State and Local Cybersecurity Grant Program

Program Guidance

Release Date 10/1/2023

Round 1 Applications Due: 5 p.m. on January 10, 2024

Pre-Registration Deadline: November 15, 2023

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.

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 to 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 counties and cities from counties with a population of less than 50,000.

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 (OEM) 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 the 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

Successful applicants are awarded grants with a period of performance of 24 months and are meant to be a one-time opportunity, not a year-over-year funding opportunity. Projects must be completed, and grants closed before the period of performance ends once all milestones are completed.

For Round 1 Funded Projects, the period of performance will run April 1, 2024, through March 2026.

Reporting and Reimbursement

The SLCGP is a reimbursement grant. Grant subrecipients must provide updates to the State Administrative Agency (OEM) quarterly, using reporting forms provided by OEM. Subrecipients will provide programmatic and fiscal progress reports quarterly.

For Reimbursements, subrecipients must provide invoices and proof of payment to receive reimbursement for all eligible expenses. Using a Request for Reimbursement (RFR) form provided by OEM, subrecipients must request reimbursement by the 15th of the month following the end of the quarter in which the expense was incurred. Quarterly request for reimbursement is the expectation of this grant, but subrecipients may request reimbursement monthly if required to meet local financial needs and only after receiving the written approval by OEM. Final or closeout RFRs may not be processed if received after the 15th of the month following the final quarter.

State Funding Priorities

For SLCGP- Round 1, 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 FY22 SLCGP NOFO.

Round-1 Oregon Cybersecurity Plan Service Catalog Offerings – 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

Applicant Requirements

To be eligible to receive State and Local Cybersecurity Grant Program funding, applicants must have met all compliance requirements.

Match Requirement

There is currently no local match requirement to apply for SLCGP funds. Future SLCGP opportunities may require local matching funds.

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 a secure portal and a Web-based sub-applicant project screening form.

Program Information

For round 1, State and Local Cybersecurity Grant Program funds may be used for any of the Tier 1 Service Offerings in the Oregon Cybersecurity Plan Service Catalog that support the goals and objectives of the State and Local Cybersecurity Grant Program. For Tier 1 Service Offerings, see the table below.

	CYBER Services	CYBER Services Governance	
CYBER Services	Description/Rationale	CYBER Service Tier	CIS Control(s)
Advanced Endpoint Protection (AEP)	*This is an IT product that offers endpoint protection with the enhancements of machine learning and may include cloud computing, email, and other solutions. The products are generally offered as either Endpoint Detection and Response (EDR) or Extended Detection and Response (XDR).*	*Tier 1*	*10*
Domain Migration Services (Migration to .gov)	*Domain migration is the process of moving an entity-registered domain from one root to the other. Movement of domain names services to another involves a transition plan depending on the complexity of the entity's operation. Several things need to be considered to ensure the migration is successful and doesn't affect a business performance internet-based service.*	*Tier 1*	
Immutable Data Backup and Recovery Testing	*Data backup as a service that meets or exceeds business expectations. Data resilience refers to the ability of any data storage facility and system to bounce back despite service disruptions, such as power outages, data corruption, natural disasters, and equipment failure. It is often part of an organization's disaster recovery plan.*	*Tier 1*	*11*
Multifactor Authentication Capability (MFA)	*An authentication system that requires more than one distinct authentication factor for successful authentication. Multifactor authentication can be performed using a multifactor authenticator or by a combination of authenticators that provide different factors. This additional protection can be applied to internal or external resources, or both.*	*Tier 1*	6
Albert Sensors	*An IDS (Intrusion Detection System) solution from the Center for Internet Security that can provide a second layer of detection as well as incident response and around-the-clock support.*	Tier 1	13
Information Security Awareness Training	*Reveal your organization's employees' strengths and weaknesses and empower them against cyber criminals. Employees are part of an organization's attack surface, and ensuring they have the know-how to defend themselves and the organization against threats is a critical part of a healthy security program. If an organization needs to comply with different government and industry regulations, it must provide security awareness training to employees to meet regulatory requirements.*	Tier 1	14

URL/Web/Content filtering	*An IT service, provided as an appliance or an add-on to a next-generation firewall, that allows for the blocking of web content based on categorical classification. This service generally allows for exceptions, based on role, as well as logging information for those exceptions or potential policy violations. Some also provide additional protections for files downloaded from or by websites.*	Tier 1	9
Vulnerability Management Services & Scanning	*Vulnerability management services are designed to identify security holes within an organization's IT infrastructure, specifically related to cyber threats. Vulnerability assessment services run a series of diagnostics on an entity's devices, applications, and networks, and utilize this data to recommend areas for improvement based on urgency and scope.*	Tier 1	7
Consulting and Planning Services	*This service allows for eligible entities to procure assistance with the planning and implementation of other products and services in this catalog, along with other, general planning needs, such as those that would align GRC activities to business performance drivers, using frameworks such as NIST, PCI/DSS, ISO, GDPR, NYDFS, and others with our IT security service program.*	Tier 1	17

Reporting and Reimbursements

Program Narrative Reports – Quarterly Progress Reports

Quarterly Reports must be submitted via email to **shspadmin@oem.oregon.gov** no later than 15 days following the end of each quarter (Q1 = April, May, June; Q2 = July, August, September; Q3 = October, November December; Q4 = January, February, March)

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

RFR (Requests for Reimbursement)

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.

Requests for reimbursement may be submitted via email to shspadmin@oem.oregon.gov no later than 15 days following the end of each calendar quarter in which the expenses were made. Processing of RFRs may be delayed if quarterly program narrative and fiscal 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, 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

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 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 (OEM).

Any questions regarding this document and its guidance should be directed to:

Kevin Jeffries
Grants Coordinator
Oregon Department of Emergency Management
Mobile: 971-719-0740
Kevin.jeffries@oem.oregon.gov