**2023 California State and Local Cybersecurity Grant Program**
**Capability Assessment Questionnaire**

The State of California is conducting this assessment as a requirement under the federal State and Local Cybersecurity Grant Program (SLCGP). The assessment is based on the SLGCP required 16 elements and sub-elements listed in the grant guidance. The results of this assessment will be used to develop the SLGCP required Cybersecurity Plan for the state. This survey is not an audit, a state-imposed standard or requirement, a test, or an all-inclusive evaluation of capability.  This information is being collected for the sole purpose of the SLCGP and while the aggregate data will be presented in the cybersecurity plan, the individual entity responses will not be sent out in any summary report or the plan.

The term "organization" used throughout this assessment is synonymous with jurisdiction. Each respondent should address and answer the questions from a jurisdictional perspective, i.e., city, county, etc., as best they can.  Where a narrative response is requested, please be as detailed and specific in your answers as possible. For each question in the assessment, please select the level that best represents where your think your organization is with regard to meeting/achieving the objective or criterion described in each question. The definitions below provide an explanation for each of the answers to help you use the answer scale in the answer column. The four levels are determined by the SLGCP guidance, and the level definitions are based on the NIST Cybersecurity Framework. These questions and descriptions may not fit your organization exactly, but should help you judge your organization's overall level of capability more accurately.

| Answer Scale | | | |
|---|---|---|---|
| **Foundational Level** | **Fundamental Level** | **Intermediary Level** | **Advanced Level** |
| Organizational cybersecurity practices are not formalized, and cyber risk is understood and managed in an ad hoc and sometimes reactive manner. Prioritization of cybersecurity activities are not directly informed by organizational objectives, the threat environment, or business/mission requirements. The organization does not understand its role in the larger ecosystem with respect to either its dependencies or dependents. | Organizational cybersecurity practices are approved by management but are not established as organizational-wide policy. Prioritization of cybersecurity activities and protection needs are directly informed by organizational objectives, the threat environment, or business/mission requirements. The organization understands its role in the larger ecosystem with respect to either its own dependencies or dependents, but not both. | The organization’s cybersecurity management practices are formally approved and expressed as policy. Organizational cybersecurity practices are regularly updated based on the application of management processes to changes in business/mission requirements and a changing threat and technology landscape. The organization understands its role, dependencies, and dependents in the larger ecosystem and may contribute to the community’s broader understanding of risks. | There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. The organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators. Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts to a changing threat and technology landscape and responds in a timely and effective manner to evolving, sophisticated threats. The organization understands its role, dependencies, and dependents in the larger ecosystem and contributes to the community’s broader understanding of risks. |

**2023 California State and Local Cybersecurity Grant Program**
**Capability Assessment Questionnaire**

| No. | SLGCP Assessment Element Question | Answer | In which of the following areas does your organization have a capability gap for this element? Check as many that apply. | For each POETE area where you listed a gap or need, explain generally what those gaps and needs are. |
|---|---|---|---|---|
| 1 | At what capability level is your organization able to manage, monitor, and track information systems, applications, and user accounts? | Choose an Item | ☐ Planning<br>☐ Organization<br>☐ Equipment<br>☐ Training<br>☐ Exercises | |
| 2 | At what capability level is your organization able to monitor, audit, and track network traffic and activity? | Choose an Item | ☐ Planning<br>☐ Organization<br>☐ Equipment<br>☐ Training<br>☐ Exercises | |
| 3 | At what capability level is your organization able to enhance the preparation, response, and resiliency of information systems, applications, and user accounts? | Choose an Item | ☐ Planning<br>☐ Organization<br>☐ Equipment<br>☐ Training<br>☐ Exercises | |
| 4 | At what capability level is your organization able to implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk? | Choose an Item | ☐ Planning<br>☐ Organization<br>☐ Equipment<br>☐ Training<br>☐ Exercises | |

| No. | SLGCP Assessment Element Question | Answer | In which of the following areas does your organization have a capability gap for this element? Check as many that apply. | For each POETE area where you listed a gap or need, explain generally what those gaps and needs are. |
|---|---|---|---|---|
| 5a | At what capability level is your organization able to implement multi-factor authentication? | Choose an Item | ☐ Planning<br>☐ Organization<br>☐ Equipment<br>☐ Training<br>☐ Exercises | |
| 5b | At what capability level is your organization able to Implement enhanced logging? | Choose an Item | ☐ Planning<br>☐ Organization<br>☐ Equipment<br>☐ Training<br>☐ Exercises | |
| 5c | At what capability level is your organization able to implement data encryption for data at rest and in transit? | Choose an Item | ☐ Planning<br>☐ Organization<br>☐ Equipment<br>☐ Training<br>☐ Exercises | |
| 5d | At what capability level is your organization able to end the use of unsupported/end of life software and hardware that are accessible from the Internet? | Choose an Item | ☐ Planning<br>☐ Organization<br>☐ Equipment<br>☐ Training<br>☐ Exercises | |

| No. | SLGCP Assessment Element Question | Answer | In which of the following areas does your organization have a capability gap for this element? Check as many that apply. | For each POETE area where you listed a gap or need, explain generally what those gaps and needs are. |
|---|---|---|---|---|
| 5e | At what capability level is your organization able to prohibit use of known/fixed/default passwords and credentials? | Choose an Item | □ Planning<br>□ Organization<br>□ Equipment<br>□ Training<br>□ Exercises | |
| 5f | At what capability level is your organization able to reconstitute systems (backups)? | Choose an Item | □ Planning<br>□ Organization<br>□ Equipment<br>□ Training<br>□ Exercises | |
| 5g | At what capability level is your organization at in migrating to the .gov internet domain? | Choose an Item | □ Planning<br>□ Organization<br>□ Equipment<br>□ Training<br>□ Exercises | |
| 6 | At what capability level is your organization able to promote the delivery of safe, recognizable, and trustworthy online services, including using the .gov internet domain? | Choose an Item | □ Planning<br>□ Organization<br>□ Equipment<br>□ Training<br>□ Exercises | |

| No. | SLGCP Assessment Element Question | Answer | In which of the following areas does your organization have a capability gap for this element? Check as many that apply. | For each POETE area where you listed a gap or need, explain generally what those gaps and needs are. |
|---|---|---|---|---|
| 7 | At what capability level is your organization able to ensure continuity of operations including by conducting exercises? | Choose an Item | ☐ Planning<br>☐ Organization<br>☐ Equipment<br>☐ Training<br>☐ Exercises | |
| 8 | At what capability level is your organization able to identify and mitigate any gaps in its cybersecurity workforces, enhance recruitment and retention efforts, and bolster the knowledge, skills, and abilities of personnel (reference to NICE Workforce Framework for Cybersecurity)? | Choose an Item | ☐ Planning<br>☐ Organization<br>☐ Equipment<br>☐ Training<br>☐ Exercises | |
| 9 | At what capability level is your organization able to ensure continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks? | Choose an Item | ☐ Planning<br>☐ Organization<br>☐ Equipment<br>☐ Training<br>☐ Exercises | |
| 10 | At what capability level is your organization able to assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of your organization? | Choose an Item | ☐ Planning<br>☐ Organization<br>☐ Equipment<br>☐ Training<br>☐ Exercises | |

| No. | SLGCP Assessment Element Question | Answer | In which of the following areas does your organization have a capability gap for this element? Check as many that apply. | For each POETE area where you listed a gap or need, explain generally what those gaps and needs are. |
|---|---|---|---|---|
| 11 | At what capability level is your organization able to share cyber threat indicators and related information with the State of California and the Department of Homeland Security? | Choose an Item | ☐ Planning<br>☐ Organization<br>☐ Equipment<br>☐ Training<br>☐ Exercises | |
| 12 | At what capability level is your organization able to leverage cybersecurity services offered by the Department of Homeland Security? | Choose an Item | ☐ Planning<br>☐ Organization<br>☐ Equipment<br>☐ Training<br>☐ Exercises | |
| 13 | At what capability level is your organization able to implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives? | Choose an Item | ☐ Planning<br>☐ Organization<br>☐ Equipment<br>☐ Training<br>☐ Exercises | |
| 14 | At what capability level is your organization able to develop and coordinate strategies to address cybersecurity risks and cybersecurity threats? | Choose an Item | ☐ Planning<br>☐ Organization<br>☐ Equipment<br>☐ Training<br>☐ Exercises | |

**2023 California State and Local Cybersecurity Grant Program**
**Capability Assessment Questionnaire**

| No. | SLGCP Assessment Element Question | Answer | In which of the following areas does your organization have a capability gap for this element? Check as many that apply. | For each POETE area where you listed a gap or need, explain generally what those gaps and needs are. |
|---|---|---|---|---|
| 15 | At what capability level is your organization able to ensure rural communities have adequate access to, and participation in plan activities? | Choose an Item | ☐ Planning<br>☐ Organization<br>☐ Equipment<br>☐ Training<br>☐ Exercises | |
| 16 | At what capability level is your organization able to distribute funds, items, services, capabilities, or activities to local governments and agencies (related to cybersecurity)? If at the city/town or special district level, answer this in terms of ability to access and use funds received externally (state, federal, etc.). | Choose an Item | ☐ Planning<br>☐ Organization<br>☐ Equipment<br>☐ Training<br>☐ Exercises | |