DMVA PROGRAM 03 – STATE AND LOCAL CYBER SECURITY GRANTS PROGRAM (CSGP)

I. PROGRAM OBJECTIVES

The State and Local Cybersecurity Grant Program provides funding to eligible entities to address cybersecurity risks and threats to information systems owned or operated by, or on behalf of, state, local, or tribal governments. The SLCGP Assistance Listing Number is 97.137. More information and resources regarding SLCGP are available on CISA's website.

II. PROGRAM PROCEDURES

Funds are awarded to the Department of Military and Veterans' Affairs, Division of Homeland Security and Emergency Management (DHS&EM) upon approval of the SLCGP application by the Department of Homeland Security (DHS), Grant Programs Directorate (GPD). Federal funds are matched on a 70% / 30% cost sharing basis. Both State and local entities provide the match base on the awarded amount. Program compliance is based on federal fiscal year guidance.

III. COMPLIANCE REQUIREMENTS

All costs charged to federal awards (including both federal funding and any non-federal matching or cost sharing funds) must comply with applicable statutes, rules and regulations, and policies, and the terms and conditions of the federal award. They must also comply with the Uniform Administrative Requirements, Cost Principles, and Audit Requirements at 2 C.F.R. Part 200 unless otherwise indicated in the NOFO or the terms and conditions of the federal award. This includes, among other requirements, that costs must be incurred, and products and services must be delivered within the budget period. 2 C.F.R. § 200.403(h). The following identifies a list of activities for which a recipient may not use federal funds and any cost sharing or matching funds under federal awards:

• Matching or cost sharing requirements for other federal grants and cooperative agreements (see 2 C.F.R. § 200.306).

• Lobbying or other prohibited activities under 18 U.S.C. § 1913 or 2 C.F.R. § 200.450.

• Prosecuting claims against the federal government or any other government entity (see 2 C.F.R. § 200.435) See subsections below for information on any other funding restrictions.

Unallowable Costs

For FY 2024 SLCGP, grant funds may not be used for the following:

a. Spyware.
b. Construction.
c. Renovation.
d. To pay a ransom.
e. For recreational or social purposes.
f. To pay for cybersecurity insurance premiums.
g. To acquire land or to construct, remodel, or perform alterations of buildings or other physical facilities (This prohibition does not include minor building

modifications necessary to install and connect grant-purchased equipment that do not substantially affect a building's structure, layout, systems, or critical aspects of a building's safety, or otherwise materially increase the value or useful life of a building.);

h. For any purpose that does not address cybersecurity risks or cybersecurity threats on information systems owned or operated by, or on behalf of, the eligible entity that receives the grant or a local government within the jurisdiction of the eligible entity.
i. To supplant state or local funds; however, this shall not be construed to prohibit the use of funds from a grant for otherwise permissible uses on the basis that the SLT has previously used SLT funds to support the same or similar uses.
j. For any recipient or subrecipient cost-sharing contribution.

Submission of a Cybersecurity Plan is required for any eligible entity participating in the SLCGP. The Cybersecurity Plan is a key component of a strategic approach to building cyber resilience. The approved Cybersecurity Planning Committee, with a holistic membership representing the various stakeholder groups across the entity, is responsible for developing, approving, revising, and implementing the approved Cybersecurity Plan.

To support the FY 2024 SLCGP requirements, Cybersecurity Plans must include the following activities:
a. Conducting assessment and evaluations as the basis for individual projects throughout the life of the program; and
b. Prioritizing key cybersecurity best practices and consulting Cybersecurity Performance Goals (CPGs).

i. The CPGs are a prioritized subset of information technology and operational technology cybersecurity practices aimed at meaningfully reducing risks to both critical infrastructure operations and the American people.
ii. These goals are applicable across all critical infrastructure sectors and are informed by the most common and impactful threats and adversary tactics, techniques, and procedures observed by CISA and its government and industry partners, making them a common set of protections that all critical infrastructure entities—from large to small—should implement.
iii. The CPGs do not reflect an all-encompassing cybersecurity program. Rather, they are a minimum set of practices that organizations should implement toward ensuring a strong cybersecurity posture.
iv. The Cross-Sector CPGs are regularly updated, with a targeted revision cycle of at least every 6 to 12 months.

IV. SUGGESTED AUDIT PROCEDURES

Review State and local SLCGP agreements to determine if there are special requirements and/or products to be developed; and test expenditure records to determine if expenditures are eligible.

DMVA PROGRAM 03 – STATE AND LOCAL CYBER SECURITY GRANTS PROGRAM (CSGP)

A. ELIGIBILITY -

The auditor is not expected to verify eligibility other than that required by section III (A) above.

B. MATCHING, LEVEL OF EFFORT AND/OR EARMARKING REQUIREMENTS -

Compliance Requirement: The federal funds must be matched by State and local funds. Funds from other federal programs cannot be used to provide the local match.

Suggested Audit Procedure: Review local fund documents to ensure that no federal funds were used to provide the required local match.

C. REPORTING REQUIREMENTS -

Compliance Requirement: The local jurisdiction must provide DHS&EM a quarterly financial billing and narrative report of SLCPG activities.

Suggested Audit Procedure: Review reports for timeliness.

D. SPECIAL TESTS AND PROVISIONS -

Compliance Requirements: The local jurisdiction must be able to show NIMS adoption and implementation through completion of the Alaska Assessment.

Suggested Audit Procedures:

a) Review State of Alaska state preparedness report.
b) Review jurisdictional Alaska assessment report.
c) Review federal financial report.
d) Review biannual strategy implementation report (BSIR).
e) Review the current year Notice of Funding Opportunities (NOFO) publication and State and local SLCPG agreements to determine if there are special requirements and/or products to be developed; and test expenditure records to determine if expenditures are eligible.

For more information: State and Local Cybersecurity Grant Program | FEMA.gov