FFY 2022 State and Local Cybersecurity Grant Program

APPLICATION

MONTANA DISASTER AND EMERGENCY SERVICES

1956 Mt. Majo Street PO Box 4789

Fort Harrison, MT 59636

Released November 5, 2024

Submit Application to mtdesprep@mt.gov

Application Guide: FY22 State and Local Cybersecurity Grant Program

The FY22 State and Local Cybersecurity Grant Program (SLCGP) is a reimbursable pass-through grant program aimed at improving the cybersecurity posture of state and local government organizations by providing targeted assistance for managing and reducing systemic cyber risk.

Activities Eligible Under the FY22 SLCGP

To meet the objectives stated in the Notice of Funding Opportunity, the Montana Cybersecurity Planning Committee has identified four specific project areas to be funded by the FY22 SLCGP.

Applicants have the flexibility to apply for a combination of project areas according to the needs of their organization. Funding may be requested in one, two, three, or four of the defined project areas listed here:

- End User Cybersecurity Awareness Training
- Cybersecurity Professional Training
- Behavior-Based Endpoint Protection
- Network Monitoring & Management Intrusion Detection Systems

Eligibility Requirements for Local 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.

Cost share or match is not required for the **FFY 2022 SLCGP**. Future awards will have cost share requirements. Match amounts for future award years are as follows: FY 2023 20%, FY 2024 30%, FY 2025 40%. Local match may be in-kind/soft from eligible activities.

Structure of the Application

This application consists of a general information section followed by an attachment for each of the four project areas. All applicants will complete the general information section containing:

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

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

- End User Cybersecurity Awareness Training **Attachment 1**
- Cybersecurity Professional Training **Attachment 2**
- Behavior-Based Endpoint Protection **Attachment 3**
- Network Monitoring & Management Intrusion Detection Systems **Attachment 4**

On each of the four attachments, use the Yes/No button to indicate if funding or services are being requested.

When funding or services are requested, please provide the additional information requested for the project area.

Review and Award

Due to the unique structure and timeline of the FY22 SLCGP, applications will be accepted and reviewed on a rolling basis. Awards will be made based on available funding as projects are approved by MT DES and the Montana Cybersecurity Planning Committee. Regardless of award date, the Period of Performance for the FY22 SLCGP ends on June 30, 2026.

This guide is intended as an overview to assist applicants with navigating the FY22 SLCGP grant application. Full program requirements can be found in the guidance documents.

MT DES Contact Information

Send inquiries to the preparedness email at mtdesprep@mt.gov

PART A
Applicant Entity Information

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

UNIQUE ENTITY IDENTIFICATION NUMBER (UEI)_____
The 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.

ENITY NAME_____
ENTITY STREET ADDRESS_____
ENTITY CITY_____
ENTITY STATE_____
ENTITY ZIP CODE_____
COUNTY_____

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: _____
SIGNATORY AUTHORITY EMAIL ADDRESS: _____
SIGNATORY AUTHORITY PHONE NUMBER: _____

PROJECT MANAGER / FISCAL OFFICER

PROJECT MANAGER NAME: _____
EMAIL ADDRESS: _____
PHONE NUMBER: _____
STREET ADDRESS: _____
CITY: _____
STATE: _____
ZIP: _____

FISCAL OFFICER / AGENT: _____
FISCAL OFFICER NAME: _____
TITLE: _____
EMAIL ADDRESS: _____
TELEPHONE NUMBER: _____

TYPE OF ENTITY
SELECT THE ORGANIZATION TYPE FROM THE DROP-DOWN MENU

COUNTY GOVERNMENT

PART B
Applicant Assessment

FISCAL ASSESSMENT

- Has the applicant organization substantially changed financial management and/or grant administration systems in the last 24 months?

  ◯ YES

  ◯ NO

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

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

  ◯ YES

  ◯ NO

- 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 most recent 5.

- Has the applicant organization applied for any other grant funding to support the project that is being submitted?

  ◯ YES

  ◯ NO

- Has the applicant organization had any audit/financial findings within the last 24 months?

  ◯ YES

  ◯ NO

- Does your jurisdiction/agency have a written and approved procurement policy?
  - ◯ YES
  - ◯ NO
- 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

.GOV Domain Interest

At this time funding is not available to migrate entities to .GOV domains. MT DES is gathering information for future grant opportunities. Please note that schools are not currently eligible for .GOV domains.

- Does your organization currently use a .GOV domain?

◯ YES

◯ NO

- Is your Organization interested in migrating to a .GOV domain?

◯ YES

◯ NO

◯ DON'T KNOW

PART C
SLCGP Baseline Requirements

If Awarded funding or services through the State and Local Cybersecurity Grant Program, the applicant agrees to complete, maintain, and report of 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 quarterly performance reports using the Performance Progress Report form in the AmpliFund grant management system detailing milestones and work accomplished during the reporting period.

Initials: _____

3. Complete the no cost Nationwide Cybersecurity Review (NCSR) assessment administered by MS-ISAC during the first year of the sub-award period of performance and annually until grant closeout.

Initials: ____

4. 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:_____

5. Sign the local consent form that allows the state to utilize the SLCGP funds to provide services or direct funding to eligible entities.

Include a signed Local Consent Form in the application package when submitting.

DEPARTMENT OF MILITARY AFFAIRS
STATE OF MONTANA

Disaster & Emergency Services Division
1956 MT MAJO STREET - PO BOX 4789
FORT HARRISON, MONTANA 59636-4789
406.324.4777

THE HONORABLE GREG GIANFORTE
GOVERNOR

MAJOR GENERAL JOHN P. HRONEK
ADJUTANT GENERAL

FEDERAL FISCAL YEAR 2022
STATE AND LOCAL CYBERSECURITY GRANT PROGAM
LOCAL CONSENT AGREEMENT

I, _____, (printed name), the authorized agent on behalf of _____ (Local Governmental Entity) located at _____ (physical address) hereby expressly consent to the State of Montana's State Administrative Agency (SAA), namely the Montana Disaster and Emergency Services Division (MT DES), undertaking the following acts in accordance with the State and Local Cybersecurity Grant Program (SLCGP) for Fiscal Year (FY) 2022, Funding Opportunity Number DHS-22-137-000-01, as authorized by Section 2220A of the Homeland Security Act of 2002, as amended (Pub. L. No. 107-296) (6 U.S.C. § 665g):

- Retain up to $485,573 in SLCGP funds for FY 2022 at the State Level for Management and Administration, whole of state coordination, and training.
- Utilize $1,942,293 in SLCGP funding for the following projects approved in the State of Montana Cybersecurity Plan on behalf of and for the benefit of local governments:
    - $167,293 for end user security awareness training
    - $75,000 for cyber professionals training
    - $1,250,000 for behavior-based end-point detection and response solution
    - $450,000 for network monitoring and management intrusion detection systems

Funds and/or services provided to local and rural areas will align to the FY2022 SLCGP pass-through requirements. A minimum of 80% of federal funds, equivalent valued services, or a combination of funds and services provided under the grant will be provided to local governments, including a minimum of 25% to rural areas.

This consent is given freely and with the understanding that the Local Governmental Entity may receive items, services, capabilities, and activities (e.g. hardware, software, services) in lieu of funds from the SLCGP. This consent is only effective for the FY 2022 SLCGP funds.

Signed,

_____ _____
Signature Date

_____
Printed Name

_____
Title

ATTACHMENT 1
PROJECT – Build Cybersecurity Awareness
End User Cybersecurity Awareness Training

This project will provide funding for Cybersecurity end user training. The cybersecurity training must be annual at a minimum and include simulated phishing attacks, domain monitoring, security awareness, and phishing campaign configuration. Applicants my request up to $3.50 per license. An option to utilize the State procured contract for KnowBe4 diamond-tier cybersecurity training is available. Applicants may choose to request direct funding from a different vendor.

Are funds or services being requested for Building Cybersecurity Awareness:

- ◯ YES
- ◯ NO

What type of cybersecurity awareness training is being requested:

- ☐ State Contracted Services for End User Training (KnowBe4)
- ☐ Other End User Training
  - *If other, please identify what training is being requested and provide a short description*

How many licenses are being requested?

_____

Total Funds or equivalent cost for services: (Number of Licenses x Cost per license) Additional costs above 3.50/license will be the responsibility of the applicant.

0
_____

Briefly explain how the requested cybersecurity awareness training provides benefit to your agency and expected outcome.

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

- ◯ YES
- ◯ NO

What is the expiration date of the current contract:

_____

ATTACHMENT 2
PROJECT – Build a Professional Cybersecurity Workforce

This project will provide funding for cybersecurity training for IT privileged users and cyber professionals. Applicants may request up to $4,500 for this training; there is no guarantee that requested funds will be awarded. An option to receive a training through SANS Institute off the State Information and Technology Service Division (SITSD) is available. In this option, the state will purchase and issue out the training voucher to the approved applicant. Only one voucher per entity will be provided. Applicants may choose to purchase other cybersecurity trainings for their IT professionals. In this option, the applicant will be responsible for the purchase and request for reimbursement.

SANS Institute Courses and Certificates Website: https://www.sans.org/cyber-security-courses/

Are funds or services being requested for Building a Cybersecurity Workforce:

- ◯ YES
- ◯ NO

What type of cybersecurity awareness training is being requested:

- ☐ SANS Institute through SITSD
- ☐ Other Cybersecurity Professional Training

List the course name, course provider and description of the training being requested

Total Cost of course:

_____

Additional cost above $4,500 will be the responsibility of the applicant.

Provide a short job description for the IT/Cyber professional that will be receiving the cybersecurity training:

Recommended: Include a job description for IT/Cyber personnel if available.

ATTACHMENT 3
PROJECT – Server and Workstation Behavior-Based Endpoint Protection

This project provides behavior-based endpoint detection and response solution for servers and workstations for a whole-of state cybersecurity program. This project is only for licenses for SentinelOne antivirus software for workstations and servers. Contract and services will be provided through the State Information and Technology Services Division (SITSD). Service for FY22 is based on the terms of the contract. Entities may not receive a full 12 months depending on when you are onboarded to the system. The anticipated end date of the FY22 grant service is November 2025.

SentinelOne Website: https://www.sentinelone.com/

Are funds for SentinelOne behavior-based endpoint protection services being requested?

- ◯ YES
- ◯ NO

The applicant organization acknowledges and understands that there is a fiscal responsibility to pay local match for future years of services. Match amounts for each year of federal funding are FY 2023: 20%, FY2024: 30%, FY2025: 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: _____

How many endpoint devices (i.e. desktops, laptops) does your entity anticipate supporting with grant funds?

_____

How many licenses for servers are being requested?

_____

Estimated cost of services: $63 x # of endpoint device licenses: $ 0.00

$84 x # of server license: $ 0.00

Does your organization currently have an existing contract for behavior-based endpoint protection? *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.

_____

Please explain how the requested state services for behavior-based endpoint protection services provides benefit to your entity.

ATTACHMENT 4
PROJECT – Network Monitoring and Management Intrusion Detection Systems for County Networks

This project provides Albert Sensor Network Monitoring and Management Intrusion Detection Systems (IDS) for an additional layer of alerting and visibility to County Governments, Critical Infrastructure, Election, and Emergency Services. City governments and school districts may be eligible if funding is available. Applicants may request up to $13,560.00 (Small Average Utilization OMB-100MB) or $16,800.00 (Medium/Large Average Utilization 101MB-1.0GB) for a one-year service agreement including hardware for Albert Sensor IDS to provide security alerts for known cyber threats. The grant will also cover the one-time set-up fee of $950.00 per sensor. See the attached IDS Fact Sheet for CIS Albert Network Monitoring and Management attached at the end of this document for more information.

Are funds for an Intrusion Detection System being requested in this application?

- ◯ YES
- ◯ NO

The applicant organization acknowledges and understands that there is a fiscal responsibility to pay local match for future years of services. Match amounts for each year of federal funding are FY 2023: 20%, FY2024: 30%, FY2025: 40%. Local match may be in-kind/soft from eligible activities.

Acknowledgment: _____

The entity acknowledges and understands that Albert Sensor alerts will be shared with the Montana Analysis and Technical Information Center (MATIC).

Acknowledgment: _____

What size Albert Sensor does your entity anticipate supporting with grant funds?

- ☐ Small Average Utilization OMB-100MB for Service NOT Including Hardware - $11,160.00
- ☐ Small Average Utilization OMB-100MB for Service with Hardware - $13,560.00
- ☐ Medium/Large Average Utilization 101MB-1.0GB for Service NOT Including Hardware - $14,400.00
- ☐ Medium/Large Average Utilization 101MB-1.0GB for Service with Hardware - $16,800.00

How many Albert Sensors are being requested?

_____

Does your agency currently have an existing contract for an Intrusion Detection System? *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.

_____

Please explain how the requested Intrusion Detection System provides benefit to your entity.

CIS Center for Internet Security®

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

Elections Infrastructure ISAC®

31 Tech Valley Drive • East Greenbush, NY 12061 USA
518 266-3460 • www.cisecurity.org

About the Albert Sensor

Albert sensors are Intrusion Detection Systems (IDS) residing on State, Local, Tribal, and Territorial (SLTT) networks. These systems provide security alerts for known cyber threats, helping state and local governments identify malicious cyber activity. The Multi State Information Sharing and Analysis Center (MS-ISAC) threat intelligence and security operations personnel curate and update daily threat "signatures" from current cyber threat intelligence and reported cyber incidents. These signatures are then deployed to all Albert sensors to assist in identification of known malicious and anomalous activity. Alerts from the Albert sensors are monitored and managed 24/7/365 by the MS-ISAC Security Operations Center (SOC). For more information, visit https://www.cisecurity.org/services/albert-network-monitoring/.

Albert sensor – Quick Facts

- The Cybersecurity and Infrastructure Security Agency (CISA) funds the development and deployment of Albert sensors through the MS-ISAC. Many Albert sensors are also self-funded by SLTT government organizations.
- Albert sensor technology was specifically designed for use in state and local government organizations.
- As of early 2022, there are over 800 Albert sensors deployed across SLTT organizations. The MS-ISAC SOC receives more than 23,000 Albert "alerts" on average, each month.
- The Albert sensor is not a firewall. It passively monitors network traffic data (including logging "NetFlow" or metadata about network traffic); it does not block traffic and cannot negatively affect a member network or change the content or data traversing the network.
- The Albert IDS monitors traffic data as it flows across a network to look for matches against a set of signatures for known threats. If a match is found, an alert is sent to the MS-ISAC SOC for analysis and, if warranted, escalation to the SLTT partner. Albert sensors can only see traffic to and from devices on the network where the SLTT partner has chosen to deploy them and cannot inspect the contents of any encrypted traffic.
- The MS-ISAC SOC has no ability to "reach in" to a network and take action via an Albert sensor. If an alert is generated, any response and remediation activities must be done by the SLTT partner organization.
- Albert sensors, in combination with a layered "defense in depth" approach to cybersecurity, are proven to be highly effective in protecting against cyber threats, including known ransomware. While no IDS can detect 100 percent of malicious traffic, this capability enables network defenders to detect as much malicious activity as possible, providing a more complete picture of risk faced by SLTT governments.
- A holistic approach to cybersecurity for any organization, including SLTT government organizations and election offices, means both prevention through implementation of cyber hygiene best practices and defensive capabilities through employment of additional technologies and services like Albert sensors.

The use of Albert sensors in SLTT jurisdictions across the country has helped cybersecurity professionals understand patterns of malicious activity and inform jurisdictions how to proactively protect themselves.

###

Center for Internet Security®
CIS Services®

Contact
services@cisecurity.org
www.cisecurity.org
518-880-0699

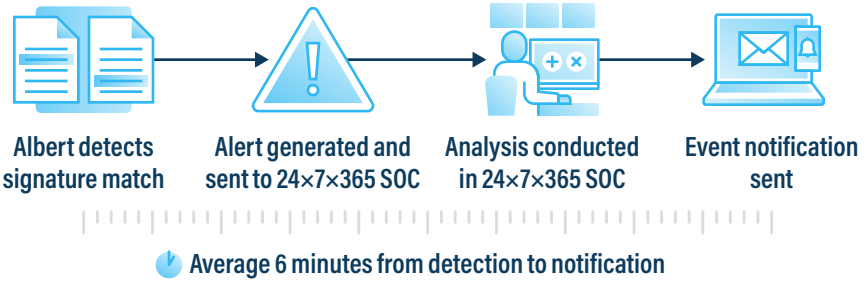
Albert Network Monitoring and Management

The Center for Internet Security, Inc. (CIS) offers a fully managed network security monitoring service called Albert. Albert is available to U.S. State, Local, Tribal, and Territorial governments, including elections entities, critical infrastructure, and public education. Albert can be used to monitor many types of traffic including networks with user workstations, web servers, or those hosting voter registration databases. Albert has the flexibility to monitor traffic at the edge and internally.

Albert provides network security alerts for both traditional and advanced network threats, helping organizations identify malicious and anomalous activity. This cost-effective Intrusion Detection System (IDS) uses open source software combined with the expertise of the CIS 24×7×365 Security Operations Center (SOC) to provide enhanced monitoring capabilities, cyber threat intelligence, and notifications of malicious activity, including full management of the device.

How Does Albert Work?

Albert looks for malicious activity by comparing network traffic to signatures that detect known malicious and anomalous activity. When a match is found, expert SOC analysts review for malicious activity and alert the customer of any valid threats. The basic lifecycle of an Albert event is as follows:



An IDS is only as effective as the signature set running on it. Albert utilizes a unique SLTT-focused and targeted signature set to ensure sensors rapidly recognize and alert on potentially malicious traffic occurring on the network.

Signatures and indicators of compromise

Albert utilizes commercial, open-source, and custom signatures developed from leveraging our federal partners for access to recently declassified signatures, indicators CIS derives from incident response cases, as well as member submitted and third-party threat data.

- Commercial Signatures
- Recently Declassified Signatures
- CIS Research – Threat Data Analysis CIRT Cases

Services Provided with Albert

- 24×7×365 network monitoring from the CIS SOC (U.S.-based)
- Alerts about potentially malicious activity
- Monthly activity summary reports

Additional Data We Collect

We collect data about the traffic, not what's in the traffic, in addition to alert data about the signatures firing.

1. Source IP
2. Destination IP
3. Source port
4. Destination port
5. TCP flags
6. Number of bytes of traffic sent and received
7. Timestamp information (start, end, and duration of connection)

Data can be analyzed in real time or retroactively through a query.

To find out more about network security monitoring, contact us today at services@cisecurity.org.

> "I now have a reliable, affordable, and trusted source that inspects ALL of my traffic in both directions."
>
> **Wesley Wilcox**
> Marion County, Florida Elections

Albert Network Monitoring Options

Organizations can opt to deploy more than one Albert sensor for high availability and can have them as an active/active or active/passive configuration.

	ALBERT ON-PREMISES
SENSOR TYPE	Physical sensor on your network
WHAT IT MONITORS	Monitors traffic on your on-prem network
SCALABLE BASED ON TRAFFIC	Yes
ALERTS ANALYZED BY CIS SOC	Yes

Pricing

The annual fee covers both the management and monitoring of Albert. CIS also offers a turnkey solution, which includes hardware.

Pricing is based on average internet connection utilization. A one-time initiation fee of $950 per sensor applies.

	CUSTOMER-PROVIDED HARDWARE			HARDWARE INCLUDED		
AVERAGE UTILIZATION	ANNUAL FEE (USD)	PER MONTH	PER DAY	ANNUAL FEE (USD)	PER MONTH	PER DAY
0MB–100MB	$11,160	$930	< $31	$13,560	$1,130	< $38
101MB–1.0GB	$14,400	$1,200	< $40	$16,800	$1,400	< $47
1.01GB–5.0GB	$26,400	$2,200	< $73	$30,000	$2,500	< $83
5.01GB+	Please contact services@cisecurity.org for more details.					

For More Information

To find out more about network security monitoring, contact us today at services@cisecurity.org.