Fiscal Year 2024 State and Local Cybersecurity Grant Program Key Changes

Release Date: Sep 23, 2024

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 communities. This document outlines key changes in the program for Fiscal Year (FY) 2024.

FY 2024 Goals and Objectives

For FY 2024, applicants are required to submit applications that address at least one of the four program objectives outlined in the Notice of Funding Opportunity (NOFO). For those states that did not apply for FY 2022 or FY 2023 SLCGP funding, or for SLCGP recipients that were unable to meet the requirements previously, please refer to Appendix A, “Program Goals and Objectives” and Appendix B, “Cybersecurity Planning Committee and Charter” of the FY 2024 SLCGP NOFO for more information on the FY 2022 requirements that must be met before development of applications for FY 2024.

FEMA Grants Outcomes (FEMA GO) System

Applicants must apply to SLCGP on the new FEMA GO system. The previous Non-Disaster Grants (ND Grants) platform will become a legacy system for grant programs from FY 2023 and earlier. For more information about FEMA GO, please review Section D of the SLGCP NOFO and FEMA Grants Outcomes (FEMA GO) | FEMA.gov for additional guidance and tools.

Unrecovered Indirect Costs as Cost Share

In May 2024, FEMA released an Information Bulletin (IB) providing clarifying information regarding the use of unrecovered indirect costs as cost share in both the FY 2022 and FY 2023 SLCGP NOFO. This clarification is applicable for FY 2022–FY 2024 awards.

For FY 2024, with prior approval by FEMA, recipients may use unrecovered indirect costs for the cost share of SLCGP awards. All requests to use unrecovered indirect costs for cost share must be submitted to your FEMA SLCGP Preparedness Officer for consideration and approval. Recipients will be notified in writing if approval is granted.

Cybersecurity Plans Resubmission

One of the priority outcomes of the SLCGP is the approval of Cybersecurity Plans for each applicant. Applicants are still required to have a Cybersecurity and Infrastructure and Security Agency (CISA)-approved Cybersecurity Plan. Cybersecurity Plans are approved for two years and annually thereafter. In FY 2024, there are no additional plan requirements, but 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 January 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.

Additionally, the FY 2024 NOFO includes an additional column in the Project Worksheet. This column, “Project Milestones,” is more aligned to the Investment Justification template and designed designed for applicants to demonstrate the project activities they will complete within the period of performance.

Project Worksheet and Investment Justification Submission

Both the Project Worksheet (PW) and Investment Justification (IJ) Forms have been updated for FY 2024 SLCGP. The Project Implementation Section (p. 4) of the IJ has been removed. The Project Implementation section on the PW has been expanded to capture the related project milestones. Completed IJs and the associated PW are still required at time of application.

Best Practices and Performance Measures

The FY 2024 Key Cybersecurity Best Practices for individual projects are consistent with FY 2023. CISA did clarify, however, that they are not required for implementation within the period of performance. Existing language was updated to the following:

- "Cybersecurity Plans must clearly articulate efforts to implement these cybersecurity best practices across the eligible entity within reasonable timelines as funding permits. Cybersecurity Planning Committees should prioritize these best practices in individual projects that assist SLT entities."

CISA remains invested in collecting data to gauge program performance. In FY 2024, additional performance measures were included to the existing list to inform applicants of the information CISA will collect through the program duration. New performance measures include the following items:

- Addressing CISA-identified cybersecurity vulnerabilities.
- Funding Endpoint Detection Response System implementation.
- Improving capabilities' ratings.
- Funding improvements for Continuity of Operations Plans.
- Meeting State Administrative Agency (SAA) performance metrics.
- Increasing the use of CISA Services.
- Enhancing Data Encryption.
- Adopting Enhanced Logging.
- Adopting Systems Reconstitution.
- Increasing Multi-State Information Sharing and Analysis Center (MS-ISAC) Membership.

Some of the new performance measures listed above have previously been included in the NOFO as best practices. CISA views the implementation of those

best practices as informative in determining the SLCGP's success.

Cost Share and Economic Hardship Factors Revisions

In the Infrastructure Investment and Jobs Act (IIJA), the statute at 6 U.S.C. § 665g(m)(l) requires SLCGP recipients to provide a non-federal cost share. For FY 2024, the minimum percentage for the cost share requirement increases from 20% to 30%. For multi-entity group projects, the cost share is 20% in FY 2024. The statute at 6 U.S.C. § 665g(m)(2) also authorizes the Department of Homeland Security (DHS) Secretary (the Secretary) to waive or modify the non-federal cost share requirements if an eligible entity or multi-entity group demonstrates economic hardship, based on guidelines published by the Secretary on what constitutes economic hardship. In addition to the factors outlined in the FY 2022 and FY 2023 SLCGP NOFOs, the Secretary recently approved the following updates to the non-statutory factors for FY 2024 SLCGP:

- For discretionary criteria, remove Factor 1.
- Retain Factors 2 and 3.

The applicant is required to submit documentation supporting their request for an Economic Hardship Waiver at the award level at the time of application by attaching the supporting document to the grant application. Once a decision on a waiver request is made, the SLCGP SAA will be notified in writing. If approved, the award package will indicate that the cost share has been waived in full or in part and might indicate a requirement for the state to submit a revised budget or scope (as applicable) for the identified project(s). If the waiver request is approved after the award has been issued, FEMA will amend the award package to indicate that the cost share has been waived in full or in part and whether the recipient must submit a revised budget or scope for the identified project(s) (as applicable).

Required and Recommended Services

The required services for SLCGP have not changed from FY 2023 to FY 2024, but additional language and tables have been added to the NOFO to identify the services required based on sub-applicant status in an easily digestible, visual format. The FY 2024 NOFO clarifies existing guidance that the only local

governments required to participate in cyber hygiene vulnerability scanning services and Nationwide Cybersecurity Review (NCSR) are those receiving subawards. Local governments receiving non-funding assistance are not required to participate.

Known Vulnerabilities Catalog

The CISA known exploited vulnerabilities (KEV) catalog is listed as a new recommended resource in the FY 2024 NOFO. The purpose of this recommendation is to encourage governments to regularly view information related to cybersecurity vulnerabilities confirmed by CISA, prioritizing those exploited in the wild. A link to the KEV catalog is included in the NOFO to encourage SLT governments to use it as part of their vulnerability management plan.