******No cost – voluntary services from DHS CISA**

**CISA Contact Information**

 **Cybersecurity Advisor – Montana**

 Joe Frohlich

 joseph.frohlich@cisa.dhs.gov

 406-461-2651

 **Protective Security Advisor – Montana**

 Randy Middlebrook

 randy.middlebrook@cisa.dhs.gov

 406-839-1165

**GRANT FUNDS**

**Infrastructure Investment and Jobs Act**

State and Local Cybersecurity Improvement Grant Program

 <https://www.congress.gov/bill/117th-congress/house-bill/3684>

Search for “SEC. 70612”

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

**CISA Services**

**CISA Cyber Resource Hub** (Cyber Resilience Review, External Dependencies Management, Cyber Infrastructure Survey, Cyber Security Evaluation Tool-CSET)

<https://www.cisa.gov/cyber-resource-hub>

**CISA Protective Security Advisors** (Assist Visit, SAFE Tool, Infrastructure Survey Tool)

<https://www.cisa.gov/protective-security-advisors>

**Cyber Hygiene Services**

<https://www.cisa.gov/cyber-hygiene-services>

 Vulnerability Scanning (Continuous Monitoring of public facing systems)

Web Application Scanning (Continuous Monitoring of public facing systems

 Phishing Campaign Assessment (Recommended every 2 years)

 Remote Penetration Test (Recommended every 2 years)

### Get Started

Email CISA at vulnerability\_info@cisa.dhs.gov with the subject line “Requesting Cyber Hygiene Services” to get started.

**CISA Preparedness Activities**

**Stop Ransomware**

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

**CISA Ransomware Guide**

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

**Ransomware Readiness Assessment** using CSET Tool

 <https://www.cisa.gov/stopransomware/cyber-security-evaluation-tool-csetr>

**Federal Government Cybersecurity Incident and vulnerability response playbooks**

<https://www.cisa.gov/uscert/ncas/current-activity/2021/11/16/new-federal-government-cybersecurity-incident-and-vulnerability>

 **CISA Tabletop Exercises**

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

 **Incident Response Assistance**

 IT Staff or IT Vendor, MS-ISAC 1-866-787-4722, CISA Central 1-888-282-0870

 **Incident Reporting**

Montana Analysis and Technical Information Center 406-444-1318, CISA Central 1-888-282-0870

**National Cybersecurity Workforce Framework** (collection of definitions that describe types of cybersecurity work and skills requires to perform it – Use for Job Descriptions)

<https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework>

 **Move to .gov** domain (.gov is for US-Based government organizations, secure and trusted)

<https://home.dotgov.gov>

**Receive Cybersecurity Alerts** –

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

**Training**

**FedVTE**

<https://fedvte.usalearning.gov/>

**CISA Incident Response Training**

<https://www.cisa.gov/incident-response-training>

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

<https://ics-training.inl.gov/learn/register>

**Additional Cyber Resources**

**Patch ALL KNOWN EXPLOITED VULNERABILITIES in your environment**

<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

**Stop Bad Practices** -

<https://www.cisa.gov/stopransomware/bad-practices>

**Get Your Stuff Off Search** –(Know what the adversary knows)

<https://www.cisa.gov/publication/stuff-off-search>

**Implement Cybersecurity Measures Now to Protect Against Potential Critical Threats**

<https://go.usa.gov/xtB8P>

**Multi-Factor Authentication** –

<https://www.cisa.gov/uscert/ncas/tips/ST05-012>

**Apache Log4j Vulnerability Guidance** –

<https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance>

**CISA Shields Up Webpage** –

<https://www.cisa.gov/shields-up>

**Voluntary services from MS-ISAC**

****

**No Cost Services for State, Local, Tribal K-12.**

**Join MS-ISAC – (There is an Elections, K-12, Local Government Working Groups)**

<https://learn.cisecurity.org/ms-isac-registration>

**Join EI-ISAC** for Elections Offices <https://www.cisecurity.org/ei-isac>

**Nationwide Cybersecurity Review (NCSR)**

<https://www.cisecurity.org/ms-isac/services/ncsr>

**CIS Controls** (\*\*\*Focus on security controls Implementation Group 1 first) –

<https://www.cisecurity.org/controls/cis-controls-list/>

**MS-ISAC NIST CSF Policy Template Guide (**copy entire link**)**

<https://www.cisecurity.org/-/jssmedia/Project/cisecurity/cisecurity/data/media/files/uploads/2021/11/NIST-Cybersecurity-Framework-Policy-Template-Guide-v2111Online.pdf>

**Malicious Domain Blocking and Reporting (**\*Set this up or have similar DNS Sec service**)**

 <https://www.cisecurity.org/ms-isac/services/mdbr/>

**Real-Time Indicator Feeds** (automate blocking of known malicious IPs and sites)

 <https://www.cisecurity.org/ms-isac/services/real-time-indicator-feeds>

**CIS** [**SecureSuite**](https://www.cisecurity.org/cis-securesuite/)(CIS Secure Benchmarks and Compliance)

 <https://www.cisecurity.org/cis-securesuite/>

**CIS MCAP**

 <https://www.cisecurity.org/ms-isac/services/>

**Fee based services**

**Albert Network Monitoring and Management**

<https://www.cisecurity.org/services/albert-network-monitoring/>

**CIS Endpoint Security Services (ESS)**

 <https://www.cisecurity.org/services/endpoint-security-services>

**All MS-ISAC Services**

<https://www.cisecurity.org/ms-isac/services>