State and Local Cybersecurity Grant Application

Application Window Closes January 9, 2025, 11:55 pm

Submit Application to: MTDES Grants@mt.gov

Table of Contents

Application Guide: State and Local Cybersecurity Grant Program 2
General Information: Part A Applicant Information 4
General Information: Part B Applicant Assessment 5
General Information: Part C SLCGP Baseline Requirements 7
Focus Area 1: Security Awareness Training for the Workforce 8
Focus Area 2: Professional Development Training for the Technical Workforce 10
Focus Area 3: Endpoint Detection and Response 12
Focus Area 4: Network Traffic Monitoring 13
Focus Area 5: Multi-Factor Authentication 14

Application Guide: State and Local Cybersecurity Grant Program

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

This guide is intended as an overview to assist applicants with navigating the SLCGP grant application. Full program requirements can be found in State and Local Cybersecurity Grant Program State Guidance.

ELIGIBLE ACTIVITIES UNDER THE SLCGP

To meet the objectives stated in *The Department of Homeland Security FY22 SLCGP NOFO* (effective April 4, 2022), the Montana Cybersecurity Planning Committee designated **five specific project focus areas** that SLCGP will fund:

- **Focus Area 1:** Security Awareness Training for Workforce (SAT)
- **Focus Area 2**: Professional Development Training for Technical Workforce (PD)
- **Focus Area 3**: Endpoint Detection and Response (EDR)
- **Focus Area 4**: Network Traffic Monitoring
- **Focus Area 5**: Multi-Factor Authentication

The five focus areas provide an 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.

ELIGIBILITY REQUIREMENTS FOR LOCAL APPLICANTS

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

Awardees are not required to match (share) costs for the FY 2022 and 2023 SLCGP. Awardees will have to match costs for FY 2024 and FY 2025 awards. Match amounts for future award years are 30% for FY 2024 and 40% for FY 2025. Match may be in-kind (soft) from eligible activities. This application will award funds from FY22 and FY23 SLCGP.

STRUCTURE OF THE APPLICATION

This application consists of a general information section (**Part A, B, and C**) followed by the five focus areas. All applicants will complete the general information section containing:

- **Part A:** Applicant Entity Information
- **Part B:** Applicant Assessment
- **Part C**: Baseline Requirements

After completing the general information section (**Parts A, B, and C**) please complete the corresponding form for each focus area:

1. Security Awareness Training for the Workforce
2. Professional Development Training - Technical Workforce
3. Endpoint Detection and Response
4. Network Traffic Monitoring (County Networks)
5. Multi-Factor Authentication

On each of the five focus areas, use the YES or NO button to validate that you are requesting funding or services. When you request funding or services, please complete the General Information sections for which you are applying.

APPLICATION REVIEW AND AWARD PROCESS

MT DES will accept and review applications on a rolling basis until January 9, 2025, at 11:55 pm. After the application period closes, the SLCGP team at MT DES will review all submission based on order of submission. Award letters will be sent out to successful applicants by January 31, 2026. DES will award funding based on availability of funds.

The SLCGP application will act as the baseline of information necessary to review your request. If awarded, the SLCGP Coordinator will work with you to gather further information needed.

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, you will be given access to services through a State of Montana managed services and will not need to purchase services. For a direct award, you will receive grant funds as a reimbursement payment. You will submit a request for reimbursement after the purchase is made, and the invoice is paid. Proof of payment documentation is required for reimbursement approval.

SLCGP CONTACT INFORMATION

Submit completed application to MTDESGrants@mt.gov.

General Information: Part A
Applicant Information

Please fill out the following information to verify eligibility and contact information for the application.

UNIQUE ENTITY IDENTIFICATION NUMBER (UEI):

UEI is the required means for entity identification for federal awards government-wide. The UEI is a 12-digit number with a combination of letters and numbers.

Entity Name:

UEI:

Physical Address:

SIGNATORY AUTHORITY

The signatory authority listed below has been informed of the submission of this grant and may receive notice about reports submitted by the Authorized Representative/Project Manager.

Name of Signatory Authority:

Title: Email Address:

Physical Address:

PROJECT MANAGER / FISCAL OFFICER

Project Manager Name:

Email Address: Phone Number:

Physical Address:

Fiscal Officer or Agent Name:

Title:

Email Address: Telephone Number:

TYPE OF ENTITY

Select the organization type from the drop-down menu:

Special Districts

General Information: Part B
Applicant Assessment

FISCAL ASSESSMENT

1. Has the applicant organization substantially changed financial management or grant administration systems in the last 24 months?

   YES ◯ NO ◯

   If yes, what changes have been implemented to the financial management system?

2. Does the applicant organization's fiscal officer maintain written policies and procedures regarding the operation of all financial management systems?

   YES ◯ NO ◯

3. Has the applicant organization received federal awards directly from a Federal Awarding Agency in the last 24 months?

   YES ◯ NO ◯

   If yes, list the grant name and awarding agency. Please list up to the 5 most recent grants and agencies.

4. Has the applicant organization applied for any other grant funding to support the project for which you are submitting this application?

   YES ◯ NO ◯

5. Has the applicant organization had any audit or financial findings within the last 24 months?

   YES ◯ NO ◯

6. Does your jurisdiction or agency have a written and approved procurement policy?

   YES ◯ NO ◯

7. Does the entity have a real or potential conflict of interest?

   YES ◯ NO ◯

   If yes, please explain. There is no penalty for disclosing a conflict of interest.

CURRENT CYBERSECURITY ASSESSMENT

1. Does your organization employ in-house IT?

   YES ◯ NO ◯

2. Does your organization use an IT service provider?

   YES ◯ NO ◯

   If YES, who is your service provider?

3. Does your service provider provide a cybersecurity service package or separate services (i.e. Endpoint Detection and Response, Security Awareness Training (general workforce), Professional Development Training (IT workforce), Network Traffic Monitoring?

   ◯ Provides a cybersecurity service package or bundle

   ◯ Provides separate cybersecurity services (does not package or bundle services)

General Information: Part C SLCGP Baseline Requirements

If an applicant receives an SLCGP award for funding or services, the applicant agrees to complete, maintain, and report on the following required objectives or information:

1. Verify and maintain contact information for staff managing the SLCGP and inform MT DES of any changes to personnel and contact information.

Initials: _____

2. Submit performance reports using the Performance Progress Report Form detailing work accomplished with grant funds if awarded.

Initials: _____

3. Register and maintain CISA's no-cost Cyber Hygiene (CyHy) Services:

a. Vulnerability Services: 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.

b. Web Application Services: 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.

Get started by emailing vulnerability@cisa.dhs.gov *with the subject line: "Requesting Cyber Hygiene Services."*

Initials:_____

4. At time of award, your award packet will include a local consent agreement that allows the state of Montana to utilize the SLCGP funds to provide services or direct funding to eligible entities. A sample form can be found here:
https://des.mt.gov/Grant-Programs/State-and-Local-Cyber-Security-Grant-Program-Resources

Focus Area 1: Security Awareness Training for the Workforce

This focus area delivers education that seeks to equip all employees of an organization with the knowledge they need to make smart cybersecurity decisions throughout daily activities and communications.

Options include:

- **Option 1:** Obtain KnowBe4 licenses through the State of Montana contract for KnowBe4 Diamond-Tier cybersecurity training. A list of KnowBe4 features can be found here: KnowBe4 Security Awareness Training Pricing
- **Option 2**: Applicants may request direct funding to purchase licenses from a vendor of their choice that offers security awareness training. At a minimum, this training must provide simulated phishing attacks, domain monitoring, security awareness, and phishing campaign configuration.
- **Option 3:** Organizations with 50 or fewer employees may qualify for security awareness training managed by CyberMontana, a statewide initiative offered through the University of Montana Cybersecurity Center. Contact Joe Hodgeson for more information.

Final approval is contingent upon available funding

General Information

1. Are you applying for funds or services for Focus Area 1: Security Awareness Training for the Workforce?

   YES ◯ NO ◯

2. **If applying for security awareness training, please select one of the three options listed below:**

   ◯ KnowBe4 services obtained through the State of Montana IT Division

   - Number of licenses requested:

   ◯ Direct Purchase of security awareness training from vendor of your choice

   - Name of provider:
   - Total amount of funding requested:
   - Number of licenses:

   ◯ CyberMontana training services (only available to organizations with 50 or fewer employees)

   - Number of licenses requested:

3. Does your organization currently have an existing contract for security awareness training? Federal funds cannot be used to supplant existing obligations but may support or enhance capabilities.

   YES ◯ NO ◯

   Expiration date of current Security Awareness Training service contract (if applicable):

4. For educational institutions, what is the breakdown of standard licenses (faculty and staff) and student licenses?

   Standard Licenses:

   Student Licenses:

Focus Area 2: Professional Development Training for the Technical Workforce

This focus area delivers advanced cybersecurity training tailored for IT professionals.

- **Option 1:** Self-paced, on-demand course voucher available through the SANS Institute. Applicants will receive a voucher to enroll in any course of their choice from the SANS Cybersecurity Course Catalog. A bundled GIAC certificate of completion is included with this option.

  Applicants are not required to make any direct payment for the SANS course or associated class materials. The issued voucher fully covers the cost and serves as the method of payment.

  The SLCGP Coordinator will assist in delivering the voucher to the designated student upon application approval.

- **Option 2:** Applicants may request professional cybersecurity courses available through recognized providers such as CompTIA, ISC2, CyberMontana, and others. All training providers are subject to approval of the SLCGP committee.

  When registering for individualized training, course registration and payment are the responsibility of the applicant organization.

  Applicants will be reimbursed by submitting proof of paid registration to MT DES, along with the required reimbursement request form and supporting documentation.
  - Baseline reimbursement is $5,100.00 per organization
  - More than one student may receive training
  - Requested funding over $5,100.00 is subject to available funding and approval by MT DES

General Information

1. Are you applying for funds or services for Focus Area 2: Professional Development Training for the Technical Workforce

   YES ◯ NO ◯

2. If yes, what type of cybersecurity professional training is being requested? Choose one of the two options below:

   ◯ SANS Institute voucher

   ◯ Funding for direct purchase of training

   Please provide the job title of the employee(s) designated to receive the cybersecurity training:

   Name of training provider:

   Amount of funding requested:

   Guidelines for Direct Purchase:

   - More than one course may be funded
   - Baseline reimbursement is $5,100.00 per organization
   - More than one student may receive training
   - Requested funding over $5,100.00 is subject to available funds and approval by MT DES

Focus Area 3: Endpoint Detection and Response

This project provides licenses for SentinelOne, endpoint detection and response solution for servers and workstations through a State Information and Technology Services Division (SITSD) contract. For more information on the services provided through SentinelOne, visit the **SentinelOne Website:** https://www.sentinelone.com/.

General Information

1. Are you applying for Focus Area 3: SentinelOne endpoint detection and response solution?

   YES ◯ NO ◯

2. How many servers and workstations (i.e. desktops, laptops) do you anticipate supporting with grant funds?

   Servers:

   Workstations:

3. The applicant acknowledges their fiscal responsibility to pay a local match (cost share) for future years of service. Match amounts for each year of federal funding are FY 2022 (none), FY 2023 (none), FY 2024 (30%), and FY 2025 (40%). Local match may be in-kind (soft) from eligible activities. For planning purposes, the cost per end-point license is $63.00 and servers are $84.00 per year.

   Acknowledge: ☐

Focus Area 4: Network Traffic Monitoring

This project supports one-year service agreements for Network Monitoring and Management Intrusion Detection Systems to provide critical cyber incident early warning and reaction time to local government entities and school districts.

Applicants may request funding for a one-year service agreement including hardware and set-up for a network monitoring and intrusion detection system such as Albert Sensor system to provide security alerts for known cyber threats.

After purchasing the Network Monitoring and Management services, the applicant will request reimbursement from MT DES.

General Information

1. Are you applying for Focus Area 3: Funds for Network Traffic Monitoring?

   YES ◯ NO ◯

2. The applicant acknowledges their fiscal responsibility to pay a local match (share) for future years of service. Match amounts for each year of federal funding are FY 2022 (none), FY 2023 (none), FY 2024 (30%), and FY 2025 (40%). Local match may be in-kind (soft) from eligible activities.

   Acknowledgment: ☐

3. The applicant acknowledges that to support whole of state cybersecurity readiness, system alerts may be shared with the Montana Analysis and Technical Information Center (MATIC).

   Acknowledgment: ☐

4. Does your agency currently have an existing Network Traffic Monitoring service contract? *Federal funds cannot be used to supplant existing obligations but can support or enhance systems.*

   YES ◯ NO ◯

   If YES, what is the expiration of the current contract? Please note, existing contracts that expire within the grant period of performance may still qualify for services after the current contract expiration date passes.

Focus Area 5: Multi-Factor Authentication

This focus area provides security technology that requires multiple sources of unique information from independent categories of credentials to verify a user's identity for a login or other transaction, creating a layered defense that makes it more difficult for an unauthorized person to gain system access.

Applicants are eligible to request this focus area to initiate new multi-factor authentication capabilities, **OR** to increase existing multi-factor authentication capabilities

Funding may be requested for a one-year service agreement including hardware and set-up for a system from a recognized provider. All providers are subject to approval of the SLCGP committee.

- Procurement and payment are the responsibility of the applicant organization.
- Applicants will be reimbursed by submitting proof of payment to MT DES, along with the required reimbursement request form and supporting documentation.

Final approval is contingent upon available funding

1. Are you applying for funds or services for Focus Area 5: Multi-Factor Authentication

   YES ◯ NO ◯

2. Does your organization currently have an existing contract for Multi-Factor Authentication? Federal funds cannot be used to supplant existing obligations but may support or enhance capabilities.

   YES ◯ NO ◯

3. What is the anticipated costs?

Note: If awarded, MT DES will work with awardee to get final costs.