FY 2023 State and Local Cybersecurity Grant Program Key Changes

OVERVIEW

The State and Local Cybersecurity Grant Program (SLCGP) focuses on strengthening cybersecurity practices and resilience of state, local, tribal, and territorial (SLTT) governments. The SLCGP enables the Department of Homeland Security (DHS) to make targeted cybersecurity investments in support of SLTT government agencies' cybersecurity. This document outlines key changes for the Fiscal Year (FY) 2023 SLCGP.

PROGRAM GOALS AND OBJECTIVES

Program objectives remain the same throughout the four-year program, but the focus on SLCGP objectives shifts as the program progresses. In the FY 2022 SLCGP, states and territories focused on **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, SLCGP applications will focus on the next program objectives:

- **Objective 2**: Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
- **Objective 3**: Implement security protections commensurate with risk.
- **Objective 4**: Ensure organization personnel are appropriately trained in cybersecurity commensurate with responsibility.

Investment Justifications will require a project for Objective 4 in FY 2023. There are four (4) required projects in FY 2023 compared to three (3) in FY 2022. States and territories with a CISA-approved Cybersecurity Plan, Committee List, and Charter must include **at least one (1) Investment Justification for Objective 3 and Objective 4**.

Investment Justification and Project Worksheet Template

The Investment Justification (IJ) and Project Worksheet (PW) templates were revised to be shortened. These templates can be found on the FY 2023 SLCGP page on grants.gov.

In addition, applicants must submit only one (1) PW with their application.

PROGRAM PRIORITIES

As the program evolves each year, establishing a Cybersecurity Planning Committee and developing a state-wide Cybersecurity Plan were removed as priorities for FY 2023 as states and territories should have completed these tasks. For FY 2023, there are no new Cybersecurity Planning Committee and Cybersecurity Plans requirements. States and territories have the option to resubmit and update their Cybersecurity Plan. Applicants are required to consult with CISA regional staff for Cybersecurity Plan resubmissions and updates.

The two (2) priority activities that the FY 2023 SLCGP funds are required to be used for are to:

- Conduct assessment and evaluations as the basis for individual projects throughout the life of the program: and
- Adopt key cybersecurity best practices and consult Cybersecurity Performance Goals.

Cybersecurity Performance Goals (CPGs)

The FY 2023 SLCGP requires applicants to adopt key cybersecurity best practices and consulting the CISA CPGs. 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. The CPGs help establish a common set of fundamental cybersecurity practices for critical infrastructure that recipients should aim to implement to ensure a strong cybersecurity posture. Grant recipients will operationalize CPGs in accordance with their approved Cybersecurity Plan.

Cybersecurity Planning Committee Membership: Critical Infrastructure and Election Security

As part of the Cybersecurity Planning Committee Composition and Scope Requirements, DHS strongly encourages membership from critical infrastructure sectors and subsectors including K-12 education, water/wastewater, healthcare, energy, defense, and elections infrastructure. CISA also encourages applicants to consider tailoring their Cybersecurity Plans and aligning projects to protect those critical infrastructure sectors and sub-sectors.

Post-Grant Requirement: CISA Cyber Hygiene Services

For FY 2023, recipients are no longer required to participate in the CISA Cyber Hygiene Web Application Scanning service. Recipients are still required to participate in the CISA Cyber Hygiene Vulnerability Scanning service.

ELIGIBILITY RESTRICTION FOR FUNDING

56 states and territories are eligible to apply for the FY 2023 SLCGP. However, to be eligible to receive FY 2023 SLCGP funding, states and territories must have accomplished the FY 2022 SLCGP requirements of submitting an approved Cybersecurity Plan and establishing a Cybersecurity Planning Committee and requisite Charter.

The FY 2022 requirements must be met prior to the development of applications for FY 2023. Eligible recipients unable to meet the FY 2022 applications may still apply for the FY 2023 SLCGP but will adhere to different criteria focused on completing FY 2022 requirements of a CISA-approved Cybersecurity Plan, Cybersecurity Planning Committee List, and Charter.

FY 2023 SLCGP AVAILABLE FUNDING

The total funding allocated for the SLCGP increased from $185 million in FY 2022 to $400 million in FY 2023. Allocation percentages to states and territories remain the same, including the population-based ratio for rural areas.

Cost Share Requirement

The minimum percentage for the cost share requirement increased from 10% in FY 2022 to 20% in FY 2023. Eligible Applicants must ensure non-federal funds available to carry out an SLCGP awards in an amount no less than 20%. However, DHS will still consider requests for cost-share waiver due to hardship.

For a multi-entity group project, the cost share is changed to 10% for the FY 2023 SLCGP.

Timing of the Local Pass-Through Requirement and Local Consent

FEMA interprets the date that an entity “receives a grant” to be the date upon which FEMA releases any funding hold(s) in the Non-Disaster (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, FY 2022 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 CISA.