



# State and Local Cybersecurity Grant Program

*Round Two*

## Program Guidance

**Applications Due:** October 15, 2024 @ 10:00PM



OREGON DEPARTMENT OF  
EMERGENCY MANAGEMENT

# Table of Contents

<b>Application Evaluation .....</b>	<b>4</b>
<b>Funding Distribution .....</b>	<b>4</b>
Competitive Funds .....	4
Regional Projects.....	4
<b>Application Contents.....</b>	<b>4</b>
<b>Applicant Instructions .....</b>	<b>5</b>
Step 1: Combined Coversheet .....	5
Step 2: Sub-applicant Coversheet.....	5
NEW STEP: How to Save and Submit the Sub-applicant Coversheet .....	6
Step 3: Project Application.....	6
I. General Project Information .....	6
II. Requirements.....	7
III. Specific Requirements.....	7
IV. Project Details.....	7
V. Project Impact.....	8
VI. Capability History.....	8
VII. Gap Information.....	8
VIII. Sustainment.....	8
IX. Milestones.....	8
Step 4: Budget.....	9
Step 5: Support Letters for Regional Projects.....	10
Step 6: Support Material / Appendices.....	10

### Round two of the State and Local Cyber Security Grant Program

For SLCGP, each city, county, tribe, and special district will submit applications through a secure FTP site provided by OEM. After registering, OEM will confirm who is eligible to apply. Access to the FTP site will be provided to those who are eligible to apply.

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]\_[Application #]

For example, an application could be named:

“Application\_GreeneCo\_MFA\_2”

“SLCGP\_GreeneCo\_Training\_2”

**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 deadline of October 15 by 10pm.**

#### **Key Dates:**

**Registration:** August 1, 2024 through September 1, 2024 <https://forms.office.com/g/wZ4gjDtFPC>

**Application Deadline:** October 15, 2024 @ 10pm

**Grant Review completed by:** November 15

**Award Recommendations submitted to Dept. of Homeland Security:** December 1, 2024

**Award Notices to applicants:** January February of 2025

**Period of Performance:** January 1, 2025 Through December 31, 2026 (24 months)

**Reporting Dates:** April 15, July 15, October 15, January 15

Kevin Jeffries  
Grants Coordinator  
Oregon Department of Emergency Management  
971-719-0740  
[kevin.jeffries@oem.oregon.gov](mailto:kevin.jeffries@oem.oregon.gov)

## Application Evaluation

The SAA (OEM) will review applications to determine whether proposals meet minimum qualifications described in the FY23 State and Local Cybersecurity Grant Program (SLCGP) Guidance and FY23 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.

## Funding Distribution

### Competitive Funds

For Round Two SCLGP, each city, county, tribe, or special district can submit up to two projects, 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.

To the greatest extent possible, applicants should pursue regional projects. During the Round Two grant cycle, 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 implementing multifactor authentication for school districts that they service.
- Federated SOC for multiple entities.
- A county providing training for cities within the county.

## Application Contents

All applications must be completed and submitted through your SLCGP application folder in through the OEM FTP site. This process must be completed for all applications.

A completed city, county, tribal, or special district application packet will include:

- Combined coversheet (*Word document*)
- For each project, in the following order:
  - Sub-applicant coversheet for each project requesting funding, (*MS Forms*)

- Project application (*Word*)
- Detailed line-item budget for each project requesting funding (*Excel*)
- Signed support letters for regional projects (pdf)

## Applicant Instructions

### Step 1: Combined Coversheet

Combined coversheet: A combined coversheet must be completed by the submitting city, county, tribe, or special district and included with the original application. Please list the regional project after local projects and place [\*] next to the applying agency's name. *Funding requests, and project names must be consistent throughout the application packets or risk disqualification.*

- a. City, county, tribal, or special district contact name, phone number and email (*should be the agency and individual submitting the application packet into the FTP*)
- b. Total funds requested within the entire application packet  
---
- c. Name of local agency requesting funds (per project)
- d. Funding requested for each project
- e. Name of projects

The combined coversheet does not need to be signed. Please submit it to the SAA(OEM) as a word document, not a PDF.

### Step 2: Sub-applicant Coversheet

**Please follow these instructions carefully. Failure to complete this step could result in your application being disqualified.**

For each project listed on the combined coversheet, a sub-application coversheet must be completed. A link to that questionnaire is embedded in the combined coversheet. You also can access the questionnaire here: <https://forms.office.com/g/wZ4gjDtFPC>

The sub-applicant coversheet questionnaire provides information directly related to subgrant agreements and must be completed in full. Coversheets must be completed for each agency that will directly receive funds. Information included in the coversheet questionnaire includes:

- Name of the city, county, tribe, or special district applying
- Name of the agency seeking funds
- Project title
- Project combined coversheet assigned number
- Amount of funds requested
- Program and fiscal contact and information, including mailing address, should be the individual who will be able to answer questions regarding the project throughout the life of the grant

- Service Catalog Offering
- Agency federal tax identification number
- EU-ID number (replaced DUNS number)\*

**\*Additional information on the new SAMS UE-ID number:**

<https://www.gsa.gov/about-us/organization/federal-acquisition-service/office-of-systems-management/integrated-award-environment-iae/iae-systems-information-kit/unique-entity-identifier-update>

## **NEW STEP: How to Save and Submit the Sub-applicant Coversheet**

When you have completed the questionnaire, your information will be automatically stored in a database. You also must print a copy BEFORE you click submit on the Forms questionnaire.

To save your work, right-click on the questionnaire and select Print to Save as a PDF. You will need to save a copy for your records. It is also highly recommended you upload your PDF into the FTP site with your other application documents.

## **Step 3: 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 proposed projects must be completed no later than **December 31, 2026**.

All projects must meet the following criteria:

- Must align to the goals and objectives in the Oregon Cybersecurity Plan
- Requirements of the Notice of Funding Opportunity (NOFO) must be met prior to applying for additional Tier 1 or Tier 2 services
- Must be an SLCGP Service Catalog Tier 1 or Tier 2

### **I. General Project Information**

**Applicant agency:** Identify the agency or agencies that will receive direct awards.

**Project title:** Assign each project a unique title that concisely describes the project. Please make sure this title is consistent throughout all your documents.

**Federal funds requested:** Provide the total funds requested through the grant.

**SLCGP Service Catalog:** Select which Service Catalog offering your agency will be applying for funding for.

**SLCGP Strategy GOAL#:** Provide which strategic SLCGP goal your agency's proposal aligns with.

**SLCGP Strategy OBJECTIVE #:** Provide the strategic SLCGP objective your agency's proposal aligns with.

**Project budget defined by POETE:** Provide detailed budget based on the provided categories. POETE = Planning, Organization, Equipment, Training, Exercises

Attribute Name	Description	Application Instructions
Planning	Dollar amount of the project supporting planning	Identify the amount of funds in the project that will be for planning activities.
Organization	Dollar amount of the project supporting organization	Identify the amount of funds in the project that will be for organization activities.
Equipment	Dollar amount of the project supporting equipment	Identify the amount of funds in the project that will be for the purchase of equipment.
Training	Dollar amount of the project supporting training	Identify the amount of funds in the project that will be for training activities.
Exercises	Dollar amount of the project supporting exercises	Identify the amount of funds in the project that will be for exercise activities.
Total	Total dollar amount for the project.	Automatically generated by the GRT from the sum of the POETE cost categories.

## II. Requirements

**Describe the cybersecurity nexus of this project:** Clearly describe how this project will address a cybersecurity gap/gaps, and how that will allow you to improve your current cyber capability.

**Describe how the project address Cyber Capability Gaps:** Clearly describe how the project ties to Oregon’s SLCGP Cybersecurity Plan.

## III. Specific Requirements

### Cybersecurity

**Describe any cyber assessment that has been completed in the last three years.** Has the jurisdiction performed a formal cyber assessment?

**Provide an overview of your cybersecurity plan or strategy, if applicable.** If the jurisdiction has not performed a formal cyber assessment, does the jurisdiction have a formal cyber security plan/strategy?

## IV. Project Details

**Describe the project.** What will this project do?

- Provide a detailed summary of what is being implemented and describe what is driving the need. Mainly prioritized business drivers.
- Identify what is in scope for this project, and what is out of scope. What are the metrics used to measure the success of this project?
- Detail what SLCGP goals and objectives the project aligns to. Please be as clear and direct as possible in your first paragraph. Supporting details may be provided in 2<sup>nd</sup> or 3<sup>rd</sup> paragraphs.

**Provide projected costs, if applicable.** Have you received quotes for the costs of the items, training, or services described above?

## **V. Project Impact**

**Describe who in the community will be directly impacted by this project and how.**

**Describe what impact this project will have on the whole community.** Provide details of who is specifically impacted by this project and how it will impact the whole community.

**Describe how the project will enhance the cyber capability for the jurisdiction.** Describe in some detail what cybersecurity services are going to be improved and how. Furthermore, include how the improvement is measured.

## **VI. Capability History**

**Describe the jurisdiction's current functionality in the chosen cyber capability.** Provide details on jurisdictions current state, including resources, skills, capabilities, etc.

## **VII. Gap Information**

**Describe the current gap in the cyber capability.** Provide details on the jurisdiction's lack of resources, skills, capabilities, etc. and how they were identified. Describe any attempts to fill the gap, and how this project will aid in addressing the gap.

**Describe how the gap was identified (real event, exercise, assessment).**

**Describe what the agency/community has done to fill the gap so far.** Provide details regarding any work which has already been done.

**Describe how the proposed project will fill the gap.** Will the project completely solve the issues, or will it get the agency/jurisdiction a percentage of the way there? What else will be needed to fill the gap?

## **VIII. Sustainment**

**Describe the jurisdiction's plan to sustain the cyber capabilities built by this project.** Provide detail on the jurisdiction's plan to sustain the project after implementation, including funding, resources, skills, capabilities, etc.

## **IX. Milestones**

The milestone list is a high-level view of the project for planning purposes. Each milestone has duration, and the overall project timeline is given. Please note that most tasks occur in parallel to achieve the overall timeline milestone goal. Many of the tasks performed during detailed planning have either been completed or are substantially complete so the total project time is extremely compressed. The graphic below is an example milestone list.





### Step 4: Budget

Each direct recipient must have its own unique budget for every project. All budgets must be completed on the provided budget sheet. The budget must be submitted through SLCGP Application Folder in OEM’s FTP Site.

The current Authorized Equipment List (AEL) is available at <https://www.fema.gov/authorized-equipment-list> (Note: The AEL has been updated and should be reviewed closely.)

For **Equipment** costs, include:

- Service Catalog Category
- Which agency and discipline will receive the equipment? Identify the quantity allocated for each agency and/or discipline that will receive the equipment.

For **Training** costs, the budget must:

- Specify the name of the course or vendor.
- Specify how many participants will receive the training (by discipline and function).
- Include a line-item breakdown of expenses (facility rental, materials, instructor fees, etc.).

For **organizational, planning and exercise** costs, the budget must include a line-item breakdown including the following expenses: personnel, contractual services, travel, supplies, rent and utilities, etc.

**Consistently denied equipment items or approaches include:**

- Projects not aligned to the SLCGP Cybersecurity Plan and included in the service catalog.
  - Equipment not supported or well documented in the project worksheet.
  - Project items listed in budget without narrative to support or justification.
- 

### Step 5: Support Letters

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 6: Support Material / Appendices

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.

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](mailto:slcgp_info@das.oregon.gov)