

FY25 SLCGP Application Sections – **REFERENCE GUIDE ONLY**

* Organization Type ⓘ

- ☐ Local Government
- ☐ Tribe
- ☐ State Agency
- ☐ Community College

* Rural Community (Population less than 50,000) ⓘ

- ☐ Yes
- ☐ No

i button:

Are you a rural community? Population < 50k (Community colleges must use the county corresponding to the official address of the main campus).

* Primary POC ⓘ

--None--

✓ Project Manager

* Project Manager Name

* Project Manager Title

* Project Manager Email

* Project Manager Phone

✓ Financial Officer

* Financial Officer Name

* Financial Officer Title

* Financial Officer Email

* Financial Officer Phone

▼ Authorizing Official

* Authorizing Official Name

* Authorizing Official Title

* Authorizing Official Email

* Phone

Project Title: 250 characters

Purpose: 1,000 characters

NCEM SLCGP Grant

* Project Title ⓘ

This is a Title

* Purpose ⓘ

Choose one:

* Project Objective ⓘ

- ☐ Objective 1: Develop and establish appropriate governance structures, including by 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.

Choose all that apply:

* Required Elements Addressed ⓘ

- ☐ (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 resilience of information systems, applications, and user accounts.
- ☐ (4) Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by risk.
- ☐ (5) Adopt and use best practices and methodologies to enhance cybersecurity.
- ☐ (6) Transition to a .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.
- ☐ (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
- ☐ (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

Choose all that apply:

*Cybersecurity Best Practices ⓘ

- ☐ (1) Implement multifactor authentication
- ☐ (2) Enable enhanced logging
- ☐ (3) Use data encryption for data at rest and in transit
- ☐ (4) End the use of unsupported/end of life software and hardware that are accessible from the internet
- ☐ (5) Prohibit use of known/fixed/default passwords and credentials
- ☐ (6) Ensure the ability to reconstitute systems (backups)
- ☐ (7) Actively engage in rapid bidirectional sharing between CISA and SLT entities to drive down cyber risk
- ☐ (8) Migrate to the .gov internet domain

Environmental, Planning, and Historic Preservation (EHP) Assessment

Per the [FY25 SLCGP NOFO](#), grant funds may **not** be used to acquire land or to construct, remodel, or perform alterations of buildings or other physical facilities; however, this prohibition does not include “minor building modifications” necessary to install and connect grant-purchased equipment that do not substantially affect a building’s structure, layout, systems, or critical aspects of a building’s safety, or otherwise materially increase the value or useful life of a building. Therefore, grant applications requesting funds to acquire land or to construct, remodel, or perform alterations of buildings or other physical facilities beyond “minor building modifications” as described above will be rejected. See [Information Bulletin No. 523: Guidance on Fiscal Years 2022–2024 State and Local Cybersecurity Grant Program \(SLCGP\) Minor Modifications to Existing Facilities or Other Physical Facilities](#) for more details.

Minor modifications may be permitted with appropriate MA Environmental Planning and Historic Preservation (EHP) review and compliance.

* Project Requires an EHP Assessment ⓘ

--None--

In the narrative sections below:

If this screen will not submit and boxes are outlined in red, you have exceeded the allowable character count. The character count includes spaces and enter/carriage returns. Therefore, please do not worry about paragraph formatting and go ahead and submit one inclusive paragraph. Alternatively, you will have the option to upload files later in the application and you may upload a file or files for these sections (enter something like “see attachment” in the fields below, if you do this). Just don’t forget to upload the attachments because this is a very competitive grant and the committee can only make selections based on what they receive. They cannot reach back out to you.

Project Narrative: 2,500 characters

NCEM SLCGP Grant

* Project Narrative

Our project ...

Budget Narrative: 2,500 characters

* Budget Narrative ⓘ

i button:

Describe in narrative form your project's budget plan, demonstrating how it will maximize cost effectiveness of grant expenditures. Describe your plan for financial sustainability (how you will maintain the respective services/equipment after life of grant). Confirm that the required local matching funds are available.

Impacts/Outcomes: 2,500 characters

* Impacts/Outcomes ⓘ

i button:

Describe in narrative form the solution; describe in detail what will be accomplished by this project. Include what procedures will be implemented, what capabilities will be enhanced, how identified threats and hazards will be mitigated, and the ways in which improvements will be measured/evaluated. Which objectives in the NOFO will be met (1-4)? [Which sub-objectives?](#) Which required elements will be met (1-16)? Which required cybersecurity best practices will be met (1-8)?

Milestone Target Completion Dates

* Execute MOA

* Procure Goods/Services

* Submit Final Reimbursement Request

* Close Out Grant

Notes on the above dates:

For FY24, MOAs have been going out: End of October 2025, so 2026
For FY25, End of Period of Performance: March 31, 2029
All reimbursement requests must be received: April 30, 2029

Create Budget Line

The required match/cost share for FY25 SLCGP is 40% of total project costs.

For example, if an applicant submits a project costing \$100,000, the applicant would be responsible for \$40,000 of those costs, and they would only be applying for \$60,000 of federal funding for the project ($\$60,000 \text{ federal funding} / .60 = \$40,000 \text{ subrecipient match/cost share}$). If an applicant is applying for a \$250,000 federal award for FY25 SLCGP, their required match/cost share would be \$166,666.67, for total project costs of \$416,666.67.

Applicants who cannot cover the required match/cost share should not apply for FY25 SLCGP.

The required match can be "hard" (cash) or "soft" (in-kind). It is simpler if the match category is in the same category as the requested funds, but it is not required. For example, if your total project costs are \$100K to purchase software, you could match the \$60K federal funds for equipment with \$40K local funds for cybersecurity training; however, it would be simpler just to match the \$60K federal funds with the additional \$40K local funds for the equipment.

Category:

Planning

Organization

Equipment (*must* have AEL)

i button:

Search for AEL here: <https://www.fema.gov/km/grants/tools/authorized-equipment-list#browse> , for example, the AEL for SAAS (software as a service) is 04AP-11-SAAS - Applications, Software as a Service.

Training

Exercise

* Category

Equipment

* AEL ⓘ

* Description

* Total Cost (Federal share + Match)

Federal Share

Match

Green box added just for notes in this Guide:

There are no fillable fields in this area because the 60/40 split will auto-calculate for you based on dollar value you enter for total cost of that expenditure.

NCEM SLCGP Grant

Would you like to create an additional budget line?

Yes

No

Previous

NCEM SLCGP Grant

Please add any additional information you want us to know below

Additional Information

The field above is optional.

Attach any **optional** documentation in support of your grant application here. This is not required, only optional. Applicants can upload as many files as desired here.

Select a file to upload

 Upload Files

Or drop files

Cybersecurity Posture Questions

* (1) Does your organization have a written security policy that employees must consent to annually?

--None--



* (2) Do all employees receive annual cybersecurity awareness training?

--None--



* (3) Does your organization have antivirus software on all workstations?

--None--



* (4) Does your organization have antivirus software on all servers?

--None--



* (5) Does your organization have a firewall?

--None--



* (6) Does your organization utilize a centralized patch management solution?

--None--



* (7) Is your organization's data regularly backed up via non-domain joined solution (external media, cloud solution, etc)?

--None--



* (8) Is your organization using intrusion detection solutions to stop external attacks?

--None--



* (9) Is your organization using intrusion prevention solutions to stop external attacks?

--None--



* (10) Are user accounts and permissions actively monitored and routinely audited?

--None--



* (11) Is your organization using any centralized logging solution?

--None--



* (12) Does your organization require multi-factor authentication for e-mail account access?

--None--



* (13) Does your organization require multi-factor authentication for Domain admin accounts (or other privileged accounts)?

--None--

* (14) Does your organization require multi-factor authentication for VPN access?

--None--

Applicant affirms and attests that the following:

* Certification 1

--None--

This application includes complete and accurate information.

* Certification 2

--None--

Submission of the project proposal does not guarantee funding.

* Certification 3

--None--

Any person who knowingly makes a false claim or statement in connection with this application may be subject to civil or criminal penalties under 18 U.S.C. section 286, 18 U.S.C. section 1001, 31 U.S.C. section 3729 and N.C.G.S sections 1-605 through 618 (North Carolina False Claims Act).

* Certification 4

--None--

Receiving SLCGP funding requires signing-up for [cyber hygiene services](#) as specified in the SLCGP NOFO.

* Certification 5

--None--

Projects with funds allocated for equipment are required to check all equipment purchases against the [FEMA Authorized Equipment List](#).

* Certification 6

--None--

Any project having the potential to impact the environment, historical or cultural resources must submit an [Environmental and Historic Preservation Form](#).

* Certification 7

--None--

Entities must be able to sustain capabilities once SLCGP funds are no longer available.

* Certification 8

--None--

Projects with funds allocated for Emergency Communications must meet applicable [SAFECOM Guidance Recommendations](#). Such investments must be coordinated with the [NC State Interoperability Executive Committee \(SIEC\)](#) to ensure interoperability and long-term compatibility.

NCEM SLCGP Application

Your application has been submitted. Thank you for applying to the SLCGP Grant.

Please click here to view your submitted application: [App-0001413](#)

Submit

To Update Application

Start at **Applications** object (*not* Home)

Don't see your application? Make sure "All Applications" is selected (and pin).

North Carolina Emergency Management (NCEM)

Home Account Profile Request for Information My LOIs Applications Awards Projects Project Management Reimbursements More

Applications

All Applications

23 items • Sorted by Application Number • Filtered by All Applications • Updated 10/30/2025, 8:32 AM

	Application Number	Account	Project Title	Budget T...	Created By	Created Date
1	App-0001413	Z_ALPHA_TE	This is a Title	\$180.00	subapplicant Jeff C...	10/30/2025, 8:32 AM
2	App-0001411	Z_ALPHA_TE	Cybersecurity Enhancement	\$83,072.40	subapplicant Jeff C...	10/29/2025, 10:32 PM
3	App-0001392	Z_ALPHA_TE	FY24 NSGP-NSS - target hardening ...	\$150,000.00	derek.dorazio	10/27/2025, 2:32 PM

Click on your application and click "Update Application" button on next screen:

North Carolina
Emergency Management (NCEM)

Home Account Profile Request for Information My LOIs Applications Awards Projects Project Management Reimbursements More

Application
App-0001411

Status: Pending Account: [Z_ALPHA_TEST](#) Notice of Funding: [FY25 State and Local Cybersecurity Grant Program \(SLCGP\)](#) Budget Total: \$83,072.40

+ Follow Update Application Withdrawal Printable View

DETAILS RELATED

EMD-000009179 - jeff.cox (Customer) created a em document. 34m ago

To Add Files

“Update Application” (as above) and cycle through the screens to get to where you need to update information or add files and continue through to submit. That will update your application.

DRAFT