Fiscal Year 2023 State and Local Cybersecurity Grant Program Key Changes

Release Date: 8? 7, 2023

Download a PDF copy of this webpage.

The State and Local Cybersecurity Grant Program (SLCGP) provides funding to eligible state, local, and territorial (SLT) governments to manage and reduce systemic cyber risk, thus improving the security of critical infrastructure and improving the resilience of the services SLT governments provide their community. This document outlines key changes in the program for fiscal year 2023.

FY 2023 Goals and Objectives

During FY 2022, applicants focused on Program Objective 1: Develop and establish appropriate governance structures, including developing, implementing, or revising Cybersecurity Plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.

In FY 2023, applicants are required to focus on implementing their Cybersecurity Plans by addressing the following program objectives:

- Objective 2: Understanding their current cybersecurity posture and areas for improvement based on continuous testing, evaluation and structured assessments.
- Objective 3: Implementing security protections commensurate with risk.
- Objective 4: Ensuring organization personnel are appropriately trained in cybersecurity, commensurate with their responsibilities.

Applicants should refer to Appendix A of the FY 2023 Notice of Funding Opportunity for more guidance on SLCGP goals, objectives, sub-objectives, and desired outcomes.

Eligible Rural Area Justification

The FY2023 SLCGP funding notice includes a definition of a rural area. Per 49 U.S.C. 5302, “rural” is any area with a population of less than 50,000 individuals. To meet the 25% rural pass-through requirement, the eligible subrecipient must be a local government entity within a rural area (a jurisdiction with a population of less than 50,000 individuals).

Timing of the Local Pass-Through Requirement and Local Consent

The below clarification is applicable for both FY 2022 and FY 2023 SLCGP awards.

FEMA interprets the date that an entity “receives a grant” to be the date FEMA releases any funding hold(s) in the ND Grants system and FEMA makes the funding available for drawdown by the State Administrative Agency (SAA). Therefore, the 45-day pass through requirement starts on the date when the amendment is issued in ND Grants releasing the funding hold, and FEMA makes the funding available to the SAA for drawdown. This pass-through requirement does not apply to funds the SAA receives for the development of the cybersecurity plan.

After project funds have been released, 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 consent must be signed by the Authorized Official (or his/her 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. The SAA's certification 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 Cybersecurity and Infrastructure Security Agency.