

# MONTANA LEAGUE OF CITIES AND TOWNS & MONTANA ASSOCIATION OF COUNTIES

# CISA SERVICES – FREE OR LOW-COST OPTIONS FOR CYBER PROTECTIONS

**Joe Frohlich**

**Cybersecurity Advisor – Montana**

Cybersecurity and Infrastructure Security Agency

[joseph.frohlich@cisa.dhs.gov](mailto:joseph.frohlich@cisa.dhs.gov)

406-461-2651



# CISA Mission

## MISSION:

- Lead the collaborative national effort to strengthen the security and resilience of America's critical infrastructure



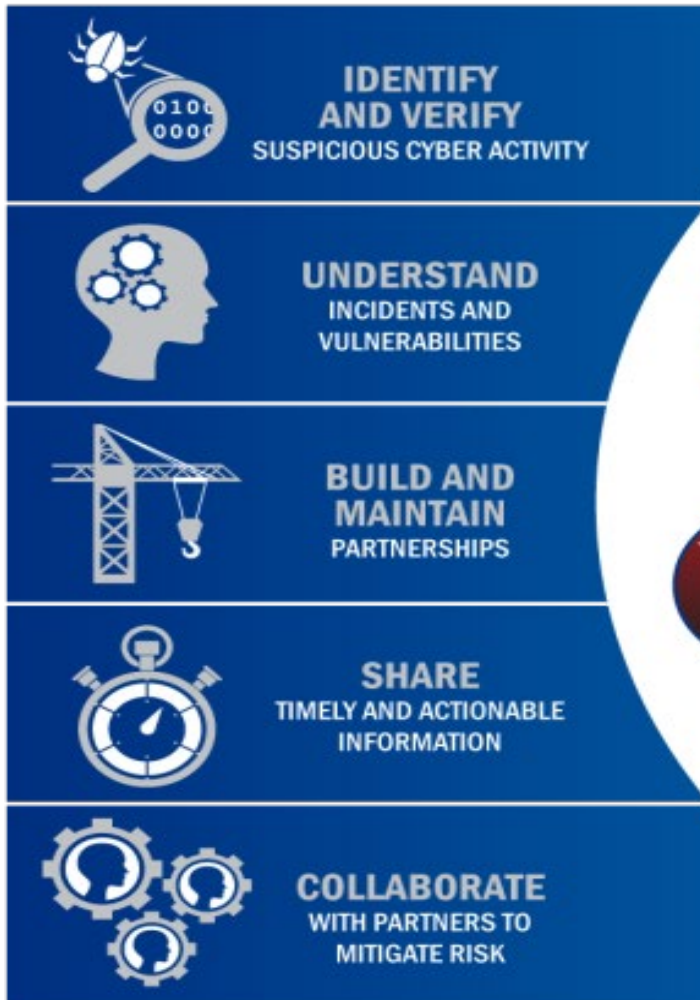
## Overall Goals:

- Goal 1 – Defend Today
- Goal 2 – Secure Tomorrow



# Serving Critical Infrastructure

## KEY ACTIVITIES:



## 16 CRITICAL INFRASTRUCTURE SECTORS:



# Cybersecurity Advisor (CSA) Program

**CISA mission:** Lead the collaborative national effort to strengthen the security and resilience of America's critical infrastructure

In support of that mission: Cybersecurity Advisors (CSAs):

- **Assess:** Evaluate critical infrastructure cyber risk.
- **Promote:** Encourage best practices and risk mitigation strategies.
- **Build:** Initiate, develop capacity, and support cyber communities-of-interest and working groups.
- **Educate:** Inform and raise awareness.
- **Listen:** Collect stakeholder requirements.
- **Coordinate:** Bring together incident support and lessons learned.



# Cybersecurity - It's Not an Impossible task



Joe Frohlich  
April 15, 2022



# Cybersecurity - Misconceptions Vs. Reality

## MISCONCEPTIONS:

- You need a BIG budget!
- A Silver Bullet Solution!
- Why would we be a target?
- There's too much to do!
- Not our problem.
- Government will save us.

## REALITY:

- Utilize free & low-cost investments
- Security by layers
- Large, Medium & Small-sized entities
- Rollover – Crawl – Walk - Run
- You own the risk
- Partner-up



# State and Local Cybersecurity Improvement Grant Program

- **Infrastructure Investment and Jobs Act (IIJA) 2021** signed into law 11/15/2021 by President Joe Biden

- State and Local Cybersecurity Improvement Act - Search for “SEC. 70612”
- 1 Billion over 4 years
  - 80% passthrough to local government
  - 25% of total state allocation must go to rural communities

- **Cybersecurity Planning Committee is required**

- State CIO/CISO will be on committee
- Planning Committee will have Local Government representation
- Planning Committee Develop Cyber State plan / Decide on Approvals

- Notice of Funding Opportunity (NOFO) tentatively issued **June/July 2022** timeframe

- NOFO will outline application process, award timelines and FAQ



Annual Funding	Federal Cost Share
• FY22: \$200M	• FY22: 90%
• FY23: \$400M	• FY23: 80%
• FY24: \$300M	• FY24: 70%
• FY25: \$100M	• FY25: 60%



# CISA CYBERSECURITY SERVICES





# CISA Cyber Resources and Assessments

## Regional Resources:

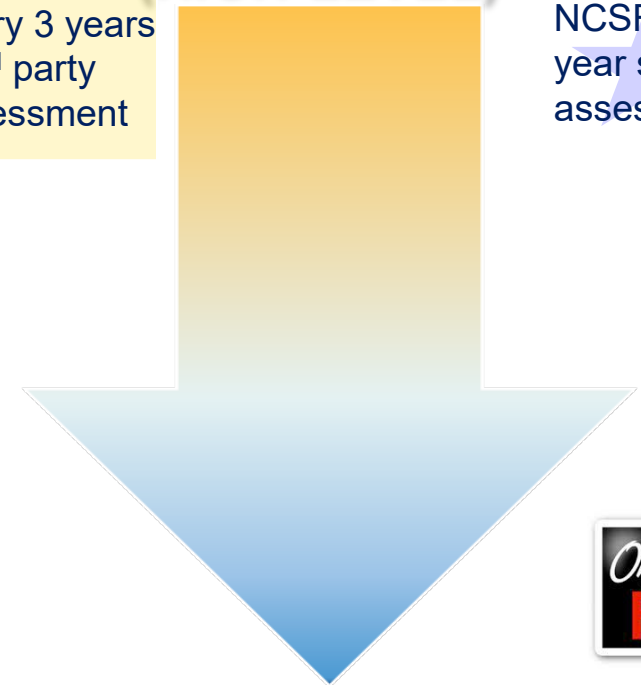
- Cyber Resilience Review (CRR) Strategic Planning Assessments Every 3 years – 3<sup>rd</sup> party assessment
- External Dependencies Management (EDM)
- Cyber Infrastructure Survey (CIS)
- Workshops (Incident Mgmt, Cyber Resilience)

## National Resources:

- Cyber Tabletop Exercises (CTTX)
- Vulnerability Scanning Service (CyHy) Continuous Monitoring Assessments ★
- Web Application Scanning (WAS)
- Phishing Campaign Assessment (PCA) Every 1-3 years – 3<sup>rd</sup> party assessment
- Remote Penetration Test (RPT)
- Validated Architecture Design Review (VADR)
- Risk & Vulnerability Assessment (RVA)

STRATEGIC  
(HIGH-LEVEL)

NCSR – Every year self assessment



TECHNICAL  
(LOW-LEVEL)






★ Sign up by emailing: [vulnerability\\_info@cisa.dhs.gov](mailto:vulnerability_info@cisa.dhs.gov) with subject line “Requesting Cyber Hygiene Services”

# CISA Cyber Assessments (Strategic / Planning)

Name	Cyber Resilience Review	Cyber Infrastructure Survey	External Dependencies Management Review	Cyber Security Evaluation Tool Assessment (CSET)
<b>Purpose</b>	Identify cybersecurity management capabilities and maturity	Calculate a comparative analysis and valuation of protective measures in-place	Assess the activities and practices utilized by an organization to manage risks arising from external dependencies	Provide detailed, effective, and repeatable methodology for assessing control systems security encompassing the organization's infrastructure, policies, and procedures
<b>Scope</b>	Critical service view	Critical service view	Critical service view	Information Technology and Operational Technology systems
<b>Time to Execute</b>	8 Hours (1 business day)	2 ½ to 4 Hours	2 ½ to 4 Hours	Varies greatly (min 2 Hours), unknown for self-assessment
<b>Information Sought</b>	Capabilities and maturity indicators in 10 security domains	Protective measures in-place	Capabilities and maturity indicators across third-party relationship management lifecycle domains	Architecture diagrams, infrastructure, policies, and procedures documents ***Ransomware Readiness***
<b>Preparation</b>	1-hour questionnaire and planning call(s)	Planning call to scope evaluation	Planning call to scope evaluation	Self-assessment available from web site and used locally
<b>Participants</b>	IT / Security Manager, Continuity Planner, and Incident Responders	IT / Security Manager	IT / Security Manager with Continuity Planner and Contract Management	Operators, engineers, IT staff, policy / management personnel, and subject matter experts
<b>Delivered By</b>	CSAs <a href="mailto:iodregionaloperations@cisa.dhs.gov">iodregionaloperations@cisa.dhs.gov</a>	CSAs <a href="mailto:iodregionaloperations@cisa.dhs.gov">iodregionaloperations@cisa.dhs.gov</a>	CSAs <a href="mailto:iodregionaloperations@cisa.dhs.gov">iodregionaloperations@cisa.dhs.gov</a>	Self-administered / CSAs <a href="https://ics-cert.us-cert.gov/">https://ics-cert.us-cert.gov/</a>

# CISA Cyber Assessments (Technical)

Name	Validated Architecture Design Review (VADR)	Phishing Campaign Assessment (PCA) 	Vulnerability Scanning (Formally Cyber Hygiene) 	Remote Penetration Test (RPT) 	Network Risk and Vulnerability Assessment (RVA)
<b>Purpose</b>	Provide analysis and representation of asset owner's network traffic, data flows, and device relationships and identifies anomalous communications flows.	Measure the susceptibility of an organization's personnel to social engineering attacks, specifically email phishing attacks.	Identify public-facing Internet security risks, through service enumeration and vulnerability scanning	Perform external penetration testing and security services to identify risks and externally exploitable pathways into systems, networks and applications.	Perform penetration testing and security services to identify risks and vulnerabilities within IT systems, networks and applications
<b>Scope</b>	Industrial Control Systems / Network Architecture/ Network Traffic	Organization / Business Unit / Email Service	Public-Facing, Network-Based IT Service	Organization / Business Unit / Network-Based IT Service	Organization / Business Unit / Network-Based IT Service
<b>Time to Execute / Availability</b>	Variable (Hours to Days) / Case by case	Approximately 6 Weeks / Within 2-6 months	Continuous / Within 2-3 days	Up to 6 weeks / 3 – 6 months	Two weeks of testing / 9 – 15 months
<b>Information Sought</b>	Network design, system configurations, log files, interdependencies, and its applications	Phishing "click rate" metrics compared to attach sophistication	Network service and vulnerability information	Network, Database, Application scope and/or access to be tested with various security tools	Network, Database, Application scope and/or access to be tested with various security tools
<b>Preparation</b>	Coordinated via Email. Planning calls	Formal rules of engagement and pre-planning	Signed agreement letter and IP address scope to be tested	Formal rules of engagement and extensive pre-planning	Formal rules of engagement and extensive pre-planning
<b>Participants</b>	Control system operators/ engineers, IT personnel, and OT personnel	IT/Security Manager, Network Administrators, end users	IT/Security Manager and Network Administrators	Management stakeholders, IT/Security Manager, Network Administrators & System Owners.	Management stakeholders, IT/Security Manager, Network Administrators, and System Owners.
<b>Delivered By</b>	Contact <a href="mailto:vulnerability_info@cisa.dhs.gov">vulnerability_info@cisa.dhs.gov</a> for more information or to request services				

# Protected Critical Infrastructure Information Program

## Protected Critical Infrastructure Information (PCII) Program Guards Your Information

- Sensitive critical infrastructure information voluntarily given to CISA is protected by law from
  - Public release under Freedom of Information Act requests,
  - Public release under State, local, tribal, or territorial disclosure laws,
  - Use in civil litigation and
  - Use in regulatory purposes.
- To learn more, visit [www.dhs.gov/pcii](https://www.dhs.gov/pcii)



# Protective Security Advisors (PSA)



# PSA Resources



- **INFRASTRUCTURE SURVEY TOOL** - Identifying facilities' physical security, security forces, security management, information sharing, protective measures, and dependencies related to preparedness, mitigation, response, resilience, and recovery;
- **Assist Visit** – Identifies and recommends protective measures at facilities, provide comparison across like assets, and track implementation of new protective measures.
- **Infrastructure Visualization Platform (IVP)** – brings a facility's digital floorplans to life by placing on it 360° panoramic photographs, immersive video, geospatial information, and hypermedia data of critical facilities, surrounding areas, and transportation routes that assist with security planning, protection, and response efforts.
- **SAFE Tool** The Security Assessment at First Entry (SAFE) tool is designed to assess the current security posture and identify options for facility owners and operators to mitigate relevant threats





# CISA CYBER HYGIENE SERVICES



# Vulnerability Scanning and Web Application Scanning – 2 No Cost Services

2020-03-30

**CYBER HYGIENE**

## REPORT CARD

Sample Organization

- 0** Hosts with unsupported software
- 14** Potentially Risky Open Services
- 9%** Increase in Vulnerable Hosts



**CISA**  
CYBER+INFRASTRUCTURE

### HIGH LEVEL FINDINGS

**LATEST SCANS**

**December 31, 2019 — March 30, 2020**  
Host Scans on All Addresses

**March 12, 2020 — March 30, 2020**  
Vulnerability Scans on All Hosts

ADDRESSES OWNED	ADDRESSES SCANNED
<b>147,274</b> No Change	<b>147,274</b> No Change
<b>HOSTS</b> <b>422</b> ↑ Increase of 6	<b>SERVICES</b> <b>3,352</b> ↓ Decrease of 24
<b>VULNERABLE HOSTS</b> <b>168</b> ↑ Increase of 14 40% of hosts vulnerable	<b>VULNERABILITIES</b> <b>383</b> ↑ Increase of 45

### VULNERABILITIES

**SEVERITY BY PROMINENCE**

- 0 CRITICAL**  
0 RESOLVED  
0 NEW
- 1 HIGH**  
0 RESOLVED  
1 NEW
- 327 MEDIUM**  
28 RESOLVED  
63 NEW
- 55 LOW**  
4 RESOLVED  
13 NEW

**VULNERABILITY RESPONSE TIME**

**0 DAYS**  
MAX AGE OF ACTIVE CRITICALS

**153 DAYS**  
MAX AGE OF ACTIVE HIGHS

**POTENTIALLY RISKY OPEN SERVICES**

- RDP: 1
- Telnet: 6
- SMB: 0
- LDAP: 0
- NETBIOS: 0

None Open | Open, No M...

Service counts are best guesses and may not be accurate. Details can be found in services.csv\* in Appendix G.

Sign up by emailing: [vulnerability\\_info@cisa.dhs.gov](mailto:vulnerability_info@cisa.dhs.gov)  
with subject line "Requesting Cyber Hygiene Services"

Joe Frohlich  
April 15, 2022



# CISA Cyber Risk Summary – SLTT GOV

Based on CISA Vulnerability Management Assessments from Jan. 1, 2020 to Dec. 31 2020



Median number of **days to remediate critical and high vulnerabilities** was **210** and **145.5**, respectively



**51%** of entities ran at least one **risky service** on an **internet-accessible host**



**60%** of entities had **filtering controls** that were bypassed by **spearphishing emails**



**14.5%** of users **clicked on malicious phishing attachments or links**

Median time for SLTT on critical vulnerabilities with “known exploits” = **418 days**

Federal systems are required to patch critical vulnerabilities in **14 days** and highs within **30**



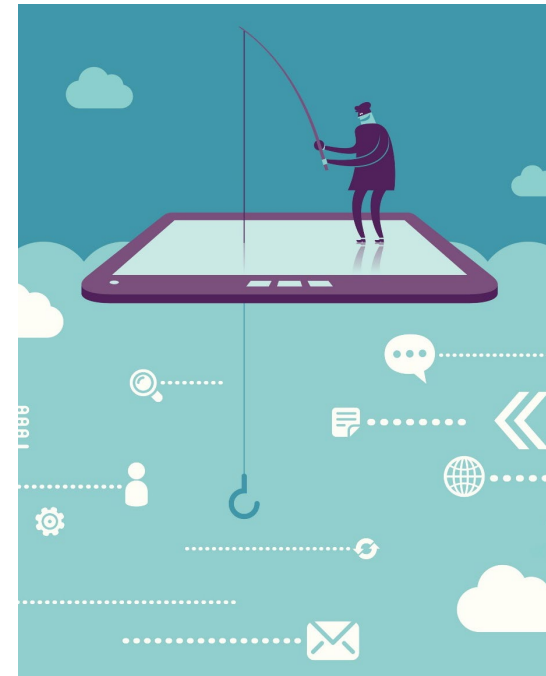
# Phishing Campaign Assessment

**Purpose:** Test an organization's susceptibility and reaction to phishing emails.

**Delivery:** Online delivery by CISA

**Benefits:**

- Identify the risk phishing poses to your organization
- Decrease risk of successful malicious phishing attacks, limit exposure, reduce rates of exploitation
- Receive actionable metrics
- Highlight need for improved security training
- Increase cyber awareness among staff
- Part of CISA Cyber Hygiene Services



Sign up by emailing: [vulnerability\\_info@cisa.dhs.gov](mailto:vulnerability_info@cisa.dhs.gov)  
with subject line "Requesting Cyber Hygiene Services"

# Remote Penetration Testing (RPT)

- **Remote Penetration Testing (RPT)** utilizes a dedicated remote team to assess and identify vulnerabilities and work with customers to eliminate exploitable pathways.
- **Testing Scenarios:**
  - External Penetration Test
  - External Web Application Test
  - Phishing Assessment
  - Open-Source Intelligence Gathering
- **Assessment Objectives:**
  - Simulate the tactics and techniques of real-world threats and malicious adversaries
  - Test centralized data repositories and externally accessible assets/resources
  - Avoid causing disruption to the customer’s mission, operation, and network infrastructure
  - Provide a proactive, risk-based approach to analyzing stakeholder systems
  - Provide expertise in identification of vulnerabilities, risk evaluation, and mitigation



Sign up by emailing: [vulnerability\\_info@cisa.dhs.gov](mailto:vulnerability_info@cisa.dhs.gov)  
with subject line “Requesting Cyber Hygiene Services”

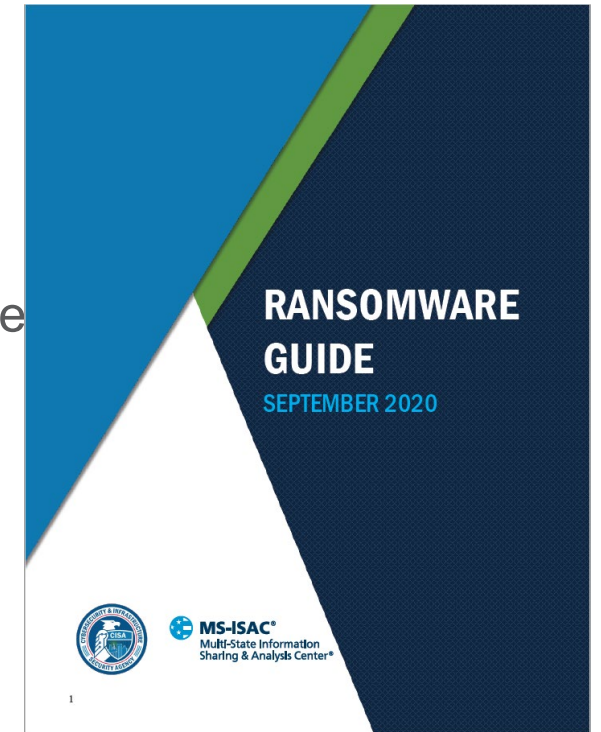
Joe Frohlich  
April 15, 2022

# CISA PREPAREDNESS ACTIVITIES



# Incident Management

- Incident Response/Management
  - Designate an incident response team
  - Assure availability of key personnel
  - If you have an incident response plan – assess it with a tabletop exercise
  - If you DO NOT have an incident response plan – create one now
    - [CISA Ransomware Guide](#)
    - [Federal Government Cybersecurity Incident and vulnerability response playbooks](#)
- CISA Ransomware Guide
  - Part 1: Ransomware Prevention Best Practices
  - Part 2: Ransomware Response Checklist



<https://www.cisa.gov/stopransomware/ransomware-guide>



<https://www.cisa.gov/stopransomware>

Joe Frohlich  
April 15, 2022

# Cyber Tabletop Exercises (CTTX)

- CISA can assist critical infrastructure owners and operators in developing their own tabletop exercises to meet the specific needs of their facilities and stakeholders.
- CISA can facilitate the TTX onsite/remotely OR you can do it yourself!
- Use CISA Tabletop Exercise Packages (CTEP) to help develop your own
  - Cyber Insider Threat
  - Ransomware Third Party Vendor CTEP Situation Manual
  - Vendor Phishing CTEP Situation Manual
  - Election Day Voting Machines
  - Wildfire (Physical Security Scenario)
  - Water and Wastewater Systems CTEP Situation Manual (Cyber-Physical Convergence Scenario)



<https://www.cisa.gov/cisa-tabletop-exercises-packages>

# Incident Response Assistance

- IT Staff or IT Vendor
- Multi-State Information Sharing and Analysis Center (MS-ISAC)
  - 24x7 MS-ISAC Security Operations Center
  - 866-787-4722** or email [soc@cisecurity.org](mailto:soc@cisecurity.org)
- CISA Central - 24x7 contact number: **1-888-282-0870**



# Incident Reporting

Montana Analysis and Technical Information Center (MATIC) : **406-444-1318**

CISA Central

24x7 contact number: **1-888-282-0870**

<https://us-cert.cisa.gov/forms/report>

\*Cyber Incident Reporting for Critical Infrastructure Act of 2022

72 hours after incident

24 hours after ransom payment





# ADDITIONAL CYBER RESOURCES



# .GOV to CISA

- CISA operates the .gov top-level domain (TLD) and makes it available to U.S.-based government organizations, from federal agencies to **local municipalities**. Helps the public know you are an *official government entity*.
- As of April 2021: Easily register and keep a .gov domain at **no cost** for qualifying U.S.-based government organizations at <https://home.dotgov.gov>
- Quickly identify your government organization on the Internet
- Ensure that the name resolves in the global domain name system (DNS)
- Maintain a trusted & secure .gov space (i.e., published policies & security best practices and .gov domain data publicly available)



# Our Nation's Cyber Workforce Foundation

The [National Cybersecurity Workforce Framework](#) is a collection of definitions that describe types of cybersecurity work and skills requires to perform it.

When used nationally, the definitions help establish universally applicable cybersecurity skills, training/development, and curricula

- ✓ 7 Categories, 30+ Specialty Areas
- ✓ Baselines knowledge, skills, and abilities & tasks



**Operate &  
Maintain**



**Securely  
Provision**



**Analyze**



**Collect &  
Operate**



**Oversight &  
Development**



**Protect &  
Defend**



**Investigate**



# Free Cyber Training and Webinars

- **FedVTE** is an online, on-demand training center that provides **free** cybersecurity training for U.S. veterans and federal, state, local, tribal, and territorial government employees.

- **Industrial Controls System Training from Idaho National Labs**

Water / Wastewater Systems

Virtual & Instructor Led Training, plus self paced training courses



- **CISA Incident Response Training** for beginner, intermediate, and advanced cyber professionals

- **Free Basic Cybersecurity Training**

National Cyber Security Alliance and Cyber.org

- **MACO / State of Montana Opportunities?**

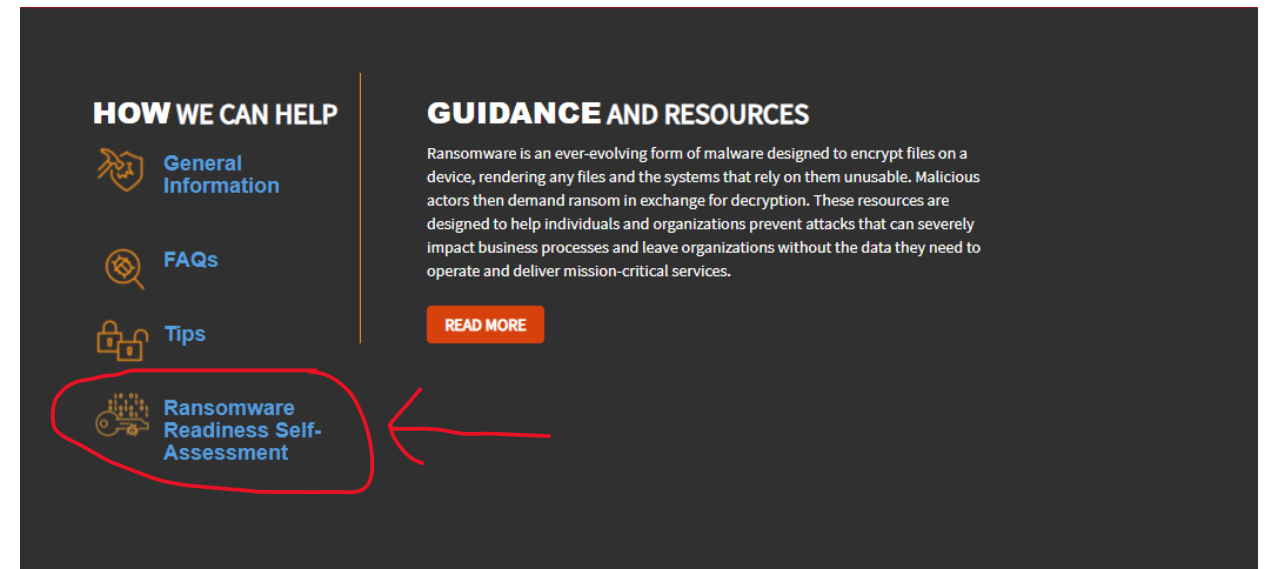
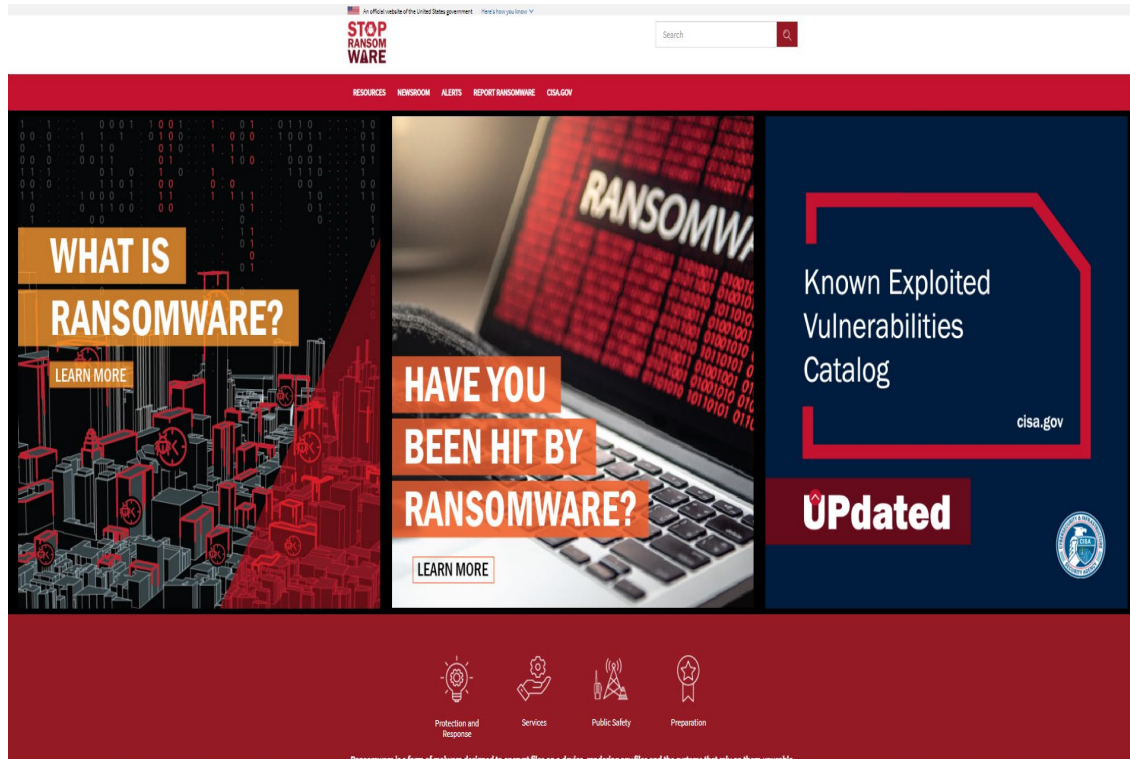
[servicedesk@mt.gov](mailto:servicedesk@mt.gov)



[apembroke@mtcounties.org](mailto:apembroke@mtcounties.org)

Joe Frohlich  
April 15, 2022

# www.cisa.gov/stopransomware



<https://www.cisa.gov/stopransomware/ransomware-guide>



# Multi-State Information Sharing and Analysis Center (MS-ISAC)

- Multi-State Information Sharing and Analysis Center

- Focal point for cyber threat prevention, protection, response and recovery for state, local, tribal, and territorial governments.

- **24x7 MS-ISAC Security Operations Center**

- 866-787-4722 or email [soc@cisecurity.org](mailto:soc@cisecurity.org)

- No Cost Services (Local Government)

- Join [MS-ISAC](#)
- [Nationwide Cybersecurity Review \(NCSR\)](#) ★
- [MS-ISAC NIST CSF Policy Template Guide](#) ★
- [Malicious Domain Blocking and Reporting \(MDBR\) \(cisecurity.org\)](#) ★
- [CIS Controls](#) (Focus on IG1 until more mature)
- [All MS-ISAC Services](#) (free and fee based)

- Fee Services

- [Albert Network Monitoring and Management \(cisecurity.org\)](#)
- [CIS Endpoint Security Services \(ESS\) \(cisecurity.org\)](#)



## Malicious Domain Blocking and Reporting (MDBR)



v8 Resources and Tools



# Montana Information Sharing Opportunities

- Montana Information Security Advisory Council (MT-ISAC)
  - Governor appointed council members from public and private sectors. Objectives are to leverage public-private partnership to enhance cybersecurity information sharing, outreach and risk awareness to help effectively protect information systems across the state. Visit <https://sitsd.mt.gov/Governance/Boards-Councils/MTISAC/> for more information.
- Montana Analysis and Technical Information Center (MATIC)
  - Karli King (Crime Analyst) [KaKing@mt.gov](mailto:KaKing@mt.gov) | 406-444-1318
- Montana Local Government Information Technology (LGIT)  
Have your IT Staff join by emailing: [affiliates@mtlgit.org](mailto:affiliates@mtlgit.org)
- Montana National Guard



# Cybersecurity is NOT an IT-only job;

# It is an organization-wide responsibility. You play a major

# role!





# Action Plan

Next Week: Schedule a Monthly or Quarterly Cyber Risk **non-public** meeting – invite IT/Security/DES staff/Office or Department Managers (Discuss with legal)

- Could be as quick as 15-30 minutes
  - Topics to consider for each meeting:
    - Discuss metrics such as Vulnerability Scans
      - sign up for [Cyber Hygiene Services](#)
    - Nationwide Cybersecurity Review ([NCSR](#)) and cyber strategic plan moving forward
    - What gaps have been identified that we can plan to mitigate
    - Look into upcoming [IIJA grant](#)
  - Find out if your City/County is [MS-ISAC](#) Member? Become a member if not!
    - Sign up for [MDBR](#)

## Future Meeting Topics

- Website Transition to [.GOV Domain](#)
- Cyber Incident Response Plan Review – Have a plan/Last Updated?
- Review [StopRansomware.GOV](#) site
  - Take the [Ransomware readiness assessment](#) (Form a team to take!)
- Employee Security Awareness Training and Stats
- Simulated [Phishing Tests](#) to Employees and Stats
- Use this slide deck to find out more about no cost services or information sharing from [CISA/MS-ISAC](#)/League of Cities/MACO (If you are a County)/MMIA/State of Montana/MT National Guard
- Reach out to CISA CSA and PSA for additional topics



# Contact Information

## General Inquiries

[iodregionaloperations@cisa.dhs.gov](mailto:iodregionaloperations@cisa.dhs.gov)

## CISA Contact Information

### Joe Frohlich

Cybersecurity Advisor  
Region 8 - Montana

[joseph.frohlich@cisa.dhs.gov](mailto:joseph.frohlich@cisa.dhs.gov)

406-461-2651

### Randy Middlebrook

Protective Security Advisor  
Region 8 - Montana

[randy.middlebrook@hq.dhs.gov](mailto:randy.middlebrook@hq.dhs.gov)

406-839-1165



Cybersecurity and Infrastructure Security Agency

Joe Frohlich  
April 15, 2022