



STATE AND LOCAL CYBERSECURITY GRANT PROGRAM (SLCGP)

Funding Opportunity Number: DHS-23-GPD-137-00-01

APPLICATION FOR COLORADO'S STATE AND LOCAL GOVERNMENTS

Grant Product Information: DHSEM intends to fund licenses for a year or more as funding allows. CrowdStrike Falcon® Complete MDR is a managed detection and response service that is used to stop technology breaches. CrowdStrike Falcon® Complete MDR provides detection, investigation, and response services to its customers 24/7/365. **Learn more at:**

[CrowdStrike's Introduction to Falcon® Complete](#)

[CrowdStrike's Falcon® Platform Frequently Asked Question \(FAQ\) Page](#)

Applicant Name:

Nicolle Rosecrans, Manager of Information Security and Compliance
Arapahoe County Government

1. For the purpose of this grant, a "rural area" is any area with a population less than 50,000 individuals. Further detail can be found in the following DOT statute:

[49 U.S.C. 5302](#) - Area or jurisdiction with less than 50,000 population. Please see Department of Commerce "urbanized area" definition if you have any questions.

Are you applying from a rural area?

No

2. An endpoint is a remote computing device that communicates back and forth with a network to which it is connected. Examples include: desktops, laptops, smartphones, tablets, servers, workstations, Internet-of-Things (IoT) devices.

What is the total number of endpoints in your system? (Please breakout workstation and server endpoints.)

2768 - Workstations; 354 Servers

3. Do you need protection for ChromeOS? If so how many Chromebooks do you have?

No

4. CrowdStrike supports the following operating systems: Windows, Linux, Mac, and AWS. What system(s) currently run on your endpoints?

Windows

5 Do you currently run an antivirus or endpoint protection product? If yes, which one(s) do you use?

Yes. Microsoft Defender Antivirus (unpaid version)

6. If awarded this grant, how many endpoints would you need to have protected? (Please breakout workstation and server endpoints.)

2768 workstations and 354 servers

7. Do you currently have an anti-virus, endpoint detection & response (EDR) solution, or a managed solution (MDR)? If so, what solution are you using?

No.

8. If you currently have a solution when does your contract end?

9. Will you allow the State of Colorado's Office of Information Technology to have visibility to your CrowdStrike portal?

This will give permission for OIT to only view data with no permission or access to your system.

Yes

10 If awarded this grant, will you give OIT permission to purchase the software licenses on your behalf? i.e. you will receive the product (software, licenses, and installation) not dollars. In addition, your agency agrees to have OIT procure the end user managed detection and response solution. This will reduce costs and increase service to your organization.

Yes

**COLORADO**

Division of Homeland Security
& Emergency Management
Department of Public Safety

STATE AND LOCAL CYBERSECURITY GRANT PROGRAM (SLCGP)**Application for Colorado's State and Local Governments**

Funding Opportunity Number: DHS-23-GPD-137-00-01

GENERAL INFORMATION AND INSTRUCTIONS

APPLICATION SUBMISSION DEADLINE: Tuesday, July 9, 2024 by End of Day

BACKGROUND AND PURPOSE

The potential consequences of cyber incidents threaten national security. Strengthening cybersecurity practices and resilience of state, local, and territorial (SLT) governments is an important homeland security mission and the primary focus of the State and Local Cybersecurity Grant Program (SLCGP). Through funding from Infrastructure Investment and Jobs Act (IIJA), also known as the Bipartisan Infrastructure Law (BIL), the SLCGP enables DHS to make targeted cybersecurity investments in SLT government agencies, thus improving the security of critical infrastructure and improving the resilience of the services SLT governments provide their community.

TIMELINE

Announcement Available:	May 28, 2024
Application Submission Deadline:	July 9, 2024
Notification of Award Recommendations:	July 26, 2024
Requests for Reconsiderations:	August 2, 2024

APPLICANT ELIGIBILITY

Eligible applicants include local governments as defined below:

“Local government” is defined in 6 U.S.C. § 101(13) as

- A) A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments, regional or interstate government entity, or agency or instrumentality of a local government;
- B) An Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; and
- C) A rural community, unincorporated town or village, or other public entity.

GRANT REQUIREMENTS

1. Applicants will be beneficiaries of the federal pass-through funds rather than sub-recipient.
2. Successful Applicants will report receipt of number of licenses and length services provided.
3. The FEMA funding requires the DHSEM & OIT to adopt cybersecurity best practices. (FY 23 NOFO SLCGP)
4. Applicants are encouraged to register with Cyber Hygiene Services -<https://www.cisa.gov/cyber-hygiene-services>.
5. Successful Applicants may need to track and report twenty (20) percent matching, in-kind costs.

INSTRUCTIONS

1. Enter applicant information in the [Applicant Info_Signatures](#) tab.
2. Obtain proper signatures on [Applicant Info_Signatures](#) tab. This can be printed, signed, and scanned if needed.
3. Enter project narrative information in the [Project Narrative](#) tab.
4. Submit the completed and signed [Applicant Info_Signatures](#) and [Project Narrative](#) documents.

Please submit all components of the application to:

cdps_slcgp@state.co.us

QUESTIONS & ASSISTANCE

Questions regarding the State and Local Cybersecurity Grant Program or any technical assistance completing your application should be directed to the following email address: cdps_slcgp@state.co.us, or Mary Byer at (303) 476-1598 or Liliya Levakin at (720) 656-4360.

Please check the website dhsem.colorado.gov frequently for any updates.

APPLICATION SUBMISSION DEADLINE: JULY 9, 2024 BY END OF DAY



STATE AND LOCAL CYBERSECURITY GRANT PROGRAM (SLCGP)

Funding Opportunity Number: DHS-23-GPD-137-00-01

APPLICATION SIGNATURE PAGE

The Recipient and responsible signatories certify by signing that they have read the Application including the Grant Requirements and will comply with, and follow, all requirements.

APPLICANT INFORMATION

Applicant Name

Applicant Agency Type

APPLICANT POINT OF CONTACT (POC)

Name of Applicant POC

Title

Agency

Address

City

State Zip Code

Primary Phone Number

Secondary Phone Number

Email Address

Signature

Date

AUTHORIZED OFFICIAL POINT OF CONTACT (POC)

Name of Authorized Official POC

Title

Agency

Address

City

State Zip Code

Primary Phone Number

Secondary Phone Number

Email Address

Signature

Date

IT DIRECTOR OR CONTRACTED AGENCY POINT OF CONTACT (POC)

Name of IT Director or Contractor POC

Title

Agency

Address

City

State Zip Code

Primary Phone Number

Secondary Phone Number

Email Address

Signature

Date