CAL OES GOVERNOR'S OFFICE OF EMERGENCY SERVICES

STATE OF CALIFORNIA

Federal Fiscal Year (FFY) 2022-2023 State & Local Cybersecurity Grant Program (SLCGP) Application Workshop

Presented by

Cal OES State & Local Projects Unit and California Cybersecurity Integration Center (Cal-CSIC)

Agenda

- Introductions
- Program Overview
- Purpose of the Grant
- Eligibility Criteria
- Allowable and Unallowable Costs
- Proposal Requirements & Documentation
- SLCGP Notice of Interest (NOI) Walkthrough
- Cybersecurity Maturity Survey Walkthrough
- Proposal Scoring
- Useful Resources

Introductions: Cal OES/Cal-CSIC

The Cal OES State & Local Projects Unit is responsible for the overall grant management of the State & Local Cybersecurity Grant Program (SLCGP). Cal-CSIC provides policy and subject matter expertise for the SLCGP, including California's SLCGP Cybersecurity Plan.

State & Local Projects Unit Staff

Liz Azevedo

Kelsey Jones

Ben Rodriguez

Trevor Martin

Cal-CSIC Staff

Eric Nehls

Program Overview

The State & Local Cybersecurity Grant Program is a federal program established through the Infrastructure Investment and Jobs Act (IIJA). Funding from this program is available for state, local, and tribal governments via competitive funding opportunity (CFO). Applicants can submit a proposal for up to $250,000 in funding. Only one proposal per Applicant will be considered for funding.

Grant Subaward Performance Period is:
December 1, 2024 – December 31, 2026.

Cal OES rates and ranks the proposals competitively. The highest ranking proposals will receive funding until all of the funding is exhausted.

Purpose of the Grant

The purpose of the SLCGP is to assist state, local, and tribal governments address cybersecurity risks and threats to information systems, and improve security of critical infrastructure and resilience of the services these entities provide to their communities.

To achieve this purpose, the following objectives have been established for the SLCGP:

1. Governance & Planning
2. Assessment & Evaluation
3. Mitigation
4. Workforce Development

All projects funded through the SLCGP must align to one or more of these objectives. Additional information about the objectives, including related sub-objectives and sample outcomes, can be found in the federal Notices of Funding Opportunity (NOFO).

Programmatic Requirements

Alignment with Cybersecurity Plan - In addition to aligning with one or more of the SLCGP Objectives, projects funded under the program must align with one or more of the 16 Cybersecurity Plan Elements as described in the NOFO and addressed in the California SLCGP Cybersecurity Plan.

National Cybersecurity Review (NCSR) – All recipients and subrecipients of SLCGP funds must complete the NCSR in the first year of their performance period, and annually thereafter.

Cybersecurity & Infrastructure Security Agency (CISA) Cyber Hygiene Service – All recipients and subrecipients of SLCGP funds must participate in CISA's Cyber Hygiene Service's Vulnerability Scanning Service as a post-award requirement of the grant.

Eligibility Criteria: SLCGP for Local/Tribal Governments (SL)

Must meet the federal definition of Local Government in 6 U.S.C. §101(13), OR

Meet the federal definition of a Tribal Government in 6 U.S.C. §665(g)(a)(7), AND

Be located in the state of California.

Eligibility Criteria: SLCGP for State Agencies (SG)

Must be an agency of the state of California.

Allowable Costs Categories

1. Planning
2. Organization
3. Equipment
4. Training
5. Exercise
6. Management and Administration (M&A)
7. Indirect Costs

Allowable Cost: Planning

Funding may be used for a range of planning activities, such as those associated with the development, review, and revision of holistic, entity-wide cybersecurity plans and other planning activities that support the Program goals and objectives.

Allowable Costs: Organization

Funds may be used for cybersecurity program management, development of whole community partnerships that support cybersecurity program governance, structures and mechanisms for information sharing between the public and private sector, and operational support, including ensuring continuity of operations for essential functions.

Personnel
Personnel hiring, overtime, and backfill expenses are permitted under this Program to perform allowable SLCGP planning, organization, training, exercise, and equipment activities.

Personnel expenses may include, but are not limited to, training and exercise coordinators, program managers and planners, and cybersecurity navigators. The Subrecipient must demonstrate that the personnel will be sustainable.

Allowable Cost: Equipment

Unless otherwise stated, equipment must meet all applicable statutory, regulatory, and/or DHS-adopted standards to be eligible for purchase using SLCGP funds. Subrecipients will be responsible for obtaining and maintaining all necessary certifications and licenses for the requested equipment.

Investments in emergency communications systems and equipment must meet applicable SAFECOM Guidance recommendations; such investments must be coordinated with the Statewide Interoperability Coordinator and the State Interoperability Governing Body to ensure interoperability and long-term capability.

Applicants should reference the FY 2022 and FY 2023 SLCGP NOFO, Section D, 12 – Funding Restrictions and Allowable Costs, e. Other Direct Costs, III. Equipment, for additional requirements and restrictions on allowable equipment costs.

Allowable Costs: Training

Allowable training-related costs under SLCGP include the establishment, support, conduct, and attendance of training and/or in conjunction with training by other federal agencies. Training conducted using SLCGP funds should align with the California SLCGP Cybersecurity Plan and address a performance gap identified through cybersecurity assessments and contribute to building a capability that will be evaluated through a formal exercise.

All training courses must receive a Training Feedback Number from Cal OES Training & Exercise prior to the start of the course. To request a Training Feedback Number, please download and complete the Training Feedback Form and forward the completed request via email to training@caloes.ca.gov .

Allowable Cost: Exercise

Exercises conducted with SLCGP funding should be managed and conducted consistent with Homeland Security Exercise and Evaluation Program (HSEEP) guidance documents.

Subrecipients are required to submit an After Action Report/Improvement Plan (AAR/IP) to the SLCGP Grants Analyst and FEMA at hseep@fema.dhs.gov no later than 90 days after completion of any exercise(s) conducted using SLCGP funds.

Allowable Cost: M&A

Management and Administration (M&A):
Organizations may use up to 5% of their award for M&A purposes. This includes: paying staff or third-party contractors/consultants to assist with the management and administration of SLCGP funds. M&A costs must not be duplicative of costs included in the Indirect Costs on the project.

Examples of M&A: Costs associated with submitting Required Documents, Cash Reimbursement Requests, Grant Modifications, Progress Reports to Cal OES, organizing invoices and procurement documents, etc.

Examples of what is **not** M&A: costs associated with designing, developing, overseeing, or managing cybersecurity projects, responding to/recovering from cybersecurity incidents, training and exercise costs, etc.

Allowable Cost: Indirect Costs

Indirect costs may be included in the project costs. Applicants with an indirect cost rate approved by their cognizant federal agency may claim indirect costs based on the established rate. Indirect costs claimed must be calculated using the base approved in the indirect cost negotiation agreement.

Unallowable Costs

- Supplantation of state or local funds
- Any subrecipient cost-sharing contribution, when required
- To pay a ransom from cyberattacks
- Spyware
- Recreational or social purposes, or for any purpose that does not address cybersecurity risks or threats on information systems owned or operated by, or on behalf of, the Subrecipient entity
- Suing the federal government or any other government entity
- Lobbying or intervention in federal regulatory or adjudicatory proceedings
- Acquiring land or constructing, remodeling, or altering buildings or other physical facilities
- Cybersecurity insurance premiums
- Any expenses incurred on your projects **OUTSIDE OF THE GRANT PERFORMANCE PERIOD**

Proposal Required Documentation

1. State FY 2024 State & Local Cybersecurity Grant – Local & Tribal (SL) Program Notice of Interest (NOI),

   OR

   State FY 2024 State & Local Cybersecurity Grant – State Agency (SG) Program NOI

2. A PDF copy of the Applicant's responses to the Cal-CSIC online Cybersecurity Maturity Survey

SFY 2024 SLCGP
Notice of Interest (NOI)
Form Overview

SLCGP Notice of Interest (NOI) Form

- The SLCGP NOI Form is a PDF fillable form that Cal OES uses to score and rank each proposal.

- Should provide a detailed description of the proposed cybersecurity project and how it aligns with the SLCGP Objectives, Cybersecurity Plan Elements, and California's Cybersecurity Plan.

- Outlines the estimated costs needed to complete the proposed cybersecurity project.

- Establishes the proposed cybersecurity project timeline and milestones for completion.

Section I: Applicant Information

Local or Tribal Government Entity: as indicated on your Federal Employer Identification Number (FEIN) letter provided by the Federal Internal Revenue Service.

Physical Address of the Project Location: Indicate the address of the location of the project.

Mailing Address, If different: Use your administrative office address, if different from project location.

UEI/FEIN/Website: Enter the Unique Entity Identifier (UEI) associated with your organization on the federal System for Award Management (SAM) website, the FEIN of your organization, and the website/url for your organization, if applicable.

Authorized Agent/Tribal Chairperson Contact Information: Name, Title/Role, phone number, and email address.

Primary Point of Contact: Name, Title/Role, phone number, and email address.

Funding Request: Up to a maximum of **$250,000** can be requested.

Partial Funding: If the Applicant is willing to accept less than their maximum request amount, they should check the box at the bottom of this page and indicate in whole dollars the minimum amount they will accept.

(This section is not scored)

Section II: Alignment with Cybersecurity Plan & SLCGP Objectives

Describe the proposed project and how it will fill identified, critical cybersecurity capability gaps.

- Thoroughly describe the project(s) being proposed, outlining the various elements or stages involved to implement and complete the project(s), including how the project aligns with one or more of the SLCGP Objectives and implements any applicable cybersecurity best practices as outlined in the California SLCGP Cybersecurity Plan. (20 Points)

- Describe how the proposed project(s) align with one or more of the 16 cybersecurity plan elements and any of the associated statewide priorities addressed in the California SLCGP Cybersecurity Plan. Please refer to the cybersecurity plan and the FY 2022 and FY 2023 NOFOs (see Appendix C, Cybersecurity Plan, Required Elements, in the NOFOs) for additional information on the cybersecurity plan elements. (20 Points)

(This section is worth 40 points total)

Section III: Impact of Loss of Network Availability

- Describe your organization’s mission/objectives and how your network supports these. (20 points)
- Describe how your network’s loss of availability would impact security, economic security, public health or safety, or any combination of those matters. (20 points)

(This section is worth 40 points total)

Section IV: Cybersecurity Posture Maturity

Describe the Applicant's current cybersecurity governance, infrastructure, and capabilities and how SLCGP funding will help improve them.

- Describe to what degree the Applicant's current cybersecurity posture aligns with the 16 Elements of Cybersecurity as identified in the California SLCGP Cybersecurity Plan (p.6) and how SLCGP funding will enhance/improve the existing posture. (20 points)

- Describe the Applicant's current cybersecurity maturity as it relates to the NIST Cybersecurity Framework 2.0 and how SLCGP funding will help enhance/improve the current cybersecurity maturity level. The Applicant should ensure the proposed project is an appropriate match to their cybersecurity level as indicated on their survey responses and addresses critical gaps. (20 points)

(This section is worth 40 points total)

Section V: Cybersecurity Gaps

Describe how the proposed project will fill critical cybersecurity capability gap(s) identified by your organization. (20 points)

(This section is worth 20 points total)

Section VI: Proposed Budget

In this Section, write yes or no for each applicable cost category and provide a brief description and estimated cost for each fund source the Applicant plans to expend in each category.

- The maximum amount of FY22 SLCG funds available per proposal is $82,500.
- The maximum amount of FY23 SLCG funds available per proposal is $167,500.
- The Total Costs at the bottom of the Proposed Budget must match the Funding Requested in Section I.

NOTE: Due to the competitive funding process, changes to the scope of work are *<u>not</u>* permitted. Please ensure the projects proposed are well planned, as any funds remaining after the end of the performance period will be disencumbered.

(This section is worth 20 points total)

Section VII: Milestones

Provide description and associated key activities that lead to the milestone event. Applicants should provide no more than 10 milestones.

Start dates should reflect the start of the grant associated key activities and end dates should reflect when the **MILESTONE EVENT WILL BE COMPLETED.**

Milestone Considerations: time to complete bidding process, time to complete work, and the organization’s time involved with managing the projects. Example of Sufficient Milestones:

Milestone 1. Create Planning activities by March 2025
Milestone 2. Conduct Exercise activities by June 2025

(This section is worth 20 points total)

Section VIII: Population (SL Program ONLY)

Check the box in this section if the total population of the Applicant organization (e.g., county or city population for county or city governments, enrollment for school districts, service area population for special districts, tribal membership for tribal governments, etc.) is ***less than*** 50,000 individuals.

This question does not apply to State Agency Applicants.

(This section is not scored)

Additional Funding & Applicant Certification

Additional Funding
Describe how the Applicant would use additional funding, if such funds become available, to expand or enhance the proposed project.

(This section is not scored)

Application Certification
The Authorized Agent or Primary Point of Contact identified in Section I must indicate that:

1. they have completed the required Cybersecurity Maturity Survey and downloaded a PDF copy of their responses, and

2. they certify the information provided, including population information (if applicable), is complete and correct to the best of their knowledge.

(This section is not scored)

Cybersecurity Maturity Survey Overview

The Cybersecurity Maturity Survey can be accessed at:

- https://www.caloes.ca.gov/cyber-surveys

The survey consists of 18 questions derived from the NIST Cybersecurity Framework 2.0. This survey is *separate* from the NCSR which is also required.

The survey site will give you the option to manually save your work and/or your final answers to a pdf file at any time before you leave the site.

The survey will not automatically save your work if you get interrupted, so we recommend downloading the pdf initially, determining your answers offline, and returning when you are ready to complete the survey in one sitting. You can download at any time and the pdf will include your answers.

When you have finished the survey, please complete both these steps:

- Download the survey as a pdf (to be included with your application)
- Click the Submit button at the bottom of the survey

Your survey results are not scored, but we will use them to determine if your proposal is appropriate to your organizational cybersecurity maturity level.

Proposal Submission

A Proposal consists of:

- **SFY 2024 State & Local Cybersecurity Grant – Local & Tribal (SL) Program Notice of Interest (NOI)**, OR
  SFY 2024 State & Local Cybersecurity Grant – State Agency (SG) Program NOI, AND
- **A PDF Copy of the Applicant's Cybersecurity Maturity Survey Responses**

The Proposal must be received via email, no later than **11:59 pm (PDT)** on **Friday, September 27, 2024** to: **StateLocalProjects@CalOES.ca.gov**

Proposals submitted after this time/date or submitted to any other email address will not be considered.

Proposal Submission: File Naming

The following naming convention should be used for submitting proposals:

- **SFY 2024_SL/SG Program CFO_ApplicantName**
- **SFY 2024_SLCGP_Maturity Survey_ApplicantName**

Example: SFY 2024_SL Program CFO_Landing County

You are encouraged to shorten long organizational names. The full names will be in the text of the document. Use capital letters to separate the names, not spaces.

For example:
Bridgerton City Unified School District = BridgertonCityUSD
Capital City Municipal Utility District = CapCityMUD
Golden State Council of Governments = GoldStateCOG

Proposal Submission: Other Instructions

Proposal documents must be submitted as PDF attachments. Embedded links or links to cloud-based storage services (e.g., Google Drive, Dropbox, etc.) will **not** be accepted.

Password-protected documents will **not** be accepted.

It is very important to note that **Cal OES staff cannot assist in the creation of the documents or advise on any content of the proposed responses on the NOI**. Cal OES staff may only provide clarification on the questions presented in the NOI Form or Cybersecurity Maturity Survey.

Proposal Scoring

This is a Competitive Funding Opportunity, meaning that your proposal will be ranked in comparison to all other Proposals received.

Important Applicant Considerations:

- Completeness of the Proposal to include all required documents.
- Alignment of the proposed project to the SLCGP Objectives, the 16 Elements of Cybersecurity, and the California SLCGP Cybersecurity Plan.
- Impact to the Applicant organization of any loss of network availability.
- The Applicant’s current cybersecurity maturity level and the appropriateness of the proposed project to that level
- Identified cybersecurity gap(s) and how the proposed project will address such gap(s).

Proposal Scoring

Funding will be awarded to the highest-ranked proposals. Evaluation of the proposals is based on six scored criteria, totaling 180 possible points.

Section	Section Title	Points
I	Applicant Information	Not Scored
II	Alignment	40
III	Impact	40
IV	Maturity	40
V	Gap(s)	20
VI	Budget	20
VII	Milestones	20
VIII	Population (if applicable)	Not Scored
	Total	180
Additional Funding	Additional Funding	Not Scored

Recommendation for Award

Final funding decisions are made by the Director of Cal OES, based on the following factors:

- Ranked score of the Proposal
- Consideration of funding priorities, including the federal rural pass-through requirement
- Prior negative administrative and programmatic performance, if applicable

Once the decision has been made, the Applicant will be notified via email.

Those selected will receive an Intent to Fund Letter.

Those not selected will receive a Denial Letter and information on the appeals process.

Resources

DHS-FEMA FY 2022 SLCGP Notice of Funding Opportunity (NOFO):

Search Results Detail | Grants.gov

DHS-FEMA FY 2023 SLCGP NOFO:

Search Results Detail | Grants.gov

CISA FY 2023 SLCGP Frequently Asked Questions:

FY 2023 State and Local Cybersecurity Grant Program FAQs (cisa.gov)

California SLCGP Cybersecurity Plan:

California_Cybersecurity_Plan_FINAL_v1.5.5_20230921.pdf

FFY 2022-2023 SLCGP State Supplement to the NOFO:

2022-23 State and Local Cybersecurity Grant Program State Supplement

Questions

Please email all questions to:

StateLocalProjects@CalOES.ca.gov