DEPARTMENT OF EMERGENCY SERVICES & PUBLIC PROTECTION

DIVISION OF EMERGENCY MANAGEMENT & HOMELAND SECURITY

# State and Local Cybersecurity Grant Program (SLCGP)

## *Participant Guide*

***1111 Country Club Rd, Middletown, CT 06457***
*Phone: 860.256.0800 / Fax: 860.256.0815*
*An Affirmative Action/Equal Opportunity Employer*

# Table of Contents

**Statement of Purpose** ..... 3

**Section I. Program Information** ..... 4

Program Overview ..... 4

Funding and Pass Through Requirements ..... 4

Cost Share ..... 5

Period of Performance ..... 6

Eligible Entities and Sub-entities ..... 6

Connecticut Cybersecurity Plan ..... 6

Connecticut Cybersecurity Planning Subcommittee ..... 6

Initial Grant Program Funding Priorities ..... 7

**Section II. Subapplication Process** ..... 8

Subapplication Process Overview ..... 8

Subapplication Selection and Determination ..... 8

**Section III. Subgrant Management** ..... 9

Subrecipient Award Information ..... 9

**Notice of Grant Award Process** ..... 9

**Performance Reporting** ..... 9

**Extensions** ..... 9

Subrecipient Financial Subaward Information and Reimbursement Processes ..... 9

Budget Modifications ..... 10

**Section IV. Allowable Costs** ..... 11

Planning ..... 11

Organization ..... 11

Equipment (AEL) ..... 11

Training ..... 12

Exercise ..... 12

Training and Exercise Approval ..... 12

**Section VI. Unallowable Costs** ..... 13

**Section VII. Reference Materials and Documents** ..... 13

## Statement of Purpose

The State and Local Cybersecurity Grant Program (SLCGP) was created in 2022 through the Infrastructure Investment and Jobs Act (IIJA) by the federal government to award grants to eligible entities to address cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, state, local, or tribal governments..

The Connecticut State and Local Cybersecurity Grant Program (SLCGP) Participant Guide has been developed to provide information about the program and its implementation in Connecticut, while also providing guidance to eligible entities about the lifecycle of the grant process. This Program guide sets out to standardize the SLCGP program throughout the State of Connecticut for all Local and State Entity Applicants.

- An Overview of this Program can be found at the below link:
  - State and Local Cybersecurity Grant Program (ct.gov)
- All forms and documents in this manual can be found at the link below:
  - State and Local Cybersecurity Grant Program--Guidance and Forms (ct.gov)
- For any questions regarding this manual or the SLCGP program please email:
  - DEMHS.SLCGP@ct.gov

# Section I. Program Information

## Program Overview

The SLCGP provides funding to state, local, tribal, and territorial (SLTT) governments to address cybersecurity risks and cybersecurity threats to SLTT-owned or operated information systems. The overarching goal of the program is to assist SLTT governments in managing and reducing systemic cyber risks. The four main objectives of the program for which all projects at the state and local level must fall into are below:

- **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.

- **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

Before funding can be distributed to states and eligible sub-entities, the Homeland Security Act of 2002, as amended by the Bipartisan Infrastructure Law requires grant recipients (States) to develop a Cybersecurity Plan, establish a Cybersecurity Planning Committee to support development of the Plan, and identify projects to implement utilizing SLCGP funding. In order to comply with federal guidance, the Connecticut Department of Emergency Services and Public Protection/Division of Emergency Management and Homeland Security (DESPP/DEMHS), acting in its role as the designated State Administrative Agency (SAA) for this program, began working with the established Statewide Cybersecurity Committee in 2022 to prioritize the following activities to meet SLCGP grant requirements:

- Establish a Cybersecurity Planning Committee;
- Develop a state-wide Cybersecurity Plan, unless the recipient already has a state-wide Cybersecurity Plan and uses the funds to implement or revise a state-wide Cybersecurity Plan;
- Identify and support projects that meet the objectives documented in the plan.

The state used the first year of the FY 2022 SLCGP grant, to complete the Cybersecurity Plan and received approval from the Federal Emergency Management Agency (FEMA) and Cybersecurity & Infrastructure Security Agency (CISA) on September 21, 2023, opening up the opportunity to fund eligible cybersecurity projects under the SLCPG.

### Funding and Pass Through Requirements

The SLCGP funding available is dependent on the fiscal year. Currently, there are two fiscal years of funding available to Connecticut entities with different cost share (i.e., match) amounts. Below is a table of available federal funding and nonfederal requirement for each open fiscal year:

| Total 2022 SLCGP $2,978,432 | |
|---|---|
| **Federal Share (90%)** | $2,680,589 |
| **Non-Federal (10%)** | $297,843 |

| Total FY2023 SLCGP $6,832,344 | |
|---|---|
| **Federal Share (80%)** | $5,465,875 |
| **Non-Federal (20%)** | $1,366,469 |

Additionally, at least 80% of the federal funds provided under the grant to local governments, including rural areas, within the jurisdiction of the eligible entity. As part of the local government pass through requirement, at least 25% of the federal funds must be provided under the grant to rural areas. Per the Homeland Security Act of 2002, **a rural area** is defined in 49 U.S.C. § 5302 as an area encompassing a population of less than 50,000 people that has not been designated in the most recent decennial census as an "urbanized area" by the Secretary of Commerce.

## Cost Share

This program has a sliding cost share match requirement that changes with each fiscal year. For the FY 2022 funding, the federal share of any activity cannot exceed 90%. For example, if a local entity estimates the total cost of a project is $100,000, the local entity's cost share will be 10% or $10,000. The cost share must be at the activity (i.e., project) level). The cost share cannot be shared across multiple projects being implemented by the same entity. For a breakdown of cost shares by fiscal year, see below:

- FY 2022: 90% federal, 10% nonfederal
- FY 2023: 80% federal, 20% nonfederal
- FY 2024: 70% federal, 30% nonfederal
- FY 2025: 60% federal, 40%nonfederal

There are two types of cost share or "match" funding allowable under this program:

- **Hard Match (Cash)**
  - Cash or hard matching includes cash spent for project-related costs. The allowable cash match must include costs that are necessary, reasonable, and allowable under the SLCGP.
- **Soft Match (In-kind)**
  - Soft match refers to contributions of the reasonable value of property or services in lieu of cash which benefit a federally assisted project or program. Only costs that are associated with the SLCGP program's goals, objectives are allowable
  - In-kind match contributions may be non-cash services provided by non-Federal third parties for work on a project. These can be in the form of real property, equipment, supplies, services, etc. These costs should be included and factored into the budgets of proposed projects. For information on cost shares, please email DEMHS.SLCGP@ct.gov

## Period of Performance

The designated Period of Performance (POP) for each Fiscal Year of the SLCGP is 48 months (4 years).

## Eligible Entities and Sub-entities

The State of Connecticut is the sole eligible entity with the ability to submit SLCGP applications to DHS/FEMA. Eligible sub-entities able to apply for SCLGP funding include, State, tribal, and local governments. "Local government" is defined in 6 U.S.C. § 101(13) as

- A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments, regional or interstate government entity, or agency or instrumentality of a local government;
- An Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; and
- A rural community, unincorporated town or village, or other public entity.

Organizations listed above should complete this sub-application and submit to DEMHS in order to be eligible to receive SCLGP funding as a subrecipient.

## Connecticut Cybersecurity Plan

Submission of a Cybersecurity Plan is required for any eligible entity participating in the State and Local Cybersecurity Grant Program (SLCGP). The Connecticut Cybersecurity Plan is a key component of a strategic approach to building cyber resilience. Connecticut worked with local, state, and regional partners to develop a comprehensive cybersecurity plan that was submitted for approval to FEMA/CISA in September of 2023 and subsequently approved. The Cybersecurity Plan establishes the state's high level goals and objectives to reduce specific cybersecurity risks and also serves as the overarching framework for the achievement of the SLCGP goal, with grant-funded projects working to achieve outcomes. The State's Cybersecurity Goals and Objectives can be found on page 6 of the plan.

## Connecticut Cybersecurity Planning Subcommittee

The primary purpose of Cybersecurity Planning Subcommittee is to assist the State of Connecticut in development of the Statewide Cybersecurity Plan in accordance with the Notice of Funding Opportunity (NOFO) and to identify and support projects that meet the objectives documented in the plan. Additional responsibilities include:

- Assisting with the development, implementation, and revision of the Cybersecurity Plan;
- Approving the Cybersecurity Plan;
- Assisting with the determination of effective funding priorities;
- Coordinating with other committees and like entities with the goal of maximizing coordination and reducing duplication of effort;
- Ensuring investments support closing capability gaps or sustaining capabilities; and
- Assisting the state in ensuring local government members, including representatives from counties, cities, and towns within the eligible entity provide consent on behalf of all local entities across the eligible entity for services, capabilities or activities provided by the eligible entity through this program.

Connecticut's Cybersecurity Planning Subcommittee is made up of relevant stakeholders in the Cybersecurity discipline and as determined in the federal NOFO, and includes the State Chief Information Officer (CIO), the State Chief Information Security Officer (CISO), representatives from municipalities and the Regional Emergency Planning Team (REPT) – Cybersecurity Emergency Support Function (ESF)-17, institutions of public education, public health representation, and representatives of rural, suburban, and high-population jurisdictions.

More information can be found in the approved bylaws of the Charted Planning Subcommittee upon request.

## Initial Grant Program Funding Priorities

The Connecticut Cybersecurity Planning Subcommittee has recommended the following priorities for funding consideration under the first round(s) of the SLCGP:

- Implementing End Point Detection and Response capabilities;
- Training and workforce development centered around Cybersecurity;
- Implementing multi-factor authentication;
- Implementing enhanced logging;
- Implementing data encryption for data at rest and in transit;
- Implementing end use of unsupported/end of life software and hardware that are accessible from the Internet;
- Prohibiting use of known/fixed/default passwords and credentials;
- Ensuring the ability to reconstitute systems (backups); and
- Migrating to the .gov internet domain.

These priority areas have been established to reflect federal NOFO priorities and based on recommendations from the chartered cybersecurity planning subcommittee. All projects submitted on a subapplication should meet or fill a gap identified on a vulnerability assessment or aim to achieve a strategic objective of the Connecticut Cybersecurity Plan.

# Section II. Subapplication Process

## Subapplication Process Overview

In order to equitably distribute the funding to the widest audience of eligible entities, the Chartered Planning Subcommittee has determined to pass-through 80% of the federal funding to eligible sub-entities through individual subawards. In order to generate subawards, a Connecticut SLCGP Subapplication has been created and will be released contingent on federal fiscal year funding availability. The following are components of the Connecticut SCLGP sub-application that must be completed in order to be considered for funding.

- Background Narrative and Gaps
- Proposed Project Description
- Work Schedule and Milestones
- Budget

More information about each section and subapplication requirements, can be found in the subapplication.

## Subapplication Selection and Determination

The Chartered Cybersecurity Planning Subcommittee will collect subapplications through the established subapplication period and organize the submissions by project type and objective. Each application will be reviewed for completeness and weighed on strength of proposed reduction in identified risk, either using gaps identified in recent vulnerability assessments or other strategic cybersecurity risk reduction efforts.

DEMHS will aggregate the subapplications and create four Investment Justifications (one for each program objective) and submit the projects to FEMA/CISA for review and approval. Project eligibility and alignment with the State's Cybersecurity Plan, will be considered before submitting to FEMA/CISA, in order to ensure projects submitted for funding are meeting with the program priorities and goals.

# Section III. Subgrant Management

The following is some, but not all, of the steps of subgrant management by awarded subrecipients under the SLCGP. For full compliance and instructions, subrecipients should refer to the Notice of Grant Award and the conditions set therein.

## Subrecipient Award Information

### Notice of Grant Award Process

The Subrecipient will receive a Notice of Grant Award Package after a submitted project application has been submitted by DEMHS to FEMA/CISA and subsequently approved. The CEO/Authorized Signatory must sign the Notice of Grant Award Page. All pages of the Notice of Grant Award document require review and acknowledgement by the Authorized Signatory. The NOGA includes information such as the subrecipient name, address, award number, FEIN and Unique Employer Identifier (UEI) or DUNS number, subaward amount, and grant award conditions. Once DEMHS has received the returned NOGA, it shall be forwarded to the Deputy Commissioner for signature and execution of the award.

### Performance Reporting

Subrecipients are required to submit quarterly reporting documents, consisting of a Quarterly Progress Report and a Quarterly Financial Report. These reports are due within 30 days of the close of the quarter (3/31; 6/30; 9/30; 12/31) regardless of whether works was performed during the quarter or not. These reports are due the first quarter after the Notice of Grant Award is returned and every quarter thereafter until the grant is closed out. Information to be provided in quarterly progress reports includes but is not limited to:

- Brief narrative of overall project(s) status;
- Summary of project expenditures;
- Description of any potential issues that may affect project completion; and
- Data collected for DHS performance measures (if applicable)

### Extensions

The federal period of performance (POP) of each fiscal year of a SLCGP grant is 48 months, with three months following the end of the POP for liquidation and closeout.

DEMHS will establish subgrant awards under this program based on project approval dates from FEMA/CISA, but always six months before the end of the appropriate federal period of performance, to encourage completion of projects in a timely manner, while also allowing flexibility for subgrant extensions in certain situations. In order to submit for a subgrant period of performance extension, subrecipients must request via email and/or submit a Grant Modification Request form and submit to the DEMHS Program Manager for review and approval.

## Subrecipient Financial Subaward Information and Reimbursement Processes

The SLCGP program is a reimbursement program. Subrecipients must submit complete requests to the DEMHS SLCGP Program Manager using a DEMHS Reimbursement Request Form, along with all associated invoices and proofs of payments (copies of checks or credit card statements).

Before a payment can be processes and issued, DEMHS will review the request form and associated documents for completeness and compliance with the grant program conditions and original and approved subgrant budget. Additionally, up-to-date quarterly reports must be on file. All documents are found electronically on the DEMHS website. The reimbursement request form summarizes the request and provides a checklist for different types of documentation that should be required. This form is included as part of the notice of grant award, and available on the DEMHS website.

## Budget Modifications

Subrecipients are permitted to reallocate funding between approved line items, with approval from the SAA and FEMA. Funds can only be reallocated to projects (line items) included in the original application. DEMHS may request a revised Project Description/Budget be submitted to DEMHS showing the adjustments.

DEMHS uses a Grant Modification Form that is used by subrecipients to request organizations complete when seeking a significant modification to the SLCGP subaward. If the modification request is a budget modification and the subrecipient is reallocating funds between pre-approved line items, then the request may be approved internally by CT DEMHS, if the budget reallocation is less than 10% of the total federal award. The subrecipient may be requested to submit the Grant Modification form to the program manager proposing the budget changes and providing an explanation and revised budget, including shifts between Planning, Organization, Equipment, Training, and Exercise (POETE) elements for DEMHS tracking.

Any changes or modifications to approved and existing scopes of work, must be submitted to DEMHS and approved by FEMA/CISA before a subrecipient may begin that work.

## Section IV. Allowable Costs

As per the Notice of Funding Opportunity, all costs charged to awards covered by this NOFO must comply with the Uniform Administrative Requirements, Cost Principles, and Audit Requirements at 2 C.F.R. Part 200, unless otherwise indicated in the NOFO or the terms and conditions of the award. Additionally, all costs charged to awards must comply with the grant program's applicable statutes, policies, requirements in this NOFO as well as with the terms and conditions of the award.

### Planning

SLCGP funds may be used for a range of planning activities, such as those associated with the development, review, and revision of the holistic, entity-wide cybersecurity plan and other planning activities that support the program goals and objectives and Cybersecurity Planning Committee requirements. P**lanning costs are only allowable under FY 2022.** For all other fiscal years after FY 2022, planning costs are not eligible.

### Organization

Some organizational costs are eligible under this program. Eligible entities must justify proposed expenditures of SLCGP funds to support organization activities within their IJ submission and must demonstrate that the personnel will be sustainable. For more information on specific eligibility, please reach out to DEMHS.SLCGP@ct.gov.

### Equipment (AEL)

Equipment costs are allowable under this program. SLCGP equipment is intended to be used to address cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, state and local governments. A comprehensive list of eligible equipment types, **(including software as a service)** and the Preparedness Programs they correspond with is published on FEMA's Authorized Equipment List | FEMA.gov.

As per the Notice of Funding Opportunity, SLCGP funds may be used to purchase maintenance contracts or agreements, warranty coverage, licenses, and user fees in support of a system or equipment. These contracts may exceed the period of performance if they are purchased incidental to the original purchase of the system or equipment as long as the original purchase of the system or equipment is consistent with that which is typically provided for, or available through, these types of agreements, warranties, or contracts. When purchasing a stand-alone warranty or extending an existing maintenance contract on an already-owned piece of equipment system, coverage purchased may not exceed the period of performance of the award used to purchase the maintenance agreement or warranty, and it may only cover equipment purchased with SLCGP funds or for equipment dedicated for SLCGP-related purposes. As with warranties and maintenance agreements, this extends to licenses and user fees as well. The use of SLCGP grant funds for maintenance contracts, warranties, repair or replacement costs, upgrades, and user fees are allowable, unless otherwise noted. Except for maintenance plans or extended warranties purchased incidental to the original purchase of the equipment, the period covered by maintenance or warranty plan must not exceed the POP of the specific grant funds used to purchase the plan or warranty.

If an item's eligibility is questioned or if it is not listed, please consult with your DEMHS State and Local Cybersecurity Grant Program Manager for a determination. DEMHS will consult with FEMA to

receive an official decision on the eligibility of the equipment in question. Additionally, the subrecipient must comply with any specific notes listed in the AEL regarding the purchase and use of equipment.

## Training

Training costs are allowable under this program. Allowable training-related costs under SLCGP include the establishment, support, conduct, and attendance of training and/or in conjunction with training by other federal agencies. Training conducted using SLCGP funds should align to the eligible entity's Cybersecurity Plan and address a performance gap identified through assessments and contribute to building a capability that will be evaluated through a formal exercise. Any training or training gaps, including training related to underserved communities that may be more impacted by disasters, including children, seniors, individuals with disabilities or access and functional needs, individuals with diverse culture and language use, individuals with lower economic capacity and other underserved populations, should be identified in an assessment and addressed in the eligible entity's training cycle.

## Exercise

Exercise costs are allowable under this program. Exercises conducted with grant funding should be managed and conducted consistent with Homeland Security Exercise and Evaluation Program (HSEEP). HSEEP guidance for exercise design, development, conduct, evaluation, and improvement planning is located at https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep. The DEMHS Training and Exercise Unit is able to assist with exercise design as necessary.

### Training and Exercise Approval

All training and exercise requests must be submitted on the subapplication or emailed to DEMHS.SLCGP@ct.gov and approved by the Chartered Planning Subcommittee and DEMHS Training and Exercise Manager prior to start.

## Section VI. Unallowable Costs

The following items or services are ineligible and therefore unallowable costs under this program. Inclusion of any of these items or services on an application or subaward, will result in modifications to eligible expenses for projects.

- To supplant state or local funds; however, this shall not be construed to prohibit the use of funds from a grant under this NOFO for otherwise permissible uses on the basis that the SLT has previously used SLT funds to support the same or similar uses;
- For any recipient cost-sharing contribution;
- To pay a ransom;
- For recreational or social purposes;
- To pay for cybersecurity insurance premiums;
- To acquire land or to construct, remodel, or perform alternations of buildings or other physical facilities;
- To match funds for other federal grants/cooperative agreements, lobbying, or intervention in federal regulatory or adjudicatory proceedings;
- To sue the federal government or any other government entity; and,
- For any purpose that does not address cybersecurity risks or cybersecurity threats on information systems owned or operated by, or on behalf of, the eligible entity that receives the grant or a local government within the jurisdiction of the eligible entity

## Section VII. Reference Materials and Documents

The following are some, but may not be all, of the referenced documents or materials that provide program guidance and strategy to Connecticut's implementation of the SLCGP:

- Federal
    - Homeland Security Act of 2002, as amended
    - FEMA/DHS National Preparedness Goal, as amended
    - FEMA/DHS National Prevention Framework, as amended
    - FEMA/DHS NOFOs and Ancillary Documents
    - FEMA/DHS State and Local Cybersecurity Grant Program (SLCGP) Program Guidance
- State
    - Approved Connecticut Cybersecurity Plan, 2023
    - State of Connecticut's Cyber Disruption Response Plan (CDRP)
    - State of Connecticut's Cybersecurity Strategy
    - State of Connecticut's Cyber Incident Response Plan