2022 NCEM State & Local Cybersecurity Grant Program (SLCGP) Application

To submit this application, rename the file to this format: [county/agency] "2022 SLCGP Grant Application" and forward to slcgp@ncdps.gov.

Organization

Legal name:			
Street:			
City:		Zip Code:	
County:			
EIN:			
UEID:			
Organization Type:	◯ Local Government ◯ Tribe ◯ State Agency ◯ Community College		
Rural Community: (population < 50,000)	◯ Yes ◯ No		

Point of Contact

Name:		Title:	
Email:		Phone:	

Project Manager

Name:		Title:	
Email:		Phone:	

Financial Officer

Name:		Title:	
Email:		Phone:	

Authorizing Official

Name:		Title:	
Email:		Phone:	

Project Information

Title:

Purpose:

Project Objective:
(select one)

- ◯ 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.
- ◯ Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
- ◯ Implement security protections commensurate with risk.
- ◯ Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

Required Elements Addressed:
(check all that apply)

- ☐ Manage, monitor, and track information systems, applications, and user accounts.
- ☐ Monitor, audit, and track network traffic and activity.
- ☐ Enhance the preparation, response, and resilience of information systems, applications, and user accounts.
- ☐ Implement a process of continuous cybersecurity vulnerability aassessments and threat mitigation practices prioritized by risk.
- ☐ Adopt and use best practices and methodologies to enhance cybersecurity.
- ☐ Transition to a .gov internet domain.
- ☐ Ensure continuity of operations including by conducting exercises.
- ☐ Identify and mitigate any gaps in the cybersecurity workforces, enhance recruitment and retention errors, and bolster the knowledge, skills, and abilities of personnel (reference to NICE Workforce Framework for Cybersecurity)
- ☐ Ensure continuity of communications and data networks in the event of an incident involving communications or data networks
- ☐ Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats.
- ☐ Enhance capabilities to share cyber threat indicators and related information between the eligible entity and the Department
- ☐ Leverage cybersecurity services offered by the Department
- ☐ Implement an information technology and operational technology modernization cybersecurity review process
- ☐ Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats
- ☐ Ensure rural communities have adequate access to, and participation in, plan activities
- ☐ Distribute funds, items, services, capabilities, or activities

Project Requires an Environmental Planning & Historic Preservation (EHP) Assessment :

◯ Yes ◯ No

Project and Budget Narrative

Project Narrative

Investment Strategy

Collaboration

Budget Narrative

Milestone timeline for individual activities

2023	2024	2025	2026

Impact/Outcomes

Planning/Organization/Training/Exercises Costs

Expenditure Area	Description	Total Cost

Equipment Costs

Qty	AEL #	Description	Total Cost

Funding Summary

Expenditure Area	Total Cost
Planning	0.00
Organization	0.00
Equipment	0.00
Training	0.00
Exercises	0.00
Total	**0.00**

Additional Information

Acknowledge the following statements (check all eight, or application will be considered incomplete):

- ☐ This application includes complete and accurate information.
- ☐ Any project having the potential to impact the environment, historic or cultural resources must submit an Environmental Planning & Historic Preservation (EHP) form.
- ☐ 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.
- ☐ Receiving SLCGP funding requires annual Nationwide Cybersecurity Review (no cost) and signing-up for required cyber hygiene services as specified in the SLCGP NOFO .
- ☐ Projects with funds allocated for equipment are required to check all equipment purchases against the FEMA Authorized Equipment List.
- ☐ Submission of the project proposal does not guarantee funding.
- ☐ Entities must be able to sustain capabilities once SLCGP funds are no longer available.
- ☐ 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 287, 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).

Sensitive Information (certify this statement only if applicable):

☐ Check this box if this application includes or contains "security features of electronic data processing systems, information technology systems, telecommunications networks, or electronic security systems, including hardware or software security, passwords, or security standards, procedures, processes, configurations, software, and codes" that you certify is not subject to public release per N.C.G.S. 132-6.1(c).

If you check this box, it is recommended that you submit this application via encrypted email and/or password protect this PDF file before submitting it (send file and password in separate emails). Consult your IT professionals for guidance on email encryption and/or password protection if needed.