www.asantecloud.com
tim@asantecloud.com
208.559.3660

Asante Cloud
1412 Idaho St
Suite 201
Boise Idaho, 83702

GRANT OPPORTUNITY BRIEF

Department of Homeland Security
State and Local Cybersecurity Grant Program (SLCGCP)
NOFO DHS 22-137-000-01

What is the State and Local Cybersecurity Grant Program?

The goal of SLCGP is to assist state, local, and territorial (SLT) governments with managing and reducing systemic cyber risk. Through IIJA funds, the SLCGP enables DHS to make targeted cybersecurity investments in SLT government agencies. SLCGP's overarching objective is to strengthen SLT government information technology (IT) networks through uniform cybersecurity governance structures and coordinated cybersecurity plans, prioritizing, testing, assessing SLT vulnerabilities, and implementing security protections.

Available Funding for NOFO

$185 M for 56 States & Territories. Project Duration is 48 months. Grants will be awarded to single entities - Governor designated State Administrative Agencies only, where at least 80% of the federal funding to must serve local governments, including at least 25% for rural areas.

Objective 1
Uniform Cybersecurity Governance Structure & Develop, Implement, or Revise Plans and Exercise Cyber Incident Response Plans.
- A uniform cybersecurity governance structure with identified senior leaders.
- Annual table-top and full-scope exercises to test cybersecurity plans.
- Develop and test cybersecurity plans, including cyber incident response plans.
- Prioritize asset (e.g., devices, data, software) protections and recovery actions based on the asset's Uniform Governance Structures Cybersecurity Planning Committee Statewide Cybersecurity Plans, Assessments, SLT Needs & Priorities, Key Practices, Exercise Cyber Incident Response Plans Implement Security Protections
- Zero Trust Architecture, Testing of Cybersecurity Plans Training criticality and business value which systems must be protected and recovered first.

Objective 2
SLT agencies understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
- SLT agencies are able to analyze network traffic.
- SLT agencies are able to respond to identified events and incidents, document root cause, and share information with partners.

Objective 3
Implement security protections commensurate with risk (outcomes of Objectives 1 & 2)
• Multi-factor authentication (MFA), prioritizing privileged users, Internet-facing systems, and cloud accounts.
• End use of unsupported/end of life software and hardware that are accessible from the Internet Prohibit use of known/fixed/default passwords and credentials.
• Ensure the ability to reconstitute systems following an incident with minimal disruption to services.
• Migrate to .gov internet domain.

Objective 4
Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility
• Ongoing phishing training, awareness campaigns are conducted, and organization provides role-based cybersecurity awareness training to all employees.

Deadline Application Submission Deadline: 11/15/2022 at 5 p.m. ET on grants.gov.
Who Can Apply
States/Territories Only one application will be submitted by the eligible entities (STATES/Territories), multiple entities can apply with one application.

Key Considerations

• Match: must meet a 10% cost share requirement for the FY 2022 SLCGP. The recipient contribution can be cash (hard match) or third-party in-kind (soft match).
• The application will consist of up to four (4) Investments, one for each SLCGP objective. Investments for SLCGP Objectives 1, 2, and 3 must have at least one project. Investments for SLCGP Objective 4 are optional for the FY 2022 SLCGP.
• The grant-funded activities of every project must align with the SLCGP solution areas: Planning, Organization, Exercises, Training and/or Equipment (POETE).
• To be eligible for FY 2022 SLCGP funding, each State/Territory application entity must submit a Cybersecurity Plan including all required NOFO elements.
• Develop a Cybersecurity Planning Committee with SLT's to develop and coordinate project objectives.
• Applications for the SLCGP from State/Territory entities must complete an Investment Justification Form (IJ Template) and project worksheets for each SLCGP objective.
• All applicants must obtain a Unique Entity Identifier (UEI) through GSA.
• $6 million in funding will be directly available to Tribal entities under the forthcoming Tribal Cybersecurity Grant Program, which DHS expects to publish the NOFO in the fall of 2022. However, Indian tribes can also receive services as a local government in the SLCGP.

Allowable Use of Funds

Specific investments made in support of the funding priorities discussed in the NOFO generally fall into one of the following allowable expense categories:

- Planning
- Equipment
- Exercises
- Management & Administration (M&A)
- Organization
- Training State/Territory FY 2022 SLCGP

CONTACT TIM

Tim Fitzpatrick
VP Business Development

tim@asantecloud.com
208.559.3660