Fiscal Year 2024 State and Local Cybersecurity Grant Program Fact Sheet

Release Date: Sep 23, 2024

Download a PDF copy of this webpage

Overview

The goal of the State and Local Cybersecurity Grant Program (SLCGP) is to help states and territories, specifically rural and local communities, address cybersecurity risks and cybersecurity threats. The SLCGP enables DHS to make targeted cybersecurity investments in SLT government agencies, thus improving the security of critical infrastructure and resilience of the services SLT governments provide to their communities.

Goals and Objectives

The Federal Emergency Management Agency (FEMA) and the Cybersecurity and Infrastructure Security Agency (CISA) created a series of overarching goals and objectives for the SLCGP based on input from SLT stakeholders and associations, and consideration of national priorities, frameworks, and the national cyber threat environment.

- Develop and implement cyber governance and planning.
- Assess and evaluate systems and capabilities.
- Implement security protections commensurate with risk.
- Build a cybersecurity workforce.

Funding

In FY 2024, $279.9 million is available under the SLCGP. Each state and territory will receive a funding allocation as determined by the statutory formula. Allocations for states and territories include a base level as defined for each entity:

1% for each state, the District of Columbia, and the Commonwealth of Puerto Rico; and 0.25% for American Samoa, the Commonwealth of the Northern Mariana Islands, Guam, and the U.S. Virgin Islands. State allocations include additional funds based on a combination of state and rural population totals. 80% of total state or territory allocations must support local entities, while 25% of the total state or territory allocations must support rural entities.

Eligibility

All 56 states and territories, including any state of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the U.S. Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands, are eligible to apply for SLCGP funds. The Governor-designated SLCGP State Administrative Agency (SAA) is the only entity eligible to submit SLCGP applications to DHS/FEMA.

Funding Guidelines

Pass-Through Requirements

The SLCGP SAA recipient must pass through at least 80% of the federal funds provided under the grant to local governments, and 25% of the federal funds must be provided to local jurisdictions within rural areas of the state or territory. The pass-through to rural entities is part of the overall 80% pass-through requirement to local governments. All pass-through entities must meet all program and grant administration requirements, as detailed in 2 C.F.R. § 200.332. For a description of eligible subrecipients, please see Section C.3.b. of the FY 2024 SLCGP Notice of Funding Opportunity (NOFO).

FEMA interprets the date that an entity “receives a grant” to be the date upon which FEMA releases the funding hold in the FEMA Grants Outcomes (FEMA GO) system. Therefore, the 45-day pass-through requirement starts on the date when the amendment is issued in FEMA GO and FEMA makes the funding available to the SAA for drawdown. After the funds have been released, FY 2024 SLCGP recipients must submit a letter to FEMA signed by the Authorized Official listed on the grant award certifying that they have met the 45-day pass-through requirement and collected any signed local government consents. Local consents

must be signed by the Authorized Official, or designee, for the local government entity receiving the items, services, capabilities, or activities in lieu of funding, and the consent must specify the amount and intended use of the funds. This letter is due no later than 10 calendar days after the 45-day period for issuing pass-through funding has passed. The letter should be emailed to FEMA-SLCGP@fema.dhs.gov. FEMA will send a copy of the letter to CISA.

Pass-through is defined as an obligation on the part of the entity or multi-entity group to make funds available to local units of government, combinations of local units, Tribal Nations, or other specific groups or organizations. With the consent of the local government, this pass-through may be in the form of in-kind services, capabilities, or activities, or a combination of funding and other services. Four requirements must be met to pass-through grant funds:

- The SLCGP SAA must make a firm written commitment to passing through grant funds or equivalent services to local government subrecipients;
- The SLCGP SAA's commitment must be unconditional (i.e., no contingencies for the availability of eligible entity funds);
- There must be documentation (i.e., subgrant award document with terms and conditions) of the commitment; and
- The award terms must be communicated to the local subrecipient.

Environmental Planning and Historic Preservation (EHP) Compliance

As a federal agency, FEMA is required to consider the effects of its actions on the environment and historic properties to ensure that all activities and programs funded by FEMA, including grant-funded projects, comply with federal Environmental Planning and Historic Preservation (EHP) laws, Executive Orders, regulations, and policies, as applicable.

Recipients and subrecipients proposing projects that have the potential to impact the environment, including, but not limited to, the construction of communication towers, modification or renovation of existing buildings, structures, and facilities, or new construction including replacement of facilities, must participate in the FEMA EHP review process. The EHP review process involves the submission of a detailed project description along with any supporting documentation requested by FEMA in order to determine whether the proposed project has the potential to impact environmental resources, including, but not limited to, threatened or

endangered species and historic properties, and identifying mitigation measures or alternative courses of action that may lessen any impact to those resources.

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

- 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).

For a full list of unallowable costs, please refer to Section D.13 of the FY 2024 SLCGP NOFO.

Multi-Entity Projects

Multiple eligible entities (states or territories) can group together to address cybersecurity risks and threats to information systems within the eligible entities' jurisdictions. There is no separate funding for multi-entity projects. Instead, these investments would be considered as group projects: each group member contributes an agreed-upon funding amount from their SLCGP award to the overall project. Each group member's financial contribution is then funded from their individual SLCGP award. Each participating state or territory in the group should include the multi-entity project in their individual Investment Justification (IJ) submissions with their application. It is expected that IJs for multi-entity projects will be almost identical. Any differences should be as a result of alignment with each group member's respective Cybersecurity Plan.

Cost-Share Requirements

Eligible entities must meet a 30% cost share requirement for the FY 2024 SLCGP, except for multi-entity projects which require a 20% cost share. The recipient contribution can be cash (hard match) or third-party in-kind (soft match). Eligible applicants must agree to make available non-federal funds to carry out an SLCGP award in an amount not less than 30% of the total project costs (federal award amount plus cost share amount). For FY 2024, in accordance with 48 U.S.C.

§1469a, cost share requirements are waived for the following: American Samoa, Guam, the U.S. Virgin Islands, and the Commonwealth of the Northern Mariana Islands.

Unless otherwise authorized by law, federal funds cannot be matched with other federal funds. The recipient's contribution should be specifically identified. These non-federal contributions have the same eligibility requirements as the federal share.

The DHS Secretary may waive or modify the non-federal share for an individual entity if the entity demonstrates economic hardship. For more information on what constitutes economic hardship and how to request a cost share waiver, please refer to Section C.5.f. of the NOFO.

Planning Committee and Cybersecurity Plan

Cybersecurity Planning Committees are charged with coordinating, developing, and approving the entity's Cybersecurity Plan. Eligible entities were required to submit Cybersecurity Plans for review and approval as part of their FY 2022 grant application. Additionally, plans are treated as living documents that can be resubmitted and updated as appropriate. CISA regional staff support is available, as needed.

All entities with a CISA-approved Cybersecurity Plan must submit their current plan to CISA via the FEMA SLCGP inbox (FEMA-SLCGP@fema.dhs.gov) no later than **Jan. 30, 2025**, and annually thereafter on the same date throughout the grant's period of performance. When they submit, entities must indicate if the plan has been revised since CISA's approval. If it has been revised, they must provide a brief explanation of any revisions.

There is no requirement for an entity to revise their CISA-approved Cybersecurity Plan unless CISA notifies them that it does not meet plan requirements.

Best Practices and Performance Measures

Entities must clearly articulate efforts to implement the Key Cybersecurity Best Practices for Individual Projects as listed in the FY 2024 NOFO. These efforts should be documented in their Cybersecurity Plan and should be prioritized in the individual projects the entity pursues. The assessment and evaluation activities

described in Objective 2 of the program can be used to measure the successes and failures of adopted Key Cybersecurity Best Practices as outlined in the Cybersecurity Plan.

Performance measures are data used to gauge program performance. The FY 2024 NOFO contains a list of performance measures, some of which overlap with the best practices, that applicants are encouraged to consider when evaluating their program performance. Referencing these measures will help applicants ensure their projects are meeting CISA standards for improving cybersecurity posture.

Application Process

Applying for an award under the SLCGP is a multi-step process. Applicants are encouraged to register early in the System for Award Management (SAM.gov) and the FEMA GO system, as the registration process can take four weeks or more to complete. Registration should be done in sufficient time to ensure it does not impact your ability to meet the required submission deadline. Please refer to Section D in the FY 2024 SLCGP funding notice for detailed information and instructions.

All application materials will be posted on Grants.gov. Eligible applicants must submit their application through the FEMA GO system. Applicants needing technical support with FEMA GO should contact FEMAGO@fema.dhs.gov or call the FEMA GO Help Desk at 1-877-585-3242, Monday – Friday from 9 a.m. – 6 p.m. ET.

Completed applications must be submitted in the FEMA GO system no later than 5 p.m. ET on December 3, 2024.

SLCGP Resources

There are a variety of resources available to address programmatic, technical, and financial questions, which can assist with SLCGP applications:

- The FY 2024 SLCGP funding notice is located online at Grants.gov.

- For additional program-specific information, please email FEMA-SLCGP@fema.dhs.gov. You may also contact your preparedness officer.
- For support regarding financial grants management and budgetary technical assistance, applicants may contact the FEMA Award Administration Help Desk, via e-mail at ASK-GMD@fema.dhs.gov.
- For support regarding programmatic elements, applicants may contact CISA via e-mail at SLCGPinfo@cisa.dhs.gov. SLTs can reach out to their CISA Regional Staff. For regional contact information, please visit cisa.gov/about/regions.