Montana Emergency Support Function #16 - Cybersecurity

Primary Agency:

Montana Department of Administration

(Month)XXXX

Maintained by Department of Military Affairs
Disaster and Emergency Services Division

*This Annex is considered operational and serves as a guide for rendering assistance whenever the **Montana Emergency Response Framework** (MERF) is activated. It supersedes all previous editions.*

DRAFT – Not ready for distribution

Record of Changes

All changes to this plan annex are to be dated on the master copy kept by the Montana Disaster & Emergency Services (DES).

Date Posted	**Change**	**Recommending Agency/Individual**

Table of Contents

Section I: Agencies

Coordinating Agency: Montana Disaster & Emergency Services	***Support Agencies:*** Department of Justice Department of Military Affairs
Primary Agency: Montana Department of Administration	

Section II: Purpose & Scope

Purpose:

ESF #16 – Cybersecurity, describes how the State of Montana (through the integration of response and recovery efforts with public and private sector cybersecurity practitioners across Montana) will coordinate plans, procedures, and resources to support the state in protecting, stabilizing, and reestablishing the cyber infrastructure threatened by natural or human-caused emergencies. The 16 critical infrastructure sectors identified by the Department of Homeland Security are heavily dependent upon the cybersecurity infrastructure – whose assets, systems, and networks are considered so vital to the United States that its incapacitation or destruction would have a debilitating effect on security, economic security, public health or safety or any combination thereof. This Annex will facilitate, coordinate, and support the following core functions of the ESF:

- Refining inter-agency and cross-sector information coordination, encouraging information sharing, and performing threat analysis.
- Establishing and maintaining the Core Security Incident Response Team to identify, detect, protect, respond to, and recover from cyber incidents.
- Implementation of the statewide cybersecurity plan which advances Montana's cyber capabilities.

Scope:

ESF #16 describes the organizational framework for support and coordination among the Montana ESF primary and support agencies for cybersecurity incident coordination including cyber terrorism, cyber incidents involving critical infrastructure information systems, technological emergencies, or other emergencies or disasters with impacts on information technology (IT) capabilities or secure data and privacy information in the State of Montana. Montana ESF primary and support agencies coordinate in accordance with relevant statutory and regulatory authorities to work together to protect life and property and coordinate with state and local departments and agencies during response, but do not supersede the authority of these entities. In select cases, there may be a need to address disruptions, damages, and/or failure from cybersecurity incidents outside the state that affects communities in Montana as many critical infrastructure systems are interconnected with other states and Canada.

All agencies and private-sector partners retain all specific responsibilities accorded to them by statute, regulation, policy, or custom. This document does not supersede or override the policies or mutual aid and assistance agreements of any local and tribal jurisdiction, government, or agency. This document does not define or supplant any emergency operating procedures or responsibilities for any other agency or organization.

The activities within the scope of this document include the following:

- Coordinating pre-cybersecurity incident management planning and actions to assist in the prevention or mitigation of cyber threats and hazards.
- Leverage the statewide cybersecurity incident response reporting process and the monthly sharing of cyber threat information and industry best practices to all of Montana's governments, critical infrastructure, and small businesses.
- Monitor and coordinate cybersecurity incident response for state, federal, and private sector partners impacted or potentially impacted by a cybersecurity incident that requires the activation of the SECC.
- Support and coordinate situational awareness and information sharing among primary and support agencies identified within this annex relating to cybersecurity incidents.
- Provide technical assistance on potential impacts to cybersecurity infrastructure in the event of a non-cyber specific event.
- Develops and maintains a cyber common operating picture with Federal, state, and industry partners.
- Develops cyber restoration priorities during disasters.

Section III: Assumptions & Relationships

Assumptions

For the purpose of designing responses in a cybersecurity threat environment, this annex outlines the following assumptions:

- Cybersecurity incident-caused disruption, damages, and/or failure of statewide critical infrastructure systems and services can occur at any time and any location and may create significant degrees of human suffering, property damage, and economic hardship.
- Cybersecurity incidents will not always unfold in a well-defined and predictable manner.
- In the early stages of a cybersecurity incident, it might not be possible to fully assess the situation and verify the level of coordination and assistance required.
- Not all tribal nations, counties, critical infrastructure owners/operators, and private businesses have cybersecurity emergency plans.
- Not all tribal nations, counties, critical infrastructure owners/operators, and private businesses cybersecurity plans are up to date or adequate.
- Local plans align with state plans, which in turn align with federal plans, in particular in the utilization of the National Incident Management System (NIMS).
- When requested, coordinate state response at the local level to provide support until their resources are exhausted.
- Tribal nations, counties, critical infrastructure owners/operators, and private businesses cybersecurity practitioners will initially employ their own emergency plans until resource shortages overwhelm their functionality.
- Critical infrastructure owners/operators and private businesses will request assistance or resources through local incident management or their local disaster and emergency services representative.

- During severe cybersecurity incident caused disruption, damages, and/or failure of statewide critical infrastructure systems and services that potentially impact community lifelines, the cybersecurity workforce in Montana may not meet the needs of communities, critical infrastructure owners/operators, and private businesses.
- Cybersecurity resource shortages are projected during response and recovery efforts.
- The State of Montana may be unable to satisfy all emergency resource requests during cybersecurity incident caused disruption, damages, and/or failure of statewide critical infrastructure systems.

Relationships

This document does not relieve tasked agencies with the responsibility for emergency planning. The following section outlines the relationships between state agencies and local, tribal, private, and non-governmental organization cybersecurity practitioners in supporting ESF #16 response and recovery activities:

<u>Local & Tribal Governments</u>

Local and tribal governments typically have close collaborative relationships with cybersecurity practitioners in their respective jurisdictions. Increasingly, businesses and critical infrastructure sectors essential for maintaining and stabilizing community lifelines are represented at Emergency Operations Centers (EOC) operated by the government providing situational awareness to neighboring, state, and federal emergency management officials. These collaborative relationships provide the foundation for coordinating cybersecurity operations between public and private entities and enabling readiness through multi-sector planning and exercises that are supported, as appropriate, by State agencies.

At the local and tribal levels, information sharing and requests for assistance from the private sector are typically reviewed by impacted jurisdictions or within EOCs. Local and tribal government partners should collaborate with their private sector partners to collect, assess, prioritize, and support private sector requirements, consistent with applicable laws and regulations. If local and tribal support assets are inadequate for meeting requests for assistance to stabilize community lifelines, the local emergency management entity will forward requests to the State Emergency Coordination Center (SECC).

<u>Private Sector/Non-Governmental Organizations</u>

The private sector plays a leading role in designing and executing the coordination functions and other priorities of private-public collaboration. The private sector includes for-profit and nonprofit organizations, formal and informal structures, commerce, and industries that comprise the national economy and are not part of a government structure. Nongovernmental organizations (NGO) are a distinct category of organizations within the private sector and can include voluntary, ethnic, faith-based, veteran-based, disability, relief agency, and animal welfare organizations, among others.

A growing number of infrastructure owners and operators are developing cybersecurity plans and coordination mechanisms to provide voluntary, prioritized, and public-private sector support. Businesses and utilities (private and public) are also collaborating with companies that provide supplies and services critical to their emergency operations and are developing cybersecurity plans to help those supply chains function in severe cybersecurity incidents. Taken together, these advances provide rapidly expanding opportunities for public-private sector coordination.

State Government

State departments and agencies are responsible, within their statutory authorities, for providing assistance to local jurisdictions when local capabilities are overwhelmed by a disaster. The State Emergency Coordination Center (SECC) serves as the principal point for coordinating state, local, tribal, and federal resources in the coordination of emergency assistance to affected jurisdiction(s).

The SECC will coordinate with the primary agency and support agencies in the use of state resources to support ESF #16 response activities. State resources will supplement, not supplant, local resources. When activated to respond to an incident, the primary agency and support agencies will develop work priorities in cooperation with local and tribal governments and in coordination with the SECC.

If the Governor has declared an emergency, resources may be requested through the Emergency Management Assistance Compact (EMAC), the nation's state-to-state mutual aid system that is processed through the SECC.

Section IV: Core Capabilities

The following table lists the core capabilities and their key activities that the coordinating, primary, and supporting agencies within all MERF ESFs collectively support. Though not listed in the table, all ESFs, including ESF #16, support the core capabilities of Planning, Operational Coordination, and Public Information and Warning.

CORE CAPABILITIES	**Key Activities –** The SECC coordinates with the primary agency and supporting agencies to coordinate resources in support and response for the following key activities during actual or potential incidents:
Planning	• Provide over-arching ESF coordination with the Regional Emergency Operations Centers (REOCs)/SOC, Joint Field Office (JFO), and other emergency functions. • Coordinate during cyber incidents impacting GIS, the situational awareness and information sharing system, and other forms of response technology. • Coordinate the collection of status information for all technology-based systems, devices, and connections affected by, or affecting the response to, a cyber incident. • Provide state and local leadership with current status of all technology-based systems, devices, and connections consistently throughout a cyber incident.
Public Information & Warning	• Coordinate the content and release of security notifications to the public and receiving information from Public Information Officers through Cal OES Office of Crisis Communications and Media Relations and Technology Agency's Public Information Officer.
Critical Transportation	• Provide status of all primary and alternate cyber controls and components in Transportation affected by, or affecting response to, cyber incidents. • Coordinate during cyber incidents impacting traffic monitoring systems, industrial control systems, and geographic information systems (GIS).

	• Conduct global positioning system (GPS) tracking and monitoring of sensitive cargo, such as radiological materials or railway fuels
Environmental Response / Health and Safety	• Coordinate during cyber incidents impacting the equipment that monitors and releases hazardous materials, controlled by industrial control systems.
Infrastructure Systems	• Coordinate during cyber incidents impacting industrial control systems that support critical infrastructure. • Coordinate during cyber incidents impacting manufacturing equipment and other industrial control systems used in food and agriculture.
On-Scene Security, Protection & Law Enforcement	• Coordinate investigation, forensics, and arrest related to cyber incidents and request federal assistance when needed.
Operational Communications	• Provide status of all primary and alternate communications affected by, or affecting response to, cyber incidents. • Provide alternate communications during potential cyber incidents impacting GIS and digital communications.
Logistics & Supply Chain Management	• Coordinate locating alternate data processing repositories, cloud site(s), and incident reporting to facilitate and support successful data processing from an alternate location during a cyber-event.
Public Health, Healthcare, & Emergency Medical Services	• Coordinate during cyber incidents impacting public health and medical functions including, but not limited to, emergency management, healthcare facility durable equipment/infrastructure, food/drug, and radiological/nuclear systems.
On Scene Security, Protection, & Law Enforcement	• Coordinate investigation, forensics, and arrest related to cyber incidents. • Request federal assistance when needed.
Operational Communications	• Provide status of all primary and alternate communications affected by, or affecting response to, cyber incidents. • Provide alternate communications during potential cyber incidents impacting GIS and digital communications.
Public Health, Healthcare, and Emergency Medical Services	• Coordinate during cyber incidents impacting public health and medical functions including, but not limited to, emergency management, healthcare facility durable equipment and infrastructure, food and drug, and radiological systems.
Situational Assessment	• Facilitates a shared understanding of interdependencies, impacts, and opportunities for cybersecurity incident stabilization. • Enables synchronization of Requests for Information (RFIs), Critical Information Requirements (CIRs), and data sharing.

Section V: Operational Functions

The following table lists the operational functions of the ESFs in support of incident caused disruption, damages, and/or failure of statewide critical infrastructure systems and services response and recovery activities:

Primary Agency	**Operational Functions –** Department of Administration serves as the primary agency. The operational functions for the primary agency may include the following:
Department of Administration	**Director's Office** • The Director's Office directs, oversees, and ensures a heightened level of service in the continuance and implementation of all programs during an incident, emergency, or disaster. **State Information Technology Services Division** • Provides information technology services to more than 100 government customers and is responsible for maintaining and structuring critical technological and telecommunications systems to provide information to internal and external partners. • Directs and monitors security requirements for all state-owned information technology. • Establishes and maintains the Information Systems Incident Response Team (ISIRT). • Maintains and ensures coordination of radio frequencies within the state. • Information Technology Division personnel are trained in restoration and repair of information technology resources.
SUPPORTING AGENCIES	**Operational Functions –** The operational functions for the support agencies may include the following:
Montana Department of Military Affairs	**Army and Air National Guard** *Upon approval by the Governor:* • Can offer cybersecurity technicians. • State, Tribal and Local Governments may request ANG assistance through the Disaster Emergency Services (DES) Duty Officer. **Disaster & Emergency Services** • Coordinates National Guard assistance, when requested and upon approval by the Governor. • Coordinates and/or deploys personnel to fill positions in operations centers and on emergency response teams and other entities as necessary. • Coordinate emergency-related response and recovery functions related to ESF #16 mission. • Provides assistance in the allocation and prioritization of cybersecurity resources. • Coordinates the prevention, protection, mitigation, response, and recovery actions among cybersecurity infrastructure practitioners at state and local levels. • Coordinates and/or provides situational awareness regarding cybersecurity infrastructure. • Coordinates EMAC, Federal, International, and domestic offers of technician assistance and support for cybersecurity.

	- Coordinates state emergency planning activities that include immediate, short-term, and long-term strategic planning for cybersecurity.
Department of Justice	**Highway Patrol Division** - Leads efforts to protect communications infrastructure from the effects of acts of terrorism and support efforts to protect communications infrastructure from the effects of manmade disasters. - Initiates and conducts investigations involving allegations of critical infrastructure cybercrime. **Montana Analysis & Technical Information (MATIC)** - Designated by the Governor as the fusion center in Montana. - A focal point for the collection, analysis, and dissemination of public safety and threat related information for the purposes of decision making for local, state, federal, and tribal partners while ensuring the rights and privacy of citizens. - Provides relevant information on criminal activity and credible threats that could potentially threaten public safety and critical infrastructure security to appropriate partners.
Available and Qualified State Agency IT Personnel	- State Information Technology personnel who are available and trained in assisting SITSD in restoration and repair of information technology resources when requested.