occurring or has occurred. The event is unlikely to affect public health or safety, economic security, or civil liberties. Affected entities can manage the event with possible consulting/advising by supporting agencies and that agency is capable of remediation. Limited contact with Liaison Officers or deployment of response assets to networks or systems suspected of having been successfully targeted or exploited may occur.

Resulting Effects:

- Minor changes to normal activity occurred or are occurring – vulnerability is being exploited with limited affect.
- Credible warnings, alerts, and indicators received.
- Malware compromised a non-critical system, but no further action occurred.
- A limited scope/duration denial of service attack occurred with minor impact.

Communication Procedures: Level 2 communications procedures are nearly identical to previous levels, however, CRTs and CRMG personnel may utilize additional communication methods to pass sensitive information, files, logs, etc. to appropriate parties. For more information, see the Cyber Response Team Operational Plan.

Note: *All Level 0 and Level 1 procedures are continued at Level 2. Items listed below are additional activities relevant to Cybersecurity Threat Level 2 (Low)*

Phase	Action Item	Agency
Cybersecurity Threat Level 2 – Low (Green)	• Continue activities from previous levels. • May support the affected entity directly or through technical assistance if requested. • May request additional personnel to participate in the CRMG.	CRMG
	• Continue activities from previous levels.	CRT
	• Continue activities from previous levels. • Assess potential impacts to State of Wisconsin IT enterprise.	State CISO
	• Continue activities from previous levels. • WEM DO: Pass any additional information received regarding the incident in subsequent reporting to DMA Cybersecurity Operations.	WEM
	• Continue activities from previous levels.	WSIC
	• Continue activities from previous levels. • Track for potential future inclusion in the WI User Defined Operating Picture (UDOP).	DMA/WI-JOC
	• Continue activities from previous levels.	DMA Cybersecurity Operations

Table 3-6: Cybersecurity Threat Level 3 and Corresponding Command and Control Actions

Cybersecurity Threat Level 3 – Medium (Yellow)		
Definition: Event may affect public health or safety, economic security, and civil liberties. Agencies have identified malicious activity with a minimal level of damage to information systems or disruption across one or more agencies. One to three days are required for recovery actions and systems may need to be taken offline for this period. **Resulting Effects:** • Exploit conducted with moderate level of success. • Compromise of secure system(s). • Data spillage/Doxing. • Attackers appear to have gained administrative privileges. • A virus or worm is spreading quickly through public and/or private networks. • Distributed Denial of Service (DDOS) attack with long lasting effects. **Communications Procedures:** Conference calls and email remain the primary communications tools. RAVE alerts are used to convene the Cyber Response Management Group, including senior leadership (TAG, DET Administrator, WEM Administrator, WSIC Special Agent in Charge, etc.) An operational rhythm of regular calls or briefings is established to maintain situational awareness during the incident. A WebEOC site may be opened depending on the nature of the incident. Alternative secure communications platforms may be used to pass sensitive information.		
Phase	**Action Item**	**Agency**
Cybersecurity Threat Level 3 – Medium (Yellow)	• Determine whether an emergency declaration is necessary. • May direct the deployment of appropriate state assets to support the affected entity.	TAG
	• Continue activities from previous levels. • Convenes immediately via conference call to discuss incident response, information gaps, etc. • Determine if virtual or physical meeting are most feasible.	CRMG
	• Continue activities from previous levels. • All team members are alerted and may activate to conduct initial liaison to investigate a threat in a government or private sector entity.	CRT
	• Continue activities from previous levels. • Ensure agency CISOs successfully complete remediation activities if needed.	State CISO
	• Continue activities from previous levels. • May activate SEOC and sustain level of activation commensurate with level of physical effects and disruption. • WEM DO continue activities from previous levels • May create an incident site in Web EOC to document the lifecycle of the incident. • The DO (or SEOC staff) receives and monitors potential deployments of WI Cyber Response Team assets.	WEM

	• Prepares to support affected agency with COOP efforts, if needed. • May convene the Business EOC to assist with response to any physical impacts and/or share information. • May notify FEMA Region 5 Regional Response Coordinating Center. • May establish common operating picture for consequence management.	
	• Continue activities from previous levels. • Notify state partner agencies per SOP.	WSIC
	• Continue activities from previous levels. • Plan mission support package in line with expected needs to remedy the situation.	DMA/WI-JOC
	• Continue activities from previous levels. • Establish CRMG conference call with appropriate members via RAVE Alert.	DMA Cybersecurity Operations

Table 3-7: Cybersecurity Threat Level 4 and Corresponding Command and Control Actions

Cybersecurity Threat Level 4 – High (Orange)		
Definition: Likely to result in demonstrable impact to public health and safety, economic security or civil liberties of WI citizens and business. Malicious activity is identified with a moderate level of damage or disruption. Physical effects of disruption to critical infrastructure or lifeline sectors. Escalation to Level 4 is likely if cyber-incident effects manifest in physical effects with any critical infrastructure sector. **Resulting Effects:** • Malicious activity results in widespread outages or complete network failures. • Data exposure with severe or highly sensitive impact. • Significantly destructive compromises to systems or disruptive activity with no known remedy. • Mission critical application failures with imminent impact on the health, safety, or economic security of the state. • Compromise or loss of administrative controls of critical system(s). • Loss of critical supervisory control and data acquisition (SCADA) systems. **Communications Procedures:** Communications at Level 4 are identical to those used at Level 3.		
Phase	**Action Item**	**Agency**
Cybersecurity Threat Level 4 – High (Orange)	• Continue activities from previous levels. • Meet to ascertain boundaries of the event and proscribe immediate actions based on size and scope.	CRMG
	• Continue activities from previous levels.	CRT
	• Continue activities from previous levels. • May direct an LNO to report to the SEOC. • Determine whether to initiate COOP measures for DET.	State CISO
	• Continue activities from previous levels. • Creates a Web EOC incident site to document the incident lifecycle. • May request an LNO from CRT and/or WSIC to report to the SEOC. • Establish common operating picture for consequence management.	WEM
	• Continue activities from previous levels.	WSIC
	• Continue activities from previous levels.	DMA/WI-JOC
	• Continue activities from previous levels. • Begin assessment of sustained prolonged operations.	DMA Cybersecurity Operations

Table 3-8: Cybersecurity Threat Level 5 and Corresponding Command and Control Actions

Cybersecurity Threat Level 5 – Severe (Red)

Definition: An event likely to result in a significant impact to public health or safety, economic security, or civil liberties of WI citizens. Malicious activity is identified with a severe level of damage or disruption. Physical effects of disruption to critical infrastructure or lifeline sectors occur.

Resulting affects:

- Malicious activity results in widespread outages or complete network failures.
- Data exposure with severe or highly sensitive impact.
- Significantly destructive compromises to systems, or disruptive activity with no known remedy.
- Mission critical application failures with imminent impact on the health, safety, or economic security of the state.
- Compromise or loss of administrative controls of critical system(s).
- Loss of critical supervisory control and data acquisition (SCADA) system(s).

Communications Procedures: Conference calls and email remain the primary communications tools (If available). RAVE alerts are used to convene the CRMG. An operational rhythm of regular calls or briefings is established to maintain situational awareness during the course of the incident. A WebEOC site will be opened to share consequence management information and process resource requests. Alternate communication methods, i.e., satellite phones, cell phones, and radios, will be used if internet systems are unavailable or untrusted. Alternative secure communications platforms may be used to pass sensitive information.

Phase	Action Item	Agency
Cybersecurity Threat Level 5 – Severe (Red)	• Continue activities from previous levels. • Determine necessity of future meetings or recurrence of meetings.	CRMG
	• Continue activities from previous levels.	CRT
	• Continue activities from previous levels. • Will direct an LNO to serve as part of the SEOC.	State CISO
	• Continue activities from previous levels. • Maintain level of SEOC activation commensurate with level of physical effects and disruption.	WEM
	• Continue activities from previous levels.	WSIC
	• Continue activities from previous levels.	DMA/WI-JOC
	• Continue activities from previous levels.	DMA Cybersecurity Operations

Table 3-9: Cybersecurity Threat Level 6 and Corresponding Command and Control Actions

Cybersecurity Threat Level 6 – Emergency (Black)

Definition: An event likely to result in a significant impact to public health or safety, economic security, or civil liberties of WI citizens. Malicious activity is identified with a catastrophic level of damage or disruption. Widespread physical effects of disruption to critical infrastructure or lifeline sectors occur.

Resulting affects:

- Malicious activity results in widespread outages or complete network failures.
- Data exposure with severe or highly sensitive impact.
- Significantly destructive compromises to systems, or disruptive activity with no known remedy.
- Mission critical application failures with imminent 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.

Communications Procedures: Conference calls and email remain the primary communications tools (If available). RAVE alerts are used to convene the CRMG. An operational rhythm of regular calls or briefings is established to maintain situational awareness during the course of the incident. A WebEOC site will be opened to share consequence management information and process resource requests. A HSIN connect site may also be established to share sensitive information. Alternate communication methods, i.e., satellite phones, cell phones, and radios, will be used if internet systems are unavailable or untrusted.

Phase	Action Item	Agency
Cybersecurity Threat Level 6 – Emergency (Black)	• Continue activities from previous levels. • Meet on a recurring basis to provide input to the CRMG based on the event/incident.	CRMG
	• Continue activities from previous levels.	CRT
	• Continue activities from previous levels. • Act as LNO to NCCIC to coordinate national response.	State CISO
	• Continue activities from previous levels.	WEM
	• Continue activities from previous levels.	WSIC
	• Continue activities from previous levels.	DMA/WI-JOC
	• Continue activities from previous levels.	DMA Cybersecurity Operations

3.6 Communications

3.6.1 Prompt notification of key personnel in a cyber-threat or incident is critical. Each agency with a role in a cyber-incident response shall identify key personnel and a means to rapidly alert them.

3.6.2 A cyber-incident may rapidly spread across public and private sector networks spanning geographic and political jurisdictional boundaries. Significant cyber-incidents may quickly require state or national coordinated response actions.

3.6.3 Decision-makers must have reliable and readily available communications resources to coordinate a cyber-incident response. ESF-2 *Communications* addresses emergency communications, and a list of communications resources is maintained by DMA/WEM.

3.6.4 All communications during any cyber-incident will be sent through designated channels and personnel.

3.6.5 Backup Communications: Many communications modes are dependent on the cyberspace environment and may be subject to disruption in a cyber-incident. The WEM Communications Office can provide information on alternative communication resources.

In the event of degraded communications, intermittent or untrustworthy communications, severe communications disruption, or lack of contingency communications, the SEOC functions as the primary operations center for directing physical recovery efforts and hosting the CRMG. The Femrite Data Center serves as a secondary option for coordinating a response to a cyber incident. An alternate site for the SEOC is Camp Williams at Volk Field, Wisconsin. The alternate site is designated for exceptional circumstances wherein the state or nation is under widespread emergency conditions and the Madison metro area must be evacuated.

3.6.5.1 When required or as mandated by an authorized agent or body, WISCOM may serve as the primary out-of-band communications between affected cyber nodes, key cyber facilities, and command post locations. The talk group would be determined at the time of the incident. The SEOC serves as the net control station. Repositioning of mobile or deployable communications may be initiated to provide needed emergency communications for response actions.

3.6.6 Key Information Systems: Regardless of the level of the incident, gaining and maintaining situational awareness, especially for senior state leaders is vital. Additional key information systems or platforms that assist coordination and response include:

3.6.6.1 WEM's Emergency Management Software System: Regardless of the event escalation and its resulting effects, WI maintains awareness through WEM's emergency management portal - WebEOC. During a cyber incident, WebEOC will be used to process resource requests, develop a common operating picture, and handle consequence management.

3.6.6.2 The Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC) uses an integrated system-of-systems that delivers a range of capabilities, including intrusion detection, analytics, intrusion prevention, and information sharing. This system, Communications and Cyber Common Operating Picture (DHS CCOP) (UNCLASSIFIED and CLASSIFIED), is a new and maturing capability. For the state, the JOC has primary responsibility to monitor the CCOP and use its data to inform leadership and the CRMG of developing cyber-incidents. The JOC is the primary contributor for the state with events WI will submit to the CCOP, upon leadership clearance.

(1) Events submitted to the CCOP face a further review at the national level. While all reported events are tracked, all may not be reflected back onto the CCOP (this is at the discretion of the DIR NCCIC). Events are added to the DHS CCOP at all levels of the incident, however, in the first two levels, the affected entity determines whether the event is posted to the CCOP. When events in WI reach levels 3-6, event listing is mandatory.

3.6.7 Public Answering Centers: Answering centers (9-1-1 Call Centers), in addition to social media, often facilitate the first reports of physical effects of cyber incidents on our citizens and businesses.

3.6.7.1 Each call center is responsible to develop and maintain its own policies on reporting cyber-incidents. These policies should, however, include notification to the Cyber Watch and Warning Organizations listed in Section 3.1.

3.7 Other Agency Plans and Documents

3.7.1 National Cyber Incident Response Plan, December 2016

3.7.2 Presidential Policy Directive/PPD-41 – United States Cyber Incident Coordination

3.7.3 WI Cyber Disruption Response Strategy, October 30, 2015.

3.7.4 Framework of Improving Critical Infrastructure Cybersecurity, Version 1.1, National Institute of Standards and Technology. April 16, 2018.

3.7.5 Army National Guard, Defensive Cyberspace Operations Element Concept of Operations (CONOP), July 2019.

3.7.6 Wisconsin Cyber Strategy and Planning Working Group Charter, January 2016.

3.7.7 Cybersecurity Subcommittee Approval, June 2021.

3.7.8 Cybersecurity Subcommittee Charter, June 2021.

3.7.9 Cyber Response Team Operational Plan.

Table 3-10: Record of Changes

#	Date	Agency/Individual	Change
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			
18.			

Intentionally left blank