Montana State and Local Cybersecurity Grant Program Guidance

Guidance Released: November 17, 2025

MONTANA DISASTER AND EMERGENCY SERVICES

1956 Mt. Majo Street
PO Box 4789
Fort Harrison, MT 59636

STATE & LOCAL CYBERSECURITY GRANT PROGRAM
TABLE OF CONTENTS

State and Local Cybersecurity Grant Program

The purpose of the State and Local Cybersecurity Grant Program (SLCGP) is to improve public sector cybersecurity readiness and reduce collective cyber risk through targeted investment in State and Local Government organizations.

Funding for this program is provided by the U.S. Department of Homeland Security (DHS), Federal Emergency Management Agency (FEMA), Grant Programs Directorate (GPD). Funds are appropriated under authority of the Infrastructure Investments and Jobs Appropriations Act (Pub. L. No. 117-58). Montana Disaster and Emergency Services (MT DES) is the State Administrative Agency (SAA) eligible to apply for the SLCGP on behalf of the state and make subawards to approved applicants.

Assistance Listings Number: 97.137
Assistance Listings Title: State and Local Cybersecurity Grant Program (SLCGP)
Funding Opportunity Number: DHS-22-137-000-01

Application materials are available on the MT DES website. Completed applications should be submitted to MTDESGrants@mt.gov.

KEY DATES:

- **Application opens on November 17, 2025**
- **MT DES will accept applications until January 9, 2025, at 11:55PM. After the application period closes, applications will be reviewed based on the order of submission.**
- **Applicants that are approved for funding will be notified by January 31, 2026. Official award documents will be sent subsequently, and must be signed and returned to MT DES.**
- **Projects will be awarded based on the availability of funds.**
- **Period of performance (POP) ends on June 30, 2026. No extensions are available.**

1.0 Overview

Our nation faces unprecedented cybersecurity risks, including increasingly sophisticated adversaries, widespread vulnerabilities in commonly used hardware and software, and broad dependencies on networked technologies for the day-to-day operation of critical infrastructure. Cyber incidents have no geographic boundaries; incidents impacting Montana public sector organizations may have cascading effects across the state, region, and nation.

The SLCGP grant requires the state to develop a Cybersecurity Plan, establish a Cybersecurity Planning Committee to support the development of the plan, adopt key cybersecurity best practices, and identify projects to implement using the SLCGP funding.

2.0 Purpose and Objectives

The purpose of the SLCGP is to strengthen public sector cybersecurity practices and address cybersecurity risks and threats to data, networks, and information systems. Reference section 5.1 of this document for a list of eligible sub-recipients.

Montana Cybersecurity Planning Committee designated funding for five project focus areas: security awareness training for the general workforce, professional development education for the technical workforce, endpoint detection and response, network traffic monitoring, and multi-factor authentication. Awards for the five focus areas will either be a direct award or an award for services in lieu of funding.

The overall goal of this grant is to improve the cybersecurity posture of state and local government organizations by providing assistance for managing and reducing systemic cyber risk through the following objectives:

- Objective 1: Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.
- Objective 2: Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
- Objective 3: Implement security protections commensurate with risk.
- Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

3.0 Funding

The SAA must obligate at least 80 percent of funds awarded to local and tribal governments, with a minimum of 25 percent of the overall award going to rural areas. 20 percent of the funds may be utilized for state level projects, with the SAA retaining up to 5 percent of funds awarded for administration costs.

- For this grant, rural jurisdictions are defined as counties, tribes, and cities with a population of less than 50,000.
- Funds will be sub-awarded to eligible entities through an application process.

- Final approval is contingent upon available funding.

4.0 Grant Requirements – State Level

Note: Information in section 4.0 applies to MT DES as the State Administrative Agency and is provided in this guidance document for reference and general understanding. The following activities are statutorily required at the state level as a condition of the grant:

- Establish a Cybersecurity Planning Committee.
- Develop or revise a state-wide Cybersecurity Plan.
- Evaluate individual projects for effectiveness throughout the life of the program.
- Adopt key cybersecurity best practices.

Cybersecurity Planning Committee

The Planning Committee is responsible for developing, implementing, and revising Cybersecurity Plans (including individual projects); formally approving the Cybersecurity Plan (along with the chief information officer or chief information security officer); assisting with determination of effective funding priorities (i.e., work with entities within the eligible entity's jurisdiction to identify and prioritize individual projects). This will be led by Montana State Information Technology Services Division (SITSD).

The Cybersecurity Planning Committee must include the following entities:

- Eligible Entity (state administrative agency)
- County, City, and town representation
- Institutions of public education
- Institutions of public health
- As appropriate, representatives from rural, suburban, and high-population jurisdictions.

Montana formed its Cybersecurity Planning Committee and adopted the committee charter on November 14, 2022. The committee includes 15 voting members and 5 advisory members representing the required cybersecurity planning entities.

Information on the Cybersecurity Planning Committee can be found here:

https://des.mt.gov/Grant-Programs/State-Local-Cyber-Security-Grant-Program

Cybersecurity Plan

Montana is required to submit a Cybersecurity Plan that adheres to the 16 required elements identified in section 2220A of the Homeland Security Act of 2002 as amended by the BIL. The Cybersecurity Plan must include a description of state and local roles, an assessment of capabilities for each element, address resources and timeline for implementing the Plan, and identify metrics. State and local governments are encouraged to take a holistic approach in the development of their Plan as entities must be able to sustain capabilities once SLCGP funds are no longer available. The role of state entities as coordinator and service provider to local entities should be encouraged and supported.

On November 28, 2023, DHS, FEMA approved the 2022-2024 State of Montana Cybersecurity Plan, allowing the state to request funding holds to be released for approved projects.

The Montana Cybersecurity Plan can be found here:

https://des.mt.gov/Grant-Programs/State-Local-Cyber-Security-Grant-Program

5.0 Eligibility Requirements for Local Applicants

5.1 Eligible Applicants

Eligible Applicants for competitive awards include local and tribal governments. Local government means a city, town, county, consolidated city-county, special district, or school district or subdivision of these entities. Nonprofit, for-profit, and other entities not deemed as a local government entity are not eligible to receive SLCGP funds.

5.2 Applications

Applications are based on five focus areas, providing the opportunity for targeted investment to close an eligible applicant's cybersecurity gaps. Applicants have the flexibility to apply for a combination of services in the five focus areas based on the needs (cybersecurity gaps) of their organization.

5.3 Cost Share or Match

Cost share or match is not currently required for the **SLCGP**. Future awards will have cost share requirements. Match amounts for future award years are as follows: FY 2023 0%, FY 2024 30%, FY 2025 40%. Local match may be in-kind/soft from eligible activities. Federal funds may be reduced, eliminated, or include additional responsibilities in the future. Applicants should prepare for future project sustainment independent of SLCGP funding.

5.4 Unique Entity Identifier (UEI)

The federal government now requires the Unique Entity Identifier (UEI) numbers that are created in SAM.gov. This number is required to apply for and receive SLCGP funds. Jurisdictions that do not have a UEI may request one through SAM.gov.

5.5 Applicant Agent or Authorized Representative

The applicant agent or authorized representative is the individual who is able or given authority to make legally binding commitments for the applicant organization.

The application forms require names and contact information for the applicant organization's Authorized Representative, Project Manager, and Fiscal Agent. Acceptance of the award will be established with the electronic signature of the Principal Elected Official or other individual authorized to enter into a legal agreement on behalf of the organization.

5.6 Application Review and Recommendation

Applications will be evaluated by MT DES staff through a review process to determine the application completeness and eligibility based on state and federal program guidance. Final approval is contingent upon available funding.

6.0 Project Categories and Activities

Federal funds made available through this award may only be used for the approved purposes set forth by the Montana Cybersecurity Planning Committee and must be consistent with statutory authority for the award. Award funds may not be used for matching funds for any other Federal award, lobbying, or intervention in federal regulatory or adjudicatory proceedings. In addition, federal funds may not be used to sue the Federal Government or any other government entity.

Sub-recipients must comply with all the requirements in 2 C.F.R. Part 200 (Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards) https://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title02/2cfr200_main_02.tpl

- Costs charged to SLCGP must be consistent with the Cost Principles for Federal Awards, 2 C.F.R Part 200, Subpart E.
- Any costs incurred or obligated prior to the execution of an award are not allowed.

Unless otherwise stated, equipment must meet all mandatory regulatory and/or DHS/FEMA-adopted standards to be eligible for purchase using these funds. In addition, subrecipients will be responsible for, at their own expense, obtaining and maintaining all necessary certifications and licenses for the requested equipment.

6.1 Training

Training costs are allowable under the SLCGP as described in Section 2.0 of this document. Training conducted using SLCGP funds must align to the focus areas approved by the Montana Cybersecurity Planning Committee. Training should address a performance gap identified through assessments and contribute to the reduction of systemic cyber risk.

6.2 Management and Administration

Management and Administration (M&A) activities are those directly relating to the management and administration of SLCGP funds, such as financial management and monitoring. Sub-recipients may use a maximum of up to 5% of funding for M&A purposes.

SLCGP funds used for M&A must have supporting documentation (i.e. timecards (salary), invoices/receipts (goods), and general ledgers). M&A must be coded separately on the general ledger so that it is clear as to how many hours were allocated toward M&A for the grant.

7.0 Unallowable Costs and Activities

7.1 Unallowable Costs

The grant specifically restricts the use of funds for construction and renovation. Any project requiring an Environmental and Historic Preservation (EHP) review is not allowed.

- Other Unauthorized costs include, but are **not limited to**, the following:

- Cost-sharing contributions
- Ransom payments
- Recreational or social purposes
- Cybersecurity insurance premiums
- General maintenance and repairs
- Parking tickets or other traffic tickets
- Sole source contracts and procurements not pre-approved by MT DES
- Stand-alone working meals
- Alcoholic beverages
- Supplanting any expense already budgeted
- Entertainment
- Laundry
- Late payment fees
- Drone training

7.2 Supplanting

Grant funds must supplement, not supplant, replace, or offset state or local funds that have been appropriated for the same purpose. **If supplanting is determined, sub-recipients will be required to repay grant funds expended in support of those efforts.**

7.3 Telecommunication, Video Surveillance Equipment and Services

Sub-recipients may not use any FEMA funds to procure or obtain China made or China affiliated telecommunication, video surveillance equipment or services. Reference FEMA policy #405-143-1 https://www.fema.gov/sites/default/files/documents/fema_policy-405-143-1-prohibition-covered-services-equipment-gpd.pdf

Additional guidance is available at https://www.ecfr.gov/current/title-2/subtitle-A/chapter-II/part-200/appendix-Appendix%20II%20to%20Part%20200

8.0 Procurement

All FEMA awards are subject to the federal procurement standards under the *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards* found at 2 C.F.R. § 200.317-200.327. Applicants selected for funding does not constitute award. Any costs incurred or obligated prior to the execution of an award are not allowed.

When purchasing under a FEMA award, a **state entity** must follow its own procurement policies and procedures pursuant to 2 C.F.R. § 200.317 as well as all other applicable state and federal laws, executive orders, and implementing regulations.

When purchasing under a FEMA award, a **non-state entity** must have and use documented procurement procedures, consistent with state, local, and Tribal laws and regulations and conforming to appliable federal law and the procurement standards identified in 2 C.F.R. § 200.317-200.327. For **a non-state entity**, where a difference exists between a federal procurement standard and a state, local, and/or

Tribal procurement standard or regulation, the **non-state entity** must apply the most restrictive standard.

MT DES may request a copy of an entity's documented procurement procedures which reflect applicable state and local laws and regulations. Procurement procedures must conform to applicable Federal law and the standards identified in 2 C.F.R. § 200.318

For more information on federal procurement see 2 C.F.R. § 200.320.

For more information on MT Procurement laws, rules, policies, and executive orders please visit State Procurement Bureau.

9.0 Award Administration Information

9.1 Award Administration

Notification of award approval is made through the sub-recipient's authorized representative listed in the application. Awards will be made to the sub-recipients no later than 45 days following the state's acceptance of the Federal award and release of funds. Each of the five approved project areas will have a separate award issued. Sub-recipients who wish to decline the award must provide a written notice of intent to decline.

SLCGP awards for the five focus areas will either be a direct award or an award of services in lieu of funding. All awards must be accepted by the Principal Elected Official or designated representative with the legal authority to enter into an agreement on behalf of the subrecipient organization.

9.2 Nationwide Cybersecurity Review - Required

The NCSR is a free, anonymous, annual self-assessment designed to measure gaps and capabilities of an entity's cybersecurity programs. It is based on the National Institute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and the MS-ISAC. Sub-recipients are required to complete the NCSR, administered by the MS-ISAC, during the first year of the award/subaward period of performance and annually. The NCSR is available at no cost to the user and takes approximately 2-4 hours to complete. The NCSR is expected to be open from October – January. Due to changes at the federal level, the status of this requirement is to be determined.

For more information, visit Nationwide Cybersecurity Review (NCSR) (cisecurity.org).

9.3 CYBER HYGIENE SERVICES - Required

All awarded sub-recipients will be required to sign up for and utilize the following services:

- Web Application Scanning: an "internet scanning-as-a-service." This service assesses the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and government best practices and standards.
- Vulnerability Scanning: evaluates external network presence by executing continuous scans of public, static Ips for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts.

To register for these services, email vulnerability_info@cisa.dhs.gov with the subject line

"Requesting Cyber Hygiene Services – SLCGP" to get started. Indicate in the body of your email that you are requesting this service as part of the SLGCP.
For more information, visit CISA's Cyber Hygiene Information Page.

10.0 Reporting

10.1 Progress Reports

Montana DES will gather performance information from subrecipients for use in annual reporting of grant activities to FEMA.

10.2 Reimbursement Requests

SLCGP awards for the five focus areas will either be a direct award or an award of services in lieu of funding. For service in lieu of funding, subrecipients will be given access to services through a State of Montana managed services and will not need to purchase services.

For projects with direct awards, sub-recipients must submit at least one payment request upon completion of the project to receive grant funds.

Applicants will be reimbursed by submitting proof of payment to MT DES, along with the required reimbursement request form and supporting documentation. Supporting Documentation must include:

- Proof of payment (i.e., general ledger or warrant check)
- Invoices
- Receipts

Reimbursements are allowable only for expenditures made during the grant period of performance.

10.3 Accruals

Sub-recipients with an open grant will be required to submit an accrual form prior to the end of the State Fiscal Year (SFY) to account for any expenditures or valid obligations that have occurred in the SFY and not been reimbursed prior to June 30. Sub-recipients that do not submit an accrual form and supporting documentation and then request reimbursement for goods or services from the prior SFY are at risk of non-payment due to lack of accrual funds.

11.0 Monitoring/Technical Assistance

11.1 Monitoring

Sub-recipients will be monitored by MT DES staff, both programmatically and financially, to ensure that the project goals, objectives, performance requirements, timelines, milestone completion, budgets, and other related program criteria are being met.

11.2 Technical Assistance

Technical assistance will be provided through desk-based reviews of financial reimbursement requests and project status reports. In addition, on-site technical assistance visits will be performed according to MT DES schedules, as requested, or as needed. Technical assistance will involve the review of the financial, programmatic, performance, compliance, administrative processes, policies, activities, and

other attributes of each Federal assistance award and will identify areas where further assistance, corrective actions or other support may be needed.

12.0 Project Closeout and De-Obligated Funds

12.1 Closeout

Closeout of SLCGP projects will be administered by MT DES upon determination of grant completion in accordance with 2 C.F.R. § 200.344 and upon receipt of a signed sub-recipient letter requesting closeout. MT DES will complete a project and file review prior to closing out a project and provide the sub-recipient with a closeout confirmation letter.

12.2 De-obligated Funds

Projects that are completed under budget will have funds de-obligated during the grant closeout process and will no longer be available to the sub-recipient. De-obligated funds will be utilized during the grant period of performance to fund additional projects. The Cybersecurity Planning Committee will make recommendations for re-awarding grant funds to eligible and approved projects. The committee reserves the right to conduct an interim application process for de-obligated funds.

13.0 MT DES Contact Information

MT DES will provide programmatic support and technical assistance for the SLCGP Grant. Contact the Preparedness Grants Team at MTDESGrants@mt.gov.