MONTANA EDUCATIONAL TECHNOLOGISTS ASSOCIATION

PROTECTING OUR FUTURE: SAFEGUARD K-12 SCHOOLS FROM PHYSICAL AND CYBER THREATS

CISA Mission

MISSION:

- Lead the National effort to understand, manage, and reduce risk to our cyber and physical infrastructure.

Vision:

- A secure and resilient critical infrastructure for the American people.

CISA's Priorities for 2023

Priorities for 2023:

- K-12
- Election Security
- Public Health & Hospitals
- Water and Wastewater

Protecting Out Future: Cybersecurity for K-12

K-12 Cybersecurity Act of 2021 required CISA to report on cybersecurity risks facing elementary and secondary schools

Recommendations for K-12

1. Invest in the most impactful security measures and build toward a mature cybersecurity plan
2. Recognize and actively address resource constraints.
3. Focus on collaboration and information sharing.

CISA's Recommendations for K-12

1. **Invest in the most impactful security measures and build toward a mature cybersecurity plan**

   - Deploy multi-factor authentication (MFA)
   - Mitigate known exploited vulnerabilities
   - Implement and test backups
   - Regularly exercise an incident response plan
   - Implement a strong cybersecurity training program
   - Adopt CISA's Cybersecurity Performance Goals (CPGs)

https://www.cisa.gov/protecting-our-future-cybersecurity-k-12

CISA's Recommendations for K-12

2. Recognize and actively address resource constraints.

- Work with the state planning committee to leverage the State and Local Cybersecurity Grant Program (SLCGP).
- Utilize free or low-cost services to make near-term improvements in resource-constrained environments.
- Expect and call for technology providers to enable strong security controls by default for no additional charge.
- Minimize the burden of security by migrating IT services to more secure cloud versions.

https://www.cisa.gov/protecting-our-future-cybersecurity-k-12

CISA's Recommendations for K-12

3. Focus on collaboration and information sharing.

- Join relevant collaboration groups, such as MS-ISAC,K12six, and Cyber406.
- Work with other information-sharing organizations, such as fusion centers, state school safety centers, other state and regional agencies, and associations.
- Build a strong and enduring relationship with CISA and FBI regional cybersecurity personnel.

https://www.cisa.gov/protecting-our-future-cybersecurity-k-12

Sampling of CISA's Voluntary & No-Cost Cybersecurity Offerings

• Assessments & Evaluations

R1

- Strategic
  - Cyber Resilience Review (CRR™)
  - ★ Cyber Resilience Essentials (CRE)
  - Cyber Infrastructure Survey (CIS)
  - External Dependencies Management (EDM)
  - ★ Cyber Security Evaluation Tool (CSET™)
- Technical

R2

  - ★ Vulnerability Scanning (CyHy)
  - Web Application Scanning (WAS)
  - Phishing Campaign Assessment (PCA)
  - Remote Penetration Test (RPT)

Preparedness Activities

- ★ Tabletop Exercises R3
- Security Alerts, Tips and other updates (US-Cert)
  - National Cyber Awareness System
  - Known Exploited Vulnerabilities (KEV) ★ R1
- Informational Products and Recommended Practices
- Cybersecurity Training and Webinars
- Guides and "Playbooks"
  - Cross-Sector Cybersecurity Performance Goals (CPG) ★ R1
  - Ransomware Guide
- National Cybersecurity Workforce Framework

CISAs Recommendations for K-12

1. Invest in the most impactful security measures and build toward a mature cybersecurity plan = R1
2. Recognize and actively address resource constraints. = R2
3. Focus on collaboration and information sharing. = R3

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

CISAs Recommendations for K-12

1. Invest in the most impactful security measures and build toward a mature cybersecurity plan
2. Recognize and actively address resource constraints.

State and Local Cybersecurity Grant Program

- Infrastructure Investment and Jobs Act (IIJA) amended Homeland Security Act of 2022 and appropriated $1B over 4 years

- A cybersecurity planning committee is a requirement.
  - Public education is required to be on committee
    - Carol Phillips from Elder Grove School District
    - Jason Hecock from Kalispell Public Schools
    - State CIO – Kevin Gilbertson is Chair
    - State CISO – Andy Hanks is Vice Chair

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

- **<u>Roles of planning committee</u>**
  - Develop, implement, and revise Cybersecurity Plans
  - Approve Cybersecurity Plans
  - Assist with determination of effective funding priorities (i.e., individual projects)

<u>CISAs Recommendations for K-12</u>

2. Recognize and actively address resource constraints.

State and Local Cybersecurity Grant Program – Montana Breakdown

Allocation Year	Match %	Statewide	State Share (20%) (FED)	Local Share (80%) (FED)
Year 1	Waived	**$2,427,866**	$485,573	$1,942,293
Year 2	20%	$4,860,000	$972,000	$3,888,000
Year 3	30%	$3,650,000	$730,000	$2,920,000
Year 4	40%	$1,200,000	$240,000	$960,000

CISAs Recommendations for K-12

2. Recognize and actively address resource constraints.

Multi-State Information Sharing and Analysis Center (MS-ISAC) & K12 SIX

- Multi-State Information Sharing and Analysis Center
  - **24x7 MS-ISAC Security Operations Center**
    - 866-787-4722 or email soc@cisecurity.org
- No Cost Services (K-12)

R3
- Join MS-ISAC

R1
- Nationwide Cybersecurity Review (NCSR) ★

R2
- 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)

R3
- K12 Security Information eXchange (K12 SIX)

MS-ISAC® Multi-State Information Sharing & Analysis Center®

Albert CIS Network Monitoring

Malicious Domain Blocking and Reporting (MDBR)

CIS SecureSuite® Membership

IG1

CIS Controls

v8 Resources and Tools

MCAP Malicious Code Analysis Platform

K12 SIX

CISAs Recommendations for K-12

1. Invest in the most impactful security measures and build toward a mature cybersecurity plan = R1
2. Recognize and actively address resource constraints. = R2
3. Focus on collaboration and information sharing. = R3

Cyber406 strives to improve Montana's cybersecurity defensive posture across private and public sectors by increasing the state's ability to prevent, identify, and eradicate cyber threat vulnerabilities through a systematic approach of Collaboration, Operations, Education, and Research.

https://www.cyber406.org/

CISAs Recommendations for K-12

3. Focus on collaboration and information sharing.

Incident Responce 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
- CISA Central - 24x7 contact number: **1-888-282-0870**
- Internet Crime Complaint Center (IC3) https://www.ic3.gov/
  - FBI – Lead Federal agency for cyber crime
- Montana Analysis and Technical Information Center (MATIC)
  - 406-444-1318

IR Templates

- Microsoft Word IR Template Based off Federal IR Playbook – Tailored to Montana – ***Link will expire April 9th
- K12 SIX – Essential Cyber Incident Response Runbook, K12 SIX
- Other Examples:
  - Federal Government Cybersecurity Incident and Vulnerability Response Playbooks, CISA
  - State Cybersecurity Best Practices Incident Response Plan, State Educational Technology Directors Association
  - Ransomware Guide, CISA & MS-ISAC

Contact Information

CISA Contact Information

Joe Frohlich Cybersecurity State Coordinator Region 8 - Montana	joseph.frohlich@cisa.dhs.gov 406-461-2651
Travis Light Cybersecurity Advisor Region 8 - Montana	travis.light@cisa.dhs.gov 406-894-8374
Randy Middlebrook Protective Security Advisor Region 8 - Montana	randy.middlebrook@cisa.dhs.gov 406-839-1165
Albert Mendoza Protective Security Advisor Region 8 - Montana	albert.mendoza@cisa.dhs.gov 202-702-0798

General Inquiries

iodregionaloperations@cisa.dhs.gov