DEPARTMENT OF EMERGENCY SERVICES & PUBLIC PROTECTION

DIVISION OF EMERGENCY MANAGEMENT
& HOMELAND SECURITY

State and Local Cybersecurity Grant Program (SLCGP)

Eligible Entity Subapplication

APPLICATION DUE
no later than 5:00PM on July 19th 2024

Table of Contents

Subapplication Instructions

Completed application packages should be emailed to DEMHS.SLCGP@ct.gov with the subject line: "CT-SCLGP_Round 1_Entity Name" no later than 5:00PM on July 19th 2024

Applicant Data Sheet:

Please provide the requested information of this form. Please note that your grant award and any related documents will be sent to you via e-mail, so it is imperative that you include e-mail addresses in the contact boxes. The application must be approved by an authorized person in your organization (digital or ink signatures are acceptable), and this person should be listed as a contact in your data sheet. Please include more than one point of contact for your organization.

Background Narrative and Gaps

Use this section to provide a needs statement for your project and how the proposed projects will close existing gaps and an overview of the population served. Provide or attach a clear description of the existing conditions that your project is intended to mitigate. You may also include information about the frequency with which incidents or threats occur and the potential impacts of disruptions or incidents including any cascading impacts to the State.

Proposed Project Description

Provide a detailed project description and/or scope of work (SOW) for all work required to implement the proposed activity and the associated cost and timeframes as it relates to the state and federal priority areas and program objectives.

Work Schedule and Milestones

Please provide a detailed work schedule and timeframe for the proposed project (attach a separate schedule or add additional lines as necessary). Make sure work schedule allows for grant administration, bidding, installation, and unanticipated delays. Be conservative and request more time than you think you need – you will not be penalized for completing the project sooner than the requested performance period. The SLCGP has a four-year period of performance to complete eligible activities.

Budget (Separate Spreadsheet):

Using the provided spreadsheet, submit a detailed line item budget/cost estimate including line descriptions or narratives that describe all anticipated costs associated with the proposed project description.

If 'in-kind' contributions related to the project are being claimed as part of the grant match requirements, the subapplication budget should reflect the basis for the valuation of the Contributions.

This application is for use by eligible sub-entities and non-Executive Branch state agencies.

Please reach out to DEMHS.SLCGP@ct.gov with any questions or issues with this application

Key Program Information

Eligible 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 sub-recipient.

State of Connecticut Cybersecurity Grant Program 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.

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.

Required CISA Services If Awarded:

All SLCGP recipients and subrecipients are required to participate in a limited number of free services by CISA. For these required services and memberships, please note that participation is not required for submission and approval of a grant but is a post-award requirement.

- **Web Application Scanning** is an "internet scanning-as-a-service." This service assesses the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and government best practices and standards.
- **Vulnerability Scanning** evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts.
- **Completing the Nationwide Cybersecurity Review**, administered by the MS-ISAC, during the first year of the award/subaward period of performance and annually thereafter. The NCSR is a free, anonymous, annual self-assessment designed to measure gaps and capabilities of a SLT's cybersecurity programs.

Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services:

Recipients and subrecipients of FEMA federal financial assistance are subject to the prohibitions described in section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (FY 2019 NDAA), Pub. L. No. 115-232 (2018) and 2 C.F.R. §§ 200.216, 200.327, 200.471, and Appendix II to 2 C.F.R. Part 200. Beginning August 13, 2020, the statute – as it applies to FEMA recipients, subrecipients, and their contractors and subcontractors – prohibits obligating or expending federal award funds on certain telecommunications and video surveillance products and contracting with certain entities for national security reasons.

Guidance is available at FEMA Policy #405-143-1: Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services or superseding document.

Additional guidance is available at Contract Provisions Guide: Navigating Appendix II to Part 200 - Contract Provisions for Non-Federal Entity Contracts Under Federal Awards.

Effective August 13, 2020, FEMA recipients and subrecipients may not use any FEMA funds under open or new awards to:

- Procure or obtain any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology of any system;
- Enter into, extend, or renew a contract to procure or obtain any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology of any system; or
- Enter into, extend, or renew contracts with entities that use covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system.

Section I. Applicant Data Sheet

SECTION I. SLCGP FUNDING APPLICATION INFORMATION AND DATA SHEET

Email Completed Applications To:
DEMHS.SLCGP@ct.gov

1. Name of Municipality or Entity Applying for Subgrant:

2. Period of Award for this Subgrant: 12/01/2022-08/30/2026

3. Project Point of Contact Name & Address
Name: Title:
Organization:
Address Line 1:
Address Line 2:
City/State/Zip:
Phone: Fax:
E-mail:

4. Official Authorized to Sign for the Applicant:
Name: Title:
Organization:
Address Line 1:
Address Line 2:
City/State/Zip:
Phone: Fax:
E-mail:

5. Municipal/Entity Financial Officer
Name: Title:
Organization:
Address Line 1:
Address Line 2:
City/State/Zip:
Phone: Fax:
E-mail:

6. Fiscal Point of Contact: (If Different than Financial Officer)
Name: Title:
Organization:
Address Line 1:
Address Line 2:
City/State/Zip:
Phone: Fax:
E-mail:

7. Applicant FEIN:

8. Applicant UEI #:

9. Applicant Fiscal Year End:

10. Date of Last Audit:

11. Dates Covered by Last Audit: to

12. Date of Next Audit:

13. Dates to be Covered by Next Audit: to

Please note that the information required for boxes 9 through 13 refers to the sub-grantee's audit cycle.

FEDERAL AUDIT AND DEBARMENT REQUIREMENT CERTIFICATION

14. ACKNOWLEDGEMENT OF FEDERAL SINGLE AUDIT SELF REPORTING REQUIREMENTS

- Sub-grantees that are required to undergo a Federal Single Audit as mandated by OMB Circular A-133 must alert CT DEMHS, in writing, to any specific findings and/or deficiencies with regard to the use of federal grant funds within 45 days of receipt of their audit report. This notification must identify the finding(s) / deficiencies and a corrective action plan for each.
- All sub-grantees must submit to CT DEMHS a copy of the audit report section pertaining to use of federal grant funds regardless of any findings or deficiencies, within 45 days of the receipt of that report.

Initial to indicate that this requirement has been read and understood:___________.

INITIAL

15.ACKNOWLEDGEMENT OF DEBARMENT REQUIREMENTS:

- The sub-grantee will confirm the eligibility status (via Sam.gov) of all vendors/contractors that the sub-grantee pays with SLCGP subaward funds. The subgrantee will confirm that the vendors/contractors do not appear on the SAM's Exclusion List of federally suspended vendors.

Initial to indicate that this requirement has been read and understood:___________.

INITIAL

16. I, the undersigned, for and on behalf of the named municipality, state agency, or regional planning organization, do herewith apply for this subgrant, attest that, to the best of my knowledge, the statements made herein are true, and agree to any general or special grant conditions attached to this grant application form.

SIGN & DATE

Authorized Signatory: X ______________________________________ Date: ____________________

Rural Area Identifier

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.

Please indicate whether your organization or entity identifies under the definition of "Rural Area" as defined above.

○ **Rural** ○ **Non-Rural**

Section II. Background Narrative and Gaps

The State of Connecticut Chartered Planning Subcommittee has recommended that the first iteration of State and Local Cybersecurity Grant Program (SCLGP) funding be focused on **End Point Detection and Response** (Objective 3) and **Workforce Development and Training** (Objective 4). Additional recommendations for funding include emphasizing projects that complete one or more of the following cybersecurity best practices:

- 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.

A. Provide a baseline understanding of the existing cybersecurity gaps, risks, and threats that the applicant entity faces which have influenced the development of this project proposal. Also, please include a summary of the current capabilities within your organization to address these threats and risks. Any information provided regarding vulnerabilities is protected information and will not be shared publicly.

B. **What Objective from the State and Local Cybersecurity Grant Program does your project align with?**

□ **Governance and Planning:**
Develop and establish appropriate governance structures, as well as plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations

□ **Assessment and Evaluation:**
Identify areas for improvement in SLTT cybersecurity posture based on continuous testing, evaluation, and structured assessments.

□ **Mitigation:**
Implement security protections commensurate with risk (outcomes of Objectives 1 and 2), using the best practices as described in element 5 of the required 16 elements of the cybersecurity plans and those further listed in the NOFO.

□ **Workforce Development:**
Ensure organization personnel are appropriately trained in cybersecurity, commensurate with their responsibilities as suggested in the National Initiative for Cybersecurity Education.

C. **Describe how your proposal and the associated project(s) identified, addresses gaps and/or sustainment in the Connecticut Cybersecurity Plan.**

Section III. Proposed Project Description

A. **Provide below or attach a clear description of the proposed project and the work to be accomplished. If you would like to attach additional materials, use the gray button below and they will be attached to this PDF application**

Click to Upload Scope of Work Narrative As Attachment

B. **Describe how the project(s) proposed are commensurate with cybersecurity vulnerabilities identified in a recent cybersecurity vulnerability assessment of your organization (vendor-provided, CT National Guard, etc.).**

Any information provided regarding vulnerabilities is protected information and will not be shared publicly.

C. **Please select the appropriate State of Connecticut Cybersecurity priority area that your proposed project aligns with. If none apply, please indicate in the "other" box.**

□	Endpoint Detection and Response*	
□	Workforce Development and Training*	
□	Implement multi-factor authentication	
□	Implement enhanced logging	
□	Data encryption for data at rest and in transit	
□	End use of unsupported/end of life software and hardware that are accessible from the Internet	
□	Prohibit use of known/fixed/default passwords and credentials	
□	Ensure the ability to reconstitute systems (backups)	
□	Migration to the .gov internet domain.	
□	Other – *please define*	

**Indicates a priority of the Cybersecurity Planning Subcommittee*

D. Briefly describe how this project aligns to the 16 required elements of a Cybersecurity Plan outlined in Appendix C (page 66) of the the FY 2022 SLCGP Notice of Funding Opportunity. If not applicable, indicate as N/A Upload Additional Attachments if Desired

1.	Manage, monitor, and track information systems, applications, and user accounts	
2.	Monitor, audit, and track network traffic and activity	
3.	Enhance the preparation, response, and resiliency of information systems, applications, and user accounts	
4.	Implement a process of continuous cybersecurity risk factors and threat mitigation. practices prioritized by degree of risk	
5.	Adopt and use best practices and methodologies to enhance cybersecurity (references NIST)	
	a. Implement multi-factor authentication	
	b. Implement enhanced logging	
	c. Data encryption for data at rest and in transit	
	d. End use of unsupported/end of life software and hardware that are accessible from the Internet	
	e. Prohibit use of known/fixed/default passwords and credentials	
	f. Ensure the ability to reconstitute systems (backups)	
	g. Migration to the .gov internet domain	
6.	Promote the delivery of safe, recognizable, and trustworthy online services, including using the .gov internet domain	
7.	Ensure continuity of operations including by conducting exercises	
8.	Identify and mitigate any gaps in the cybersecurity workforces, enhance recruitment and retention efforts, and bolster the knowledge, skills, and abilities of personnel (reference to NICE Workforce Framework for Cybersecurity)	
9.	Ensure continuity of communications and data networks in the event of an incident involving communications or data networks	
10.	Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the eligible entity	
11.	Enhance capabilities to share cyber threat indicators and related information between the eligible entity and the Department	
12.	Leverage cybersecurity services offered by the Department	
13.	Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives	
14.	Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats	
15.	Ensure rural communities have adequate access to, and participation in plan activities	
16.	Distribute funds, items, services, capabilities, or activities to local governments	

Section IV. Budget

State and Local Cybersecurity Grant Program Project Budget Instructions:

Enter the estimated cost for each allowable project. If a project / item is not listed, email DEMHS.SLCGP@ct.gov for allowability. If deemed allowable, include the item in the appropriate Ŏl·űŜƎƻǸèɸ Project eligibility guidelines may be found in the State and Local Cybersecurity Grant Program (SLCGP) Participant Guide and Grant Information

wŜűǸƻl·ŎűʎØŜ tǸƻƨŜŎűăY

ǈ Ŧ l·ƴŜʄƎʎōfŜ Ŝƴűʎűè ʎYǇfŜYŜƴűŜŘ l·ƴŜʄƎʎōfŜ ŎèōŜǸăŜŎdzǸʎűè ǇǸƻƨŜŎű űKl·ű ø l·ă **not** ǇǸŜØʎƻdzăfè ōdzŘƎŜűŜŘ in past fiscal yearsΣ ʎű Yl·è ăŜŜʅ ǸŜʎYōdzǸăŜYŜƴű ŦƻǸ ăl·ʎŘ ǇǸƻƨŜŎűΣ ʎŦ űKŜ ǇǸƻƨŜŎű ōŜƎl·ƴ **after a third-party provided cybersecurity vulnerability assessment (e.g. vendor provided, National Guard, etc.) and after 12/1/2022.**

Eligible sub-entities should submit one, unified budget and subapplication, when possible, to avoid duplication of services or application review issues.

Directions:

Use the "*CT-SLGP_Round 1_Budget Spreadsheet*" *document* to complete this section

1. Enter the full cost of the project(s), the budget spreadsheet will calculate the federal and non-federal shares at the bottom.

2. Please indicate the estimated amount per project by funding category for the entity in the correlating section. A description of these categories is provided in the Participant Guide. The Participant Guide details what costs are eligible under these categories.

   The budget categories are:

   a. **Planning**
   b. **Organization**
   c. **Equipment**
   d. **Training**
   e. **Exercises**

3. If you have issues accessing the budget spreadsheet, it can be found in the attachments pane of this PDF, and also Online at:
   a. https://portal.ct.gov/demhs/grants/state-and-local-cybersecurity-grant-program/apply

4. If you have questions about how to complete the budget spreadsheet, please email DEMHS.SLCGP@ct.gov

****ONE** Budget Spreadsheet should be submitted for ***each subapplication*** per subentity if possible

Save the Budget Spreadsheet as

"CT-SCLGP_Round 1_Entity Name_Budget"

Section V. Subapplication Submission Consent and Cost Share Match Commitment

A. Match Commitment

I hereby certify that the required non-federal match of this project is available and agree to make available non-federal funds to carry out an SLCGP award in an amount not less than 10% of activities under the award. The source of the match funding is:

□ Available as a cash match from the entity named in this subapplication.

□ Available through in-kind services and documented in accordance with appropriate backup documentation not limited to, timesheets, payroll records, and other financial and project-related documentation.

Describe the source of local share:

B. Does your organization anticipate difficulty or challenges to implementing the aforementioned project(s) outlined in this sub-application due to cost share requirements?

○ **Yes**

○ **No**

C. Commitment to Required CISA Services

I hereby agree that, if awarded under this program, this organization will participate in the free services provided by CISA as a post-award requirement as outlined in the Notice of Funding Opportunity.

○ **Yes**

○ **No**

D. Subapplication Submission

To the best of my knowledge and belief, all data/information that is submitted within this Sub-Application is true and correct. I represent this Sub-applicant and am authorized by the governing body of this organization to apply for this funding and if awarded, to commit the non-federal matching share.

Type Title Date