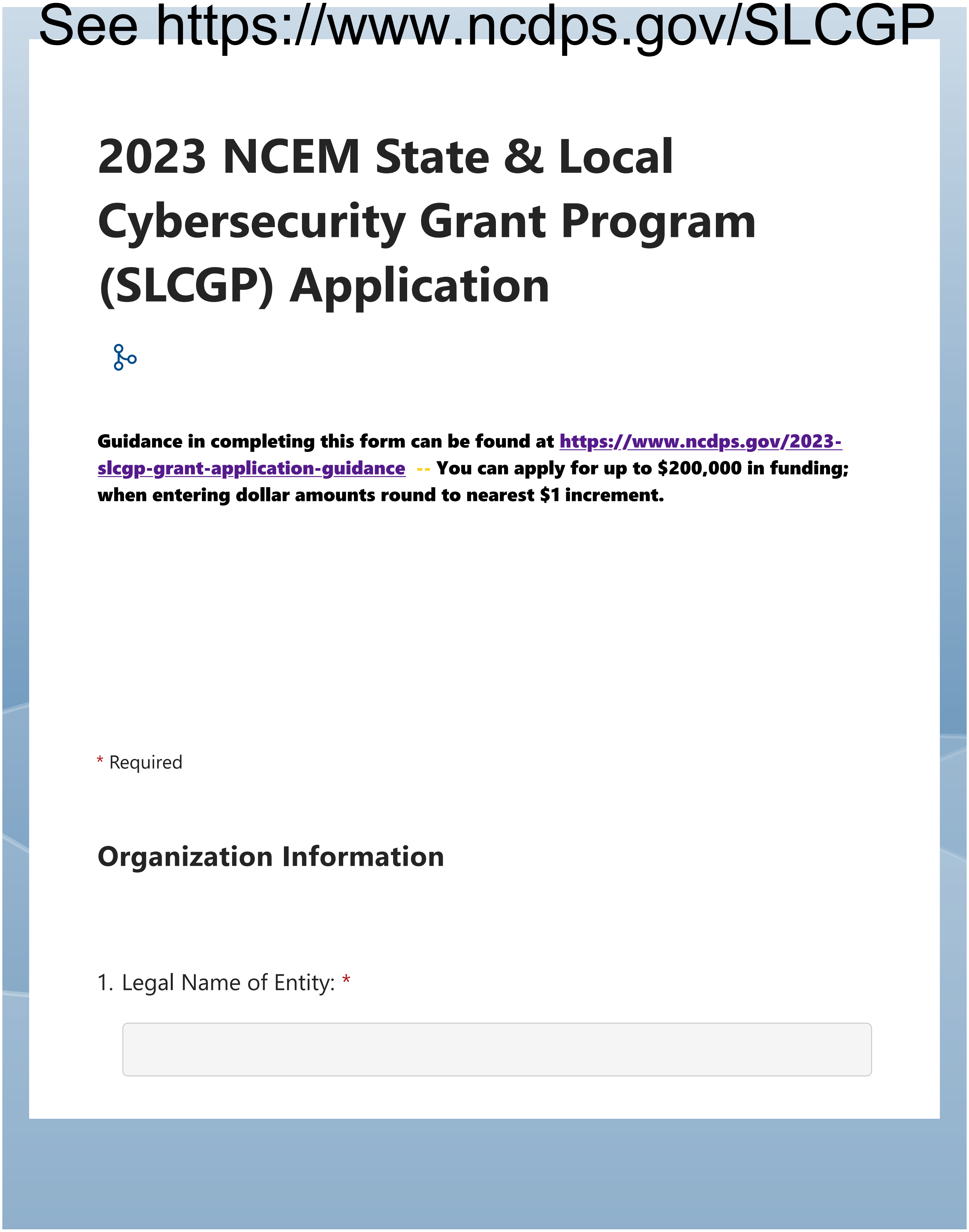
For Informational Purposes Only
See https://www.ncdps.gov/SLCGP



2023 NCEM State & Local Cybersecurity Grant Program (SLCGP) Application

Guidance in completing this form can be found at https://www.ncdps.gov/2023-slcgp-grant-application-guidance -- You can apply for up to $200,000 in funding; when entering dollar amounts round to nearest $1 increment.

* Required

Organization Information

1. Legal Name of Entity: *

2. Street Address: *

3. City: *

4. ZIP Code: *

The value must be a number

5. County: *

6. Employer Identification Number (EIN) *

7. Unique Entity ID (UEID): *

8. Organization Type: *

○ State Agency

○ Local Government *(refer to guidance doc for definition)*

○ Tribe

○ Community College *(refer to guidance doc for definition)*

○ Local School Administrative Unit *(refer to guidance doc for definition)*

9. Rural Community: *

See guidance document for definition

○ Yes

○ No

10. County Distress Tier: *

See Guidance Document

○ Tier 1

○ Tier 2

○ Tier 3

Point of Contact

11. Name: *

12. Job Title: *

13. Email: *

14. Phone Number: *

Please enter in format XXX-XXX-XXXX

Project Manager

15. Name: *

16. Job Title: *

17. Email: *

18. Phone Number: *

Please enter in format XXX-XXX-XXXX

Financial Officer

19. Name: *

20. Job Title: *

21. Email: *

22. Phone Number: *

Please enter in format XXX-XXX-XXXX

Project Information

23. Short Title: *

24. Purpose: *

25. Project Objective *

Select One

○ 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

CISA Cybersecurity Plans Elements

*Indicate at least ONE of the CISA Cybersecurity Plans Elements below that are applicable to your project, **you may also select any others that apply to your project**.*

26. Required Elements Addressed: *

□ 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 dot-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 and Budget Narrative

27. Project Narrative *

28. Investment Strategy *

29. Collaboration

30. Budget Narrative *

Milestone timeline for individual activities

Refer to https://www.ncdps.gov/2023-slcgp-grant-application-guidance

31. 2024 *

32. 2025

33. 2026

34. 2027

35. Impact / Outcomes *

PROJECT BUDGET
Planning / Organization / Exercise / Training / Costs (POETE)

See https://www.fema.gov/sites/default/files/2020-04/CPG201Final20180525.pdf, pages 30-44, for more info about Expenditure Areas (THIRA & SPR 3rd Ed)

36. Planning Expenditure

37. Planning Expenditure Total $

The value must be a number

38. Organization Expenditure

39. Organization Expenditure Total $

The value must be a number

40. Exercises Expenditure

41. Exercises Expenditure Total $

The value must be a number

42. Training Expenditure

43. Training Expenditure Total $

The value must be a number

Equipment Costs

See guidance document

44. Quantity

The value must be a number

45. AEL Number

46. Equipment Description

47. Quantity

The value must be a number

48. AEL Number

49. Equipment Description

50. Quantity

The value must be a number

51. AEL Number

52. Equipment Description

53. Planning Expenditure Description

54. Planning Expenditure Total Cost

Total entered as amount in USD $

The value must be a number

55. Organization Expenditure Description

56. Organization Expenditure Total Cost

Total entered as amount in USD $

The value must be a number

57. Equipment Expenditure Description

58. Equipment Expenditure Total Cost

Total entered as amount in USD $

The value must be a number

59. Training Expenditure Description

60. Training Expenditure Total Cost

Total entered as amount in USD $

The value must be a number

61. Exercises Expenditure Description

62. Exercises Expenditure Total Cost

Total entered as amount in USD $

The value must be a number

63. Total Combined Cost *

The value must be a number

Your Organization's Current Cyber Posture

64. Does your organization have a written security policy that employees must consent to annually? *

○ Yes

○ No

65. Do all employees receive annual cybersecurity awareness training? *

○ Yes

○ No

66. Does your organization have antivirus software on all workstations? *

○ Yes

○ No

67. If you have antivirus software on all workstations, please list your AV solutions:

68. Does your organization have antivirus software on all servers? *

○ Yes

○ No

69. If you have antivirus software on all servers, please list your AV solutions:

70. Does your organization have a firewall? *

○ Yes

○ No

71. If so, please list your firewall solution(s).

72. Does your organization utilize a centralized patch management solution? *

○ Yes

○ No

73. Is your organization’s data regularly backed up via a non-domain joined solution (external media, cloud solution, etc) *

○ Yes

○ No

74. Is your organization using intrusion detection/prevention solutions to stop external attacks? *

○ Yes

○ No

75. If so, please list the solution(s) being used.

76. Are user accounts and permissions actively monitored and routinely audited? *

○ Yes

○ No

77. Is your organization using any centralized logging solution? *

○ Yes

○ No

78. If so, please list the solution(s) being used.

79. Does your organization require multi-factor authentication for e-mail account access? *

○ Yes

○ No

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

○ Yes

○ No

81. Does your organization require multi-factor authentication for VPN access? *

○ Yes

○ No

Additional Information

If you would like to submit additional information (such as a more lengthy response to free text questions, or a more detailed listing of anything) or have questions concerning this application, please email SLCGP@NCDPS.gov for further instructions.

ATTESTATIONS

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

82. I certify the following answers are all true and correct to the best of my knowledge: *

□ 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)

You can apply for up to $200,000 in funding; when entering dollar amounts round to nearest $1 increment.

This content is neither created nor endorsed by Microsoft. The data you submit will be sent to the form owner.

Microsoft Forms