# Fiscal Year 2025 State and Local Cybersecurity Grant Program Key Changes

**Release Date: Sep 3, 2025**

The State and Local Cybersecurity Grant Program (SLCGP) provides funding to eligible state, local and territorial governments to manage and reduce systemic cyber risk, thus improving the security of critical infrastructure and improving the resilience of the services they provide to their communities. This document outlines key changes in the program for Fiscal Year (FY) 2025.

## FY 2025 Goals and Objectives

Program objectives have remained the same throughout the four-year program. For FY 2025, a detailed overview of the program goals and objectives will not be included in the Notice of Funding Opportunity (NOFO) as an appendix. Instead, program goals and objective details are available on CISA.gov.

## Program Funding, Pass-Through Requirement and Cost Share Requirement

The total funding allocated for the FY 2025 SLCGP is $91.75 million. The minimum percentage for the cost share requirement increased to 40% in FY 2025. Eligible applicants must ensure there are non-federal funds available to carry out an SLCGP award in an amount no less than 40%. For a multi-entity group project, the cost share is 30% for the FY 2025 SLCGP. Exceptions to the Pass-Through Requirement remain the same as previous fiscal years: grant funding awarded solely to support projects integral to the revision of the state or territory Cybersecurity Plan; and, the District of Columbia, the Commonwealth of Puerto Rico, American Samoa, the Commonwealth of the Northern Mariana Islands, Guam, and the United States Virgin Islands.

Cost share waivers will not be considered for any entities in FY 2025 SLCGP. For FY 2025, in accordance with 48 U.S.C. § 1469a, cost share requirements are waived only for the insular areas of the U.S. territories of American Samoa, Guam, the U.S. Virgin Islands and the Commonwealth of the Northern Mariana Islands.

## 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 Security Agency (CISA)-approved Cybersecurity Plan. Cybersecurity Plans are approved for two years and annually thereafter. In FY 2025, 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 **Jan. 30, 2026**.

All SLCGP recipients with a CISA-approved Cybersecurity Plan are required to do one of the following:

- Email your FEMA Preparedness Officer at FEMA-SLCGP@fema.dhs.gov that your entity will continue to use the CISA-approved Cybersecurity Plan; or
- Email your entity's revised Cybersecurity Plan, including a list of the revisions, to your FEMA Preparedness Officer at FEMA-SLCGP@fema.dhs.gov.
- Once the email or revised Cybersecurity Plan is received, FEMA will share that with CISA for their review and approval. FEMA will maintain records of CISA-approved plans and resubmitted plans for CISA review.

Starting in FY 2025, the requirements for Cybersecurity Plans and additional suggestions for revising or updating will **not** be included in the NOFO as an appendix. Instead, those requirements and suggestions will be available as a webpage on CISA.gov.

## Cybersecurity Planning Committees and Charter Requirements

Starting in FY 2025, requirements for cybersecurity planning committees, their associated charter and associated best practices will not be included in the NOFO as an appendix. Instead, those requirements will be available as a webpage on

CISA.gov.

## Performance Measures

CISA remains invested in collecting data to gauge program performance. In FY 2025, performance measures were adjusted to better to inform applicants of the information CISA will collect through the program duration. Each performance measure now includes a recommended target range to better communicate to applicants how CISA will measure the program's performance. Adjusted performance measures include the following:

- Percentage of entities conducting annual tabletop and full-scale exercises to test Cybersecurity Plans (40% target range).
- Amount of grant funds budgeted for cybersecurity exercises (10% target range).
- Percentage of grant funds expended on exercise plans for entities (10% target range).
- Percentage of entities conducting annual cyber risk assessments conducted to identify cyber risk management gaps and areas for improvement (80% target range).
- Percentage of entities performing phishing training (70% target range).
- Percentage of entities conducting awareness campaigns (90% target range).
- Percentage of entities providing role-based cybersecurity awareness training (90% target range).
- Percentage of entities with capabilities to analyze network traffic and activities related to potential threats (60% target range).
- Percentage of entities implementing multi-factor authentication (MFA) for all remote access and privileged accounts (70% target range).
- Percentage of entities with programs to anticipate and discontinue end-of-life software and hardware (60% target range).
- Percentage of entities prohibiting the use of known/fixed/default passwords and credentials (60% target range).
- Percentage of entities operating under the ".gov" internet domain (70% target range).
- Percentage of entities that reported CISA-identified Cybersecurity Gaps (50% target range).
- Percentage of entities with Endpoint Detection and Response systems that were funded for implementation (90% target range).

- Number of capabilities ratings improved (50% target range).
- Percentage of state/territory-created performance metrics that were met (50% target range).
- Percentage of entities participating in CISA services (50% target range).
- Percentage of entities that have implemented data encryption projects (50% target range).
- Percentage of entities that have implemented enhanced logging projects (60% target range).
- Percentage of entities that have implemented system reconstitution projects (60% target range).

Similar performance measures to those listed above have previously been included in the NOFO. CISA views the implementation of those best practices as informative in determining SLCGP's success. The following performance measures have been deprioritized in the FY 2025 NOFO:

- Number of employees that completed continuous learning activities on current cyber threats.
- Number of employees that completed education or training on software security concepts.
- Number of funding improvements that were made for Continuity of Operations Plans.
- Percentage of entities with membership in the Multi-State Information Sharing and Analysis Center (50% target range).

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.

## Required, Encouraged, and Optional Services, Memberships, and Resources

CISA added its Information Technology Sector Specific Goals (SSGs) to the Required, Encouraged, and Optional Services, Memberships, and Resources list in Appendix B of the NOFO. The Information Technology SSGs are additional voluntary practices with high-impact security actions, beyond the Cross-Sector CPGs, that outline measures IT Sector businesses and critical infrastructure

owners can take to protect themselves against cyber threats. They were developed based on CISA's operational data, research on the current threat landscape, and in collaboration with government, industry groups, and private sector experts. Additionally, all membership costs utilizing SLCGP funding must be approved in advance by FEMA.

**Recipients and subrecipients receiving FY 2025 SLCGP funding assistance are no longer required to participate in the Nationwide Cybersecurity Review (NCSR).** The NCSR is still required for SLCGP in FYs 2022, 2023, and 2024.

## Payment Reviews

FEMA is instituting additional reviews on all grant payments and obligations to ensure allowability in accordance with 2 C.F.R. § 200.305. These measures will ensure funds are disbursed appropriately while continuing to support and prioritize communities that rely on FEMA for assistance. Once a recipient submits a payment request, FEMA will review the request. If FEMA approves a payment, it will process the payment through FEMA Grants Outcomes (FEMA GO) and inform recipients accordingly for drawdown purposes. If FEMA disapproves a payment, FEMA will inform the recipient.

## Period of Performance Extension Requests

Extensions to the FY 2025 SLCGP period of performance (POP) for this program are not allowed.