

Wyoming Office of Homeland Security (WOHS)



Mikki Munson

**State of Wyoming
Critical Infrastructure Protection & Resiliency
Program Manager**

Wyoming office of Homeland Security (WOHS)

<https://hls.wyo.gov/home>

WOHS Mission Statement



**Preparing
Wyoming to
respond to and
recover from
all-hazards**

The Primary Missions Of The Wyoming Office of Homeland Security

Our Mission:

Preparing Wyoming to respond to and recover from all hazards

- Protect, prevent, mitigate, respond to and recover from natural/manmade disasters to include adversarial and technological hazards;
- Manage and administer federal homeland security and emergency preparedness grants. These grants provide necessary funding to the first responder community to enhance the capacity of state and local agencies to respond to disasters/terrorism through the following:
 - Planning
 - Organization
 - Equipment
 - Training
 - Exercises

The Primary Missions Of The Wyoming Office of Homeland Security

Our Mission:

Preparing Wyoming to respond to and recover from all hazards

- Coordinate state agencies and appropriate federal agencies during a disaster, terrorist attack, cyber events, and threats against critical infrastructure
- Conduct public education and outreach to inform the public about their role in crime prevention, mitigation, emergency preparedness for all hazards, public health measures and to encourage personal responsibility
- Support Search and Rescue operations including the administration of the Search and Rescue account; and
- Facilitate chemical, biological, radiological, nuclear and explosive response activations to incidents utilizing eight Regional Emergency Response Teams, seven bomb teams and eight canine teams strategically located throughout the state

Primary List of Programs Provided to Wyoming Residents

















- Community Resilience
- Grants-SHSP, EMPG, NSGP, HMEP, and HMA
- Regional Emergency Response Teams (RERT)
- Improvised Explosive Device Program
- Interoperable Communications
- Information Sharing- WISP and HSIN
- Exercises and Planning
- **Critical Infrastructure**
 - **Physical Security Assessments**
 - **Cyber Assistance Response Effort (CARE)**
- Public alerts - Integrated Public Alert and Warning Systems

Critical Infrastructure Protection (CIP)

- Work with the Protective Security Advisor on Site Assessments
- Work with your Emergency Manager on ICS classes, exercises, and assistance in completing your ERP
- Emergency Alerts, threats, and advisory Bulletins

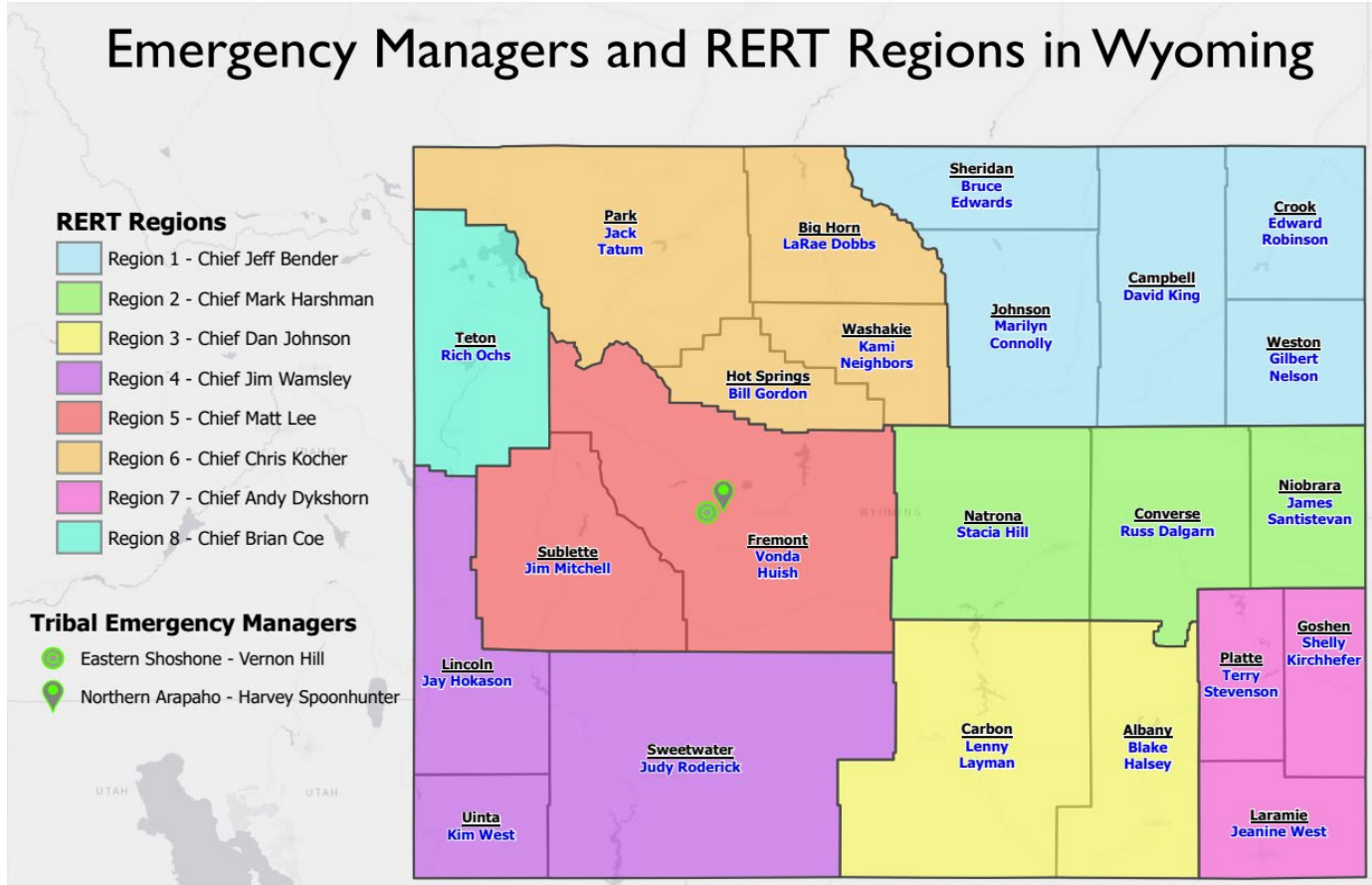
MS-ISAC and Health-ISAC
(Information Sharing and Analysis Center)

16 Critical Infrastructure Sectors & Corresponding Sector-Specific Agencies

 CHEMICAL	DHS (CISA)	 FINANCIAL	Treasury
 COMMERCIAL FACILITIES	DHS (CISA)	 FOOD & AGRICULTURE	USDA & HHS
 COMMUNICATIONS	DHS (CISA)	 GOVERNMENT FACILITIES	GSA & DHS (FPS)
 CRITICAL MANUFACTURING	DHS (CISA)	 HEALTHCARE & PUBLIC HEALTH	HHS
 DAMS	DHS (CISA)	 INFORMATION TECHNOLOGY	DHS (CISA)
 DEFENSE INDUSTRIAL BASE	DOD	 NUCLEAR REACTORS, MATERIALS AND WASTE	DHS (CISA)
 EMERGENCY SERVICES	DHS (CISA)	 TRANSPORTATIONS SYSTEMS	DOT & DHS
 ENERGY	DOE	 WATER	EPA

Emergency Managers around the state

Emergency Managers and RERT Regions in Wyoming



Cybersecurity Response Team

- Cyber Assistance Response Effort (CARE)
- 7 State Agencies
- 3 Federal Agencies
- Conduct cyber exercises
- Assist with cyber events/incidents
- Update and review the state cybersecurity plan
- Information awareness on how to report a cyber event/incident



Cyber attacks on Health care Facility

Cyber attacks healthcare facility can cause significant harm, to:

- Protected Health Information (PHI)
- Electronic Health Record (EHR)
- Electronic Medical Record (EMR)
- EHR systems: usually procured using third-party software suites, and can touch the state network (WDH)
- Cyber attacks on health care systems have spiked during the pandemic, threatening patients care and private data
- Exploitation of individuals looking for details on disease tracking, testing, and treatment
- Deface the medical facilities website or compromise the email system
- Steal customers' personal data or credit card information from the medical facilities billing system
- Install malicious programs like ransomware, which can disable business enterprise or process control operations

Cyber attacks on Health care Facility

Threats to EHR systems within health care facility

Phishing Attacks

Attackers will exploit email, attempting to trick the user into revealing login credentials or installing malicious software on the HER system/network.

Malware and Ransomware

Deployed onto a user system in number of ways (phishing, exploits, etc..) malware can impact HER data; stealing, destroying, encrypting, or holding the data for ransom.

Cloud Threats

Cloud services represent a new factor in supply chain/third party exploitation, it gives hackers a larger attack surface in which to compromise an HER system.

Insufficient Encryption

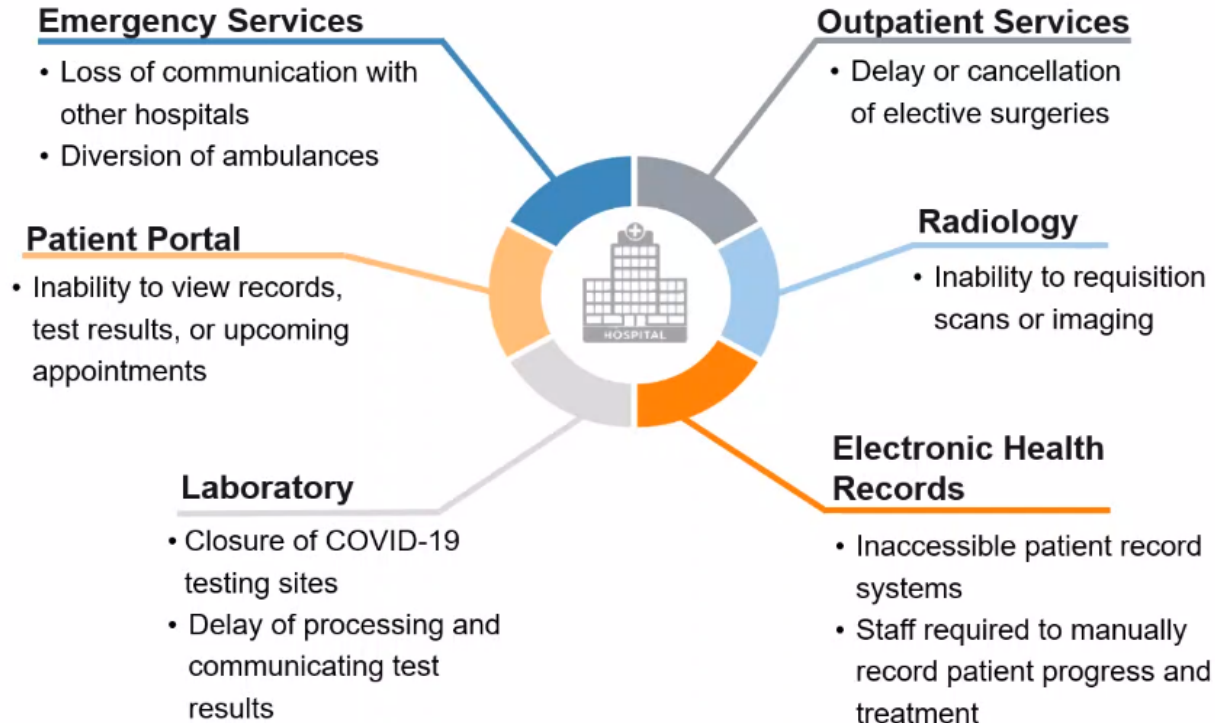
A lot of devices on the HER network use little to no encryption, this makes data in transit vulnerable to exploitative attacks, such as Man-in-the-Middle and other exfiltration methods.

Employees/Insider Threats

Personnel within the organization, whether through unwitting negligence or malicious intent, which can cause significant damage, using their credentials to gain access to EHR data systems.

Cyber attacks on Health care Facility

(U) Ransomware: Potential Effects on Hospital Systems



Cyber attacks on Healthcare Facility

How can we protect our data?

- Provide social engineering and phishing training to employees
- Develop and maintain policy on suspicious e-mails for end users; Ensure suspicious e-mails are reported
- Ensure emails originating from outside the organization are automatically marked before received
- Apply applicable patches and updates immediately after testing; Develop and maintain patching program if necessary
- Implement Intrusion Detection System
- Implement spam filters at the email gateways
- Block suspicious IP addresses at the firewall
- Implement whitelisting technology on appropriate assets to ensure that only authorized software is allowed to execute
- Implement and maintain anti-malware solution
- Conduct system hardening to ensure proper configurations

Cyber attacks on Healthcare Facility

How can we protect our data?

- Work with the Protective Security Advisor (PSA) and Cyber Security advisor (CSA) on Site and System Assessments
- Share information bulletins and potential Threats to critical infrastructure
- What are your interdependencies
- Budget funding to maintain your Cybersecurity
- Protect and patch your system
- Notify your IT department if you see something suspicious on your computer
- Report a cyber event! Contact your local emergency manager or the Wyoming Office of Homeland Security. 307-630-2767
- Work with the WIAT, DHS I&A, CISA, and FBI

Cybersecurity Best Practices

- Ensure the integrity of process control systems
- Limit remote desk protocols
- Protect sensitive medical and patient information;
- Reduce legal liabilities if patient or employee personal information is stolen;
- Change locks and passwords to systems
- Maintain customer confidence
- Exercise your ERP, meet the key players before an event. Talk with your Emergency Manager
- **Passwords:** 80% of data breaches could be prevented by using a two-factor authentication
- 17% of people use their favorite sports team and current year as their password
- **Software updates:** 77% of attacks in 2017 took advantage of vulnerabilities in the software already on your computer
- Phishing emails-91% of all cyber attacks start with a phishing email
- **USB:** 8 out of 10 companies employees use non-encrypted USB devices, such as free USBs from conferences

Responding to Cyber event

Steps for Responding to a Suspected Cyber Incident at a healthcare Facility

Response:

1. Disconnect compromised computers from the network. Do NOT turn off or reboot system.
2. Assess the scope of the compromise, and isolate all affected IT systems.
3. Open a ticket with your antivirus software or security service vendor.
4. Assess any potential damage, including impacts to treatment processes or service disruptions.
5. Initiate manual operation of equipment if control systems have been compromised.
6. Distribute any advisories or alerts to customers as needed, including customers whose records may have been compromised.
7. Identify methods to scan all IT assets to eradicate malicious code. Assess and implement recovery procedures.

Reporting:

1. Report the incident to your IT department, Wyoming Department of Health and the Wyoming Office of Homeland Security.
2. The State of Wyoming Cyber Team can help with contacting EPA, Cybersecurity and Infrastructure Security Agency (CISA), FBI, WaterISAC and MS-ISAC.

Overview of the THIRA/SPR

- THIRA: Threat & Hazard Identification Risk Assessment
 - Requirement since 2012
 - Due every 3 years
- SPR: Stakeholder Preparedness Review (SPR)
 - Prior to 2018, only required for states
 - New process included standardized targets and impacts
 - More quantitative (i.e. timeframe metrics)
 - Due every 1 year
- Guidance available:
 - CPG 201
 - FEMA Regional Office Liaison



Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) Guide

Comprehensive Preparedness Guide (CPG) 201

3rd Edition
May 2018



Homeland
Security

Value of the THIRA & SPR

- **Planning:**
 - Forum for public, private, and community collaboration
 - Provide information for other planning efforts (hazard mitigation plans, EOPs, training exercise plan (TEP), and SOPs)
 - Build work plans and strategic plans
- **Exercises:**
 - Scope, design, build, and conduct exercises to verify gaps
- **Training:**
 - Prioritize training based on gaps identified in the SPR and use the identified gaps to justify funding to close the gaps

Core Capabilities

Prevention	Protection	Mitigation	Response	Recovery		
Planning						
Public Information and Warning						
Operational Coordination						
Intelligence and Information Sharing			Infrastructure Systems			
Interdiction and Disruption			Community Resilience	Critical Transportation	Economic Recovery	
Screening, Search, and Detection				Long-Term Vulnerability Reduction		Environmental Response/Health and Safety
Forensics and Attribution	Access Control and Identity Verification	Risk and Disaster Resilience Assessment		Fatality Management Services		Housing
	Cybersecurity	Threats and Hazard Identification	Fire Management and Suppression	Natural and Cultural Resources		
	Physical Protective Measures		Logistics and Supply Chain Management		Operational Communications	
	Risk Management for Protection Programs and Activities		Mass Care Services		Public Health, Healthcare & Emergency Medical Services	
	Supply Chain Integrity and Security		Mass Search and Rescue Operations			
			On-Scene Security, Protection, and Law Enforcement			
			Situational Assessment			

See Something Say Something

Suspicious activity

You can help to prevent terrorist attacks by reporting certain activities, especially when these activities occur at or near key facilities such as government, military, utility, or other high profile sites. Suspicious activities should be reported to your local law enforcement agency.

You can also utilize Wyoming's "**If You See Something, Say Something**" program by reporting suspicious activity in Wyoming to 833-446-4188.

Phone calls to the toll-free number will be received by the WOHS Duty Officer and the information will be routed to the Wyoming Information Analysis Team for distribution as deemed appropriate.



REPORT SUSPICIOUS ACTIVITY
833-446-4188
or **9-1-1** in case of emergency



"If You See Something, Say Something" and logo are marks of the NY Metropolitan Transportation Authority.

Wyoming Information Sharing Platform (WISP)

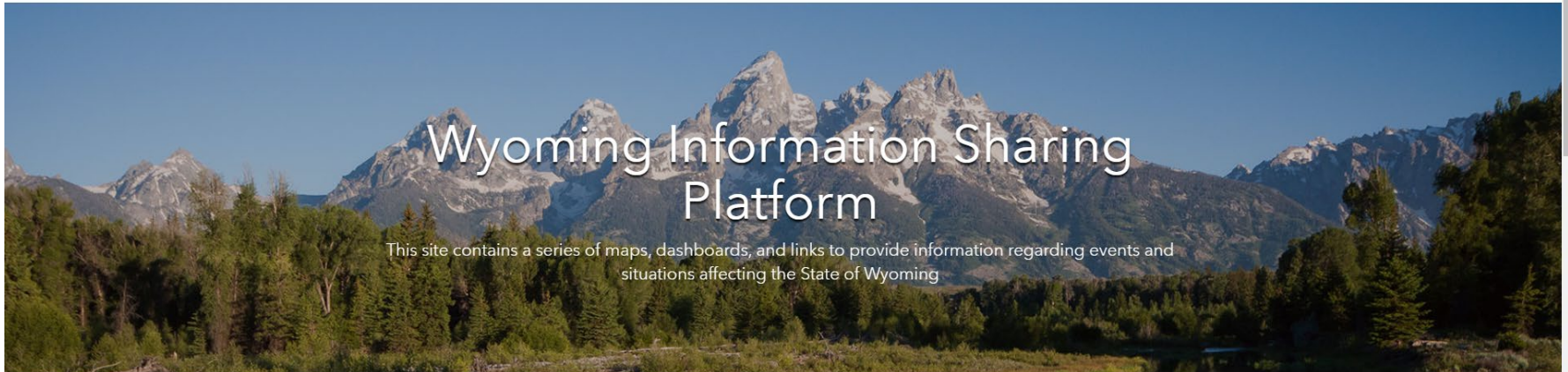
Wyoming Information Sharing Platform (WISP)

Wyoming Office of Homeland Security



- Welcome
- COVID-19
- Weather
- Fire
- Drought
- Roads
- Rivers
- Cameras
- Tourism
- County Links
- WCCA
- EOC
- EMS and Health Facilities
- SAR
- Snow
- RAPT
- Geology
- Links

Wyoming Information Sharing Platform



Tweets by @WyOHS

Wy Homeland Security
@WyOHS

WOHS is opening up a 3rd round of PPE for non-healthcare related businesses. Please fill out request form at tinyurl.com/wyomingppe.

This is not a guaranteed distribution. Do not cancel any orders you may have placed through other sources.

Deadline is 5 p.m., Aug. 7, 2020.

Wyoming Business PPE Initiat...
Wyoming has limited funds to pr...

- ### Useful Links
- Wyoming COVID-19 Information Page
 - Wyoming Department of Health
 - Wyoming Office of Homeland Security
 - Wyoming Department of Education
 - FEMA COVID-19 Page

Tweets by @GovernorGordon

Governor Mark Gordon
@GovernorGordon

Today the U.S. celebrates the 100th anniversary of the ratification of the 19th amendment, which guaranteed women the right to vote. I'm proud that Wyoming recognized women's inherent right to vote and hold office more than 50 years earlier. [#19thAmendment](#)

Questions?

Mikki Munson

State of Wyoming
Critical Infrastructure Protection & Resiliency
Program Manager

Wyoming office of Homeland Security (WOHS)

307.777.4939

mikki.munson@wyo.gov



Wyoming Office
of Homeland
Security