State and Local Cybersecurity Grant Program

Round Two

Program Guidance

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

Updated October 1, 2025

OREGON DEPARTMENT OF EMERGENCY MANAGEMENT

Table of Contents

Introduction

State and Local Cybersecurity Grant Program

The State and Local Cybersecurity Grant Program (SLCGP) supports implementation of state, city, county, and special district cybersecurity improvements and supports cybersecurity practitioners across local jurisdictions.

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.

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

Eligibility

Eligible applicants for competitive awards include local and tribal units of government. “Local unit of government” means “any county, city, village, town, district, borough, parish, port authority, transit authority, intercity rail provider, commuter rail system, freight rail provider, water district, regional planning commission, council of government, Indian tribe with jurisdiction over Indian country, authorized Tribal organization, independent authority, special district, or other political subdivision of Oregon.”

Eligible projects must have a demonstrated nexus to achieving target capabilities related to improving, preventing, preparing for, protecting against, and responding cybersecurity incidents and best practices.

Available Funding

Funding Distribution

The state administrative agency (SAA/OEM) must obligate at least 80 percent of funds awarded to local and territorial governments, with 25 percent of that going to rural areas. The SAA (OEM) may retain up to five percent of funds awarded for administration, and the remaining 15 percent will be allocated to the state government.

For this grant, rural jurisdictions are defined as any area with a population of less than 50,000 individuals.

Funds will be distributed through a competitive application process (competitive awards).

Competitive Grants and the Review Committee

The grant review committee will be the SLCGP Planning Committee. The committee is comprised of not more than 15 individuals selected to represent the various geographic areas, disciplines and

demographics of the applicant jurisdictions as defined in the Notice of Funding Opportunity (NOFO). The group will conduct a comprehensive, fair, and impartial evaluation of competitive grant applications and create a ranked list of projects.

The grant review committee's approvals will be submitted to the director of the SAA for submission. The final ranked approved list will be used once final funding levels are known. A project with a funding recommendation on the project ranked list is NOT a guarantee of funding approval.

No project is officially funded until a contract has been issued to successful applicants. Contracts will be sent within 45 days following SAA (OEM) receiving our award from FEMA. DO NOT obligate any funds until a grant contract has been received and fully executed with signatures from SAA (OEM) and your organization. You may proceed with no cost actions, such as seeking bids and quotes for goods and services, before receiving an executed agreement.

Funding decisions will be based on:

1. Overall responsiveness to the required project application worksheets and forms.
2. How well the applicant describes the project with a clearly identified gap and solution that aligns with Oregon Cybersecurity Plan.
3. The impact the project has on the applicant's community, especially underserved and underrepresented communities.
4. Whether proposed projects can be implemented within the one-year grant period of performance.
5. Whether projects will be sustained after grant funding expires.

Duration of Funding (Period of Performance)

For projects funded by the FY23 SLCGP, all projects must be completed within 12 months or by May 31, 2027, which ever is sooner. Projects funded by FY24 or FY25 SLCGP, the period of performance will be 12 months. Requests for time extensions but be received by OEM within the last quarter of the project. Approval of time extensions will be based on previous performance and reporting compliance, time available, and practicality of the proposed plan to complete the project.

Funding Reimbursement

The SLCGP is a reimbursement grant. Grant subrecipients must provide invoices and proof of payment to receive grant fund reimbursement for all eligible expenses. Quarterly reports describing activities that resulted in eligible expenses must be submitted with requests for reimbursement. Requests for reimbursements (RFR), must be submitted at least once per quarter if you spent funds during the previous quarter. If you have no expenses during that period, you will disclose that on a fiscal and programmatic report that is due by the 15th of the month following the last month of the quarter. Final or closeout RFRs and quarterly reports must be submitted within 30 days of the end of the period of performance. RFRs submitted after 30 days may not be processed.

State Funding Priorities

Projects must implement at least one of the Oregon Cybersecurity Plan Service Catalog offerings. The Service Catalog offerings are based upon the Oregon Cybersecurity Plan and federal priority areas designated in the SLCGP Notice of Funding Opportunities (NOFO).

Those italicized and marked * are required services applicants must have in place before they can seek funding for any other services, either in tier 1 or tier 2.

Tier 1 Services

- *Advanced Endpoint Protection (AEP)**
- *Domain Migration Services (Migration to .gov)**
- *Immutable Data Backup and Recovery Testing**
- *Multifactor Authentication Capability (MFA)**
- Albert Sensors
- Information Security Awareness Training
- URL/Web/Content filtering
- Vulnerability Management Services & Scanning
- Consulting and Planning Services

Tier 2 Services

- Converged Endpoint Management (XEM)
- Cybersecurity Risk Assessment Services
- DNS Filtering
- Email Security Gateway
- Enhanced Network Protection – Firewall Services
- Identity & Access Management Solutions
- Mobile Device Management (MDM) Solutions
- Penetration Testing Services
- Privileged Access Management (PAM)
- Web Application Firewall (WAF)

Tier 3 Services

- Application Security Services
- Security Information and Event Management (SIEM) Technology
- MDR/XDR Solutions
- Statewide Federated SOCs

Applicant Requirements

To be eligible to receive Round Two State and Local Cybersecurity Grant Program funding, applicants must have met all compliance requirements found in the NOFO under which they are seeking funding.

Match Requirement

The federal government waived the requirement for a match for FY22 and FY23 for the State and Local Cybersecurity Grant Program projects. FY24 funded projects may require a 30% match. FY25 funded projects will require a 40% local match. OEM is seeking a cost share waiver for FY24. At the release of this guidance, FEMA has not yet made a decision.

Supplanting

Federal funds may not supplant, replace, or offset state or local funds but will be used to supplement the amount of funds that, in the absence of federal funds, would be made available for purposes consistent with the SLCGP.

Applications

Applications will be submitted by State, City, County and Special Districts electronically through Secure FTP and a Web-based sub-applicant cover sheet. The link and access to the OEM FTP site will be provided to those deemed eligible to apply

Program Information

LSCGP funds may be used for any of the Tier 1, 2 or 3 Service Offerings in the Oregon Cybersecurity Plan Service Catalog that support the goals and objectives of the State and Local Cybersecurity Grant Program. ***However, applicants must first have the requirements of the CISA Notice of Funding Opportunity in place:***

- Advanced Endpoint Protection (AEP)
- Domain Migration Services (Migration to .gov)
- Immutable Data Backup and Recovery Testing
- Multifactor Authentication Capability (MFA)

For a complete list of services available under this grant program, see the Oregon Cybersecurity Plan

Reporting and Reimbursements

Program Narrative Reports – Quarterly Progress Reports Fiscal Report

Subrecipients will be required to submit quarterly progress and fiscal reports that contain specific information regarding the activities carried out under the Round Two State and Local Cybersecurity Grant Program. A template of the project-specific quarterly narrative progress report that includes approved milestones will be sent to subrecipients with executed agreements. Quarterly Reports must be submitted via email to slcgp.admin@oem.oregon.gov no later than 15 days following the end of each calendar quarter (March, June, September, December).

Progress reporting must clearly identify the efforts associated with the approved milestones listed in project-specific narrative progress report form.

RFR (Requests for Reimbursement)

Reimbursements will be made only for actual expenses. Requests for reimbursement (RFR) **must** be submitted quarterly if you have expenses during the previous quarter.

All requests for reimbursement must include supporting documentation to substantiate claimed expenses. Accurate and clear expenditure information will be required before reimbursement is made. Reimbursements are made only for equipment purchased and/or services performed during the grant period. A project-specific electronic version of the RFR form that includes the approved budget will be sent to subgrantees with executed agreements.

Actual Requests for reimbursement may be submitted as often as once a month, but no less than once a quarter.

Requests for reimbursement may be submitted via email to slcgp.admin@oem.oregon.gov no later than 15 days following the end of each calendar quarter (March, June, September and December). Reimbursements may be delayed if quarterly program narrative reports have not been submitted.

Please be clear, thoughtful, and consistent with the naming of your documents and attachments. If we must search your forms for answers, your reimbursement will be delayed.

Suspension or Termination of Funding

The SAA(OEM) may suspend or terminate funding, in whole or in part, or impose other restrictions for any of the following reasons:

- Failing to make satisfactory progress toward the goals, objectives or strategies set forth in the project worksheet.
- Failing to follow grant agreement requirements, or standard or special conditions,
- Proposing or implementing substantial plan changes to the extent that, if originally submitted, the project would not have been selected for funding.
- Failing to submit required reports.

- Filing a false certification in this application or other report or document.

Before taking action, the SAA (OEM) will provide the subrecipient with reasonable notice of intent to impose restrictions and will make efforts to resolve concerns.

Award Administration Information

Record retention

All award recipients must maintain records relating to their grant award including but not limited to, contracts, agreements, request for reimbursement, monitoring and audit findings, procurement records, and reports for at least Six (6) years following the end of their project.

Programmatic Required Assurances

For required assurances, please review the current year's U.S. Department of Homeland Security Grant Program Notice of Funding Opportunity (NOFO) with the understanding that any new assurances included in the NOFO will be included in grant agreements.

Procurements Standards

General

Agencies must follow the same policies and procedures used for procurement from non-federal funds, in accordance with the appropriate OMB Circular (OMB Circular A-110 or OMB Circular A-102).

Standards

Subrecipients must use their own procurement procedures and regulations, provided that the procurement conforms to applicable federal laws and standards.

Adequate Competition

All procurement transactions, whether negotiated or competitively bid and without regard to dollar value, shall be conducted in a manner so as to provide maximum open and free competition.

Sole Source Procurement (Non-Competitive)

All non-state procurement transactions must be conducted in a manner that provides, to the maximum extent, practical, open and free competition. However, should a subrecipient elect to award a contract without competition, sole source justification may be necessary.

Justification must be provided to SAA (OEM) for all non-competitively procured goods and services in excess of $100,000. Justification should include a description of the program and what is being contracted for, an explanation of why it is necessary to contract non-competitively, time constraints, and any other pertinent information. Subrecipients must provide evidence of their due

diligence and provide a local legal opinion for why the sole source procurement is justified and in accordance with local, state, and federal procurement law. *SAA (OEM) will not reimburse projects that lack this documentation*.

Non-Competitive Practices

The subrecipient must be alerted to organizational conflicts of interest or non-competitive practices among contractors that may restrict or eliminate competition or otherwise restrain trade. Contractors that develop or draft specifications, requirements, statements of work, and/or requests for proposals (RFPs) for a proposed procurement shall be excluded from bidding or submitting a proposal to compete for the award of such procurement. Any request for exemption must be submitted in writing to the Oregon Department of Emergency Management.

Any questions regarding this document and its guidance should be directed to:
Slcgp.admin@oem.oregon.gov