State and Local Cybersecurity Grant Program

Round Three –Open Quarterly

Application Instructions

Applications Due: 10:00PM on the last day of the Quarter
(March 31, June 30, September 30, December 31)

OREGON DEPARTMENT OF
EMERGENCY MANAGEMENT

Table of Contents

Starting on October 1, 2025, the State and Local Cybersecurity Grant Program (SLCGP) will collect applications throughout the year until all grant funds have been awarded. OEM will pull applications for review once every quarter.

All applications must be emailed to SLCGP.admin@oem.oregon.gov.

As you upload your documents, please use descriptive names for your files to support efficient processing and review. [Item]_ [City/County/Tribe/Special District] _[Short Title

For example, an application could be named:
"Application_GreeneCo_MFA"
"SLCGP_NW-water_gov migration"

This is a competitive grant. Applicants are responsible for the timely delivery of grant applications to the state administrative agency (SAA/OEM). Late applications or post-dated modifications to meet minimum qualifications will not be accepted. If you need assistance with applications, request assistance from Kevin Jeffries before the quarterly deadline. Late applications will be reviewed with the following quarter's applications.

Key Dates:
Project Period of Performance: 12 months or May 31, 2027, whichever is sooner.
Reporting Dates: April 15, July 15, October 15, January 15

Send questions to SLCGP.admin@oem.oregon.gov

Application Evaluation
The SAA (OEM) will review applications to determine whether proposals meet minimum qualifications described in the State and Local Cybersecurity Grant Program (SLCGP) Guidance and Notice of Funding Opportunity (NOFO). Qualified projects will be presented to the SLCGP Grant Review Committee for review and approval. Those recommendations will be presented to the SAA (OEM) for submission to FEMA and CISA.

Competitive Funds
Each city, county, tribe, or special district can submit up to two projects per quarter, regardless of the size. Applications that are submitted on behalf of a regional project are not counted against the city, county, tribe, or special district's two projects.

By default, applicants may not carry more than four projects at one time. However, depending on project progression, this limit can be adjusted by OEM.

To the greatest possible extent, applicants should pursue regional projects. Regional projects will receive priority in the competitive review process.

Regional Projects
Regional Projects are defined as projects that benefit adjacent or regional city, county, tribal, or special district jurisdictions. Partnering jurisdictions must be outside the applying city, county, tribal, or special district's geographic area. Regional projects must include letters of support from all beneficiaries named in the application. Regional projects must also describe how resources, training, or exercise will be shared.

For example,

- Educational service districts implement multifactor authentication for school districts that they service.
- Federated SOC for multiple entities.
- A county providing training for cities within the county.

Application Contents
To simplify the process and reduce paperwork, OEM has updated the application significantly. Only one application form is required. If your project is selected for funding, and if additional information is needed, OEM will work with successful applicants to provide needed details. Updated form is titled **2025 SLCGP Application**

Applicant Instructions

Step 1: Project Application

A project application must be completed for each proposed project. Each project may include multiple partner agencies but must be one cohesive project, not multiple projects with a similar focus. All projects must be completed within 12 months of award or May 31, 2027, which ever is sooner.

All applications must meet the following criteria:

- Must align to the goals and objectives in the Oregon Cybersecurity Plan
- Must align with one of the three service tiers
- Must address, unless already met, the four minimum requirements under the grant
    - Advanced Endpoint Protection (AEP)*
    - Domain Migration Services (Migration to .gov)*
    - Immutable Data Backup and Recovery Testing*
    - Multifactor Authentication Capability (MFA)*

I. Applicant information

- Provide the name, address, Unique Entity ID (UEI) and description of your agency.
- Provide organization's mission statement
- Provide info regarding status of cyber assessments
- Provide info regarding the four mandatory services

II. Project Details

- Select which cybersecurity service you will be perusing. Select one option.
- Provide a short narrative on what the project will
- Provide any price quotes you have received, if any
- Provide minimum budget details (Planning, Organization, Equipment, Training, Exercise)
- Provide short narrative describing how your project aligns with the State's Cyber Security Plan

III. Risk

As you consider your project to fill capability gaps to address Cyber Security, what threats, vulnerabilities and Consequences do you face as a result of this gap? Specifically, the service area you selected.

a) Threat – Describe the threat you are trying to guard against.
b) Vulnerabilities – Describe your vulnerabilities to that threat
c) Potential Consequences – Describe the potential consequences or impacts to your organization if this vulnerability is not resolved. What would happen if the threat was able to take advantage of the vulnerability?

IV. Solutions
In this section, consider your solution from the approved service catalog list above, to the risks identified in Part III.

- a) Identify the vulnerability (as selected in Secon III-B) to be addressed,
- b) Describe each proposed activity or investment (solution) to address the vulnerability.
- c) For each solution, include the actions, items quantity, plan, plan development, and estimated price.

V. Milestones, Project Management and Sustainability
Please list at least 4 milestones and estimated time (number of days, or weeks, or months) required to complete that milestone.

a) Describe the measurable outputs and outcomes that will indicate this was a successful project.
b) Describe the project team, their contact information, and their roles in the project
c) Describe how the project will be maintained.
d) Name your project

Step 2: Support Letters (Optional)

It is highly recommended that all projects seek letters of support from their local county or tribal emergency management, *though this is not a requirement for SCLGP Round 2*. It's important that your County or Tribal Emergency Manager is aware of your needs and capabilities. OEM will inform them of your project between the time you register and your application deadline.

Regional Projects
Support letters are required for regional projects. Letters should be in Word or PDF form and uploaded into your SLCGP Application Folder in OEM's FTP site.

Step 3: Support Material / Appendices (Optional)

Include all required support materials for the projects. If the project requires submission of promulgated plans, the page and paragraph being referenced in the application must be

submitted in the appendices. For example, all communications projects must be supported with communications strategies and plans.

FINAL STEP:

Email all application to SLCGP.admin@oem.oregon.gov. Only one Application per email. Up to two applications per organization per application period (quarter).

For questions or issues with your application, please contact the State and Local Cybersecurity Grant Program coordinator, Kevin Jeffries.

Kevin Jeffries
Homeland Security Grant Program Coordinator
Oregon Department of Emergency Management
971-719-0740
kevin.jeffries@oem.oregon.gov

For technical questions about cyber security systems, equipment, or services please contact the Oregon Department of Administrative Services, Enterprise Information Services (EIS).

SLCGP Technical Assistance
Enterprise Information Services
Cyber Security Services (CSS)
slcgp_info@das.oregon.gov

###