

Federal Fiscal Year 2024 State & Local Cybersecurity Grant Program for
State Agency (SG) – Notice of Interest (NOI)

Section I. Applicant Information (Not Scored)

California State Agency (must be an [agency of the State of California](#))

Physical Address of State Agency:

Street

City

State

Zip Code

County

Mailing Address, if different:

Street

City

State

Zip Code

Unique Entity Identifier (UEI):

Federal Employer ID Number (FEIN):

Website/URL of the Organization:

Authorized Agent Contact Information:

Name

Title/Role

Telephone Number

Email

Primary Point of Contact Information:

Name

Title/Role

Telephone Number

Email

Funding Requested (Maximum of \$250,000)

Please check this box if the Applicant is willing to accept less than the full amount requested based on scoring, proposal selection, and availability of grant funding:

☐

If partial grant funding can be accepted, please identify in whole dollars the minimum amount of grant funding that will be accepted:

Section II. Alignment with California Cybersecurity Plan & SLCGP Objectives (40 Points Total)

Describe the proposed project(s) and how each project will fill identify critical cybersecurity capability gaps.

- a. 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](#). Please refer to the FFY 2024 SLCGP State Supplement and the FFY 2024 NOFO for more information and additional considerations. (2,200 characters max with spaces; 20 points)

- b. 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 FFY 2024 NOFO (see Appendix C, Cybersecurity Plan, Required Elements, in the NOFO) for additional information on the cybersecurity plan elements. (2,200 characters max with spaces; 20 points)

Section III. Impact(s) of Loss of Network Availability (40 Points Total)

- a. Describe your organization's mission/objectives and how your network supports these. (2,200 characters max with spaces; 20 points)

- b. Describe how your network's loss of availability would impact security, economic security, public health or safety, or any combination of those matters. (2,200 characters max with spaces; 20 points)

Section IV. Cybersecurity Posture Maturity Level (40 Points Total)

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

- a. 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 (beginning on p. 6) and how FFY 2024 SLCGP funding will enhance and/or improve the existing posture. (2,200 characters max with spaces; 20 points)

- b. Describe the Applicant's current cybersecurity maturity as it relates to the functions of the National Institute of Standards and Technology Cybersecurity Framework 2.0 and how SLCGP funding will enhance and/or improve the existing cybersecurity maturity level. The Applicant should ensure the proposed project(s) is/are an appropriate match to their cybersecurity maturity level as indicated by their survey responses and address critical gaps. (2,200 characters max with spaces; 20 points)

- c. In addition to the narrative questions in this section, Applicants must complete an online survey on their organization's [cybersecurity posture maturity](#). **Upon completion of the survey, Applicants must download a copy of their responses and attach as a PDF to submit with this NOI form; proposals submitted without completing the survey may not be considered for funding.**

Section V. Cybersecurity Gap(s) (20 Points)

- a. Describe how each proposed project will fill critical cybersecurity capability gap(s) identified by the Applicant. (2,200 characters max with spaces; 20 points)

Section VI. Project Worksheet (40 Points)

Applicants are to submit for evaluation the FFY 2024 SLCGP Project Worksheet to demonstrate their project alignment to SLCGP objectives, implementation plan, and identify key project milestones. Describe the project and milestones (activities) and provide the cost estimate related to cybersecurity enhancements of the organization.

The worksheet includes instruction tabs for each of the two tabs to be filled out. The Baseline Project Information tab is worth 20 points. The Project Implementation tab is also worth 20 points.

The maximum amount available for 2024 SLCG funds is \$250,000, with the 30% match of \$107,143, for a maximum Total Project Cost of \$357,142.

Please confirm below that the Project Worksheet has been completed and submitted with your NOI. Please also confirm you will meet the required match for the 2024 SLCG funding at 30% of the total project cost.

NOTE: Due to the competitive process, changes to the scope of work are not permitted. Please ensure the projects being proposed are well planned, as any funds that remain at the end of the period of performance will be disencumbered.

- ☐ Applicant has completed and submitted the FFY 2024 SLCGP Project Worksheet.
- ☐ Applicant acknowledges, and if funded, agrees to meet the total project match at 30% of requested funds.

Utilization of Additional Funds if Available (Not Scored)

If additional funds become available, how would you utilize the funds to expand or enhance your proposed project(s)? (2,200 characters max with spaces)

Applicant Certification Information

Before submitting, please review your responses and ensure that they are complete, including the required survey and Project Worksheet. Submit the completed NOI, along with other required documents, via email to StateLocalProjects@caloes.ca.gov

IMPORTANT NOTE: Submissions received after the deadline of Friday, March 13, 2026, 11:59 PM PST will not be accepted and will be disqualified from continuing in the competitive application process. No exceptions can be made. Please plan accordingly.

☐ Applicant has completed the online cybersecurity posture maturity survey and downloaded a PDF copy of their responses.

☐ I certify that the information provided is complete and correct to the best of my knowledge.

Name, Title/Role
E-mail Address
Phone Number