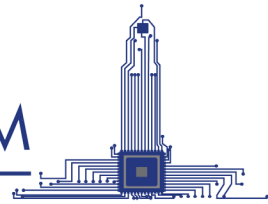


STATE AND LOCAL CYBERSECURITY GRANT PROGRAM



Subrecipient Application Form

By submitting this Subrecipient Application Form, you acknowledge and agree to the requirements of the 30% cost share as established under the State and Local Cybersecurity Grant Program (SLCGP). Information regarding cost share requirements and allowable sources can be found in the SLCGP guidelines and in the U.S. Department of Homeland Security (DHS) Notice of Funding Opportunity (NOFO).

Name:

Title:

Executive or Elected Official Sponsor:

Executive or Elected Official Sponsor Email:

Organization:

Address:

City:

State: NE

Zip Code:

Email Address:

Phone:

Organization's Tax ID#

Organization's UEI#

FIPS Code:

Have you completed the Center for Internet Security (CIS) Nationwide Cybersecurity Review (NCSR) for the current year? Yes No

Have you registered for CISA Services (e.g., Cyber Hygiene (CyHy), Cyber Resilience Review (CRR))? Yes No

Project Name:

Project Alignment with FY Objectives:

(see FY24 SLCGP NOFO)

#1 Governance and Planning

#2 Assessment and Evaluation

#3 Mitigation

#4 Workforce Development

Project Start Date:

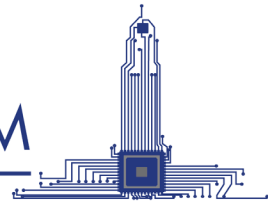
Project End Date:

Is this project to build a new or sustain an existing cybersecurity capability? (Build, Sustain)

Project Management: (Initiate, Execute, Control, Close Out)

Project Location (Zip Code):

STATE AND LOCAL CYBERSECURITY GRANT PROGRAM



Subrecipient Application Form

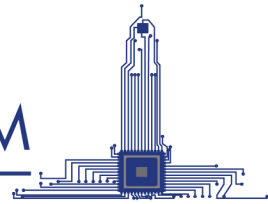
Statewide Plan and NOFO Alignment (which of these elements does your project align with - check all that apply)

- ☐ Manage, monitor, and track information systems, applications, and user accounts
- ☐ Monitor, audit, and track network traffic, activities to and from systems, applications, and user accounts
- ☐ Enhance preparation, response, and resilience of systems, applications, and user accounts
- ☐ Implement a process of continuous cybersecurity vulnerability assessment and threat mitigation
- ☐ Adopt and use best practices and methodologies to enhance cybersecurity
- ☐ Promote the delivery of safe, recognizable, and trustworthy online services through .gov sites
- ☐ Ensure continuity of operations in the event of a cybersecurity incident
- ☐ Use the NICE Framework to identify and mitigate any cybersecurity workforce gaps
- ☐ Ensure continuity of communication and data networks in the event of an incident
- ☐ Assess and mitigate cybersecurity risk and cybersecurity threats to critical infrastructure and key resources
- ☐ Enhance capabilities to share cyber threat indicators and related information
- ☐ Leverage cybersecurity services offered by CISA
- ☐ Implement an information technology and operational technology modernization cybersecurity review process
- ☐ Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats
- ☐ Ensure adequate access to, and participation in, the services and programs by rural communities
- ☐ Distribute funds, items, services, capabilities, or activities to local governments

Provide a baseline understanding of the existing cybersecurity gaps, risks, and threats that the applicant entity faces which have influenced the development of this application. Also, please include the summary of the current capabilities within the applicant jurisdiction to address these threats and risks

Describe how this application and the associated project addresses gaps and/or sustainment in the approved State Cybersecurity Plan

STATE AND LOCAL CYBERSECURITY GRANT PROGRAM



Subrecipient Application Form

Stakeholder 1
Organization:

How will this project benefit this organization:

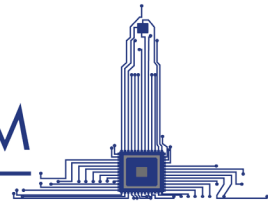
Project Scope:

Project Description:

Project Goals:

Total Dollar Amount Allocation:

STATE AND LOCAL CYBERSECURITY GRANT PROGRAM



Subrecipient Application Form

Planning money allocation (How much of the funds are going to cybersecurity planning activities)?

\$

Organization money allocation (How much of the funds are going to cybersecurity organization activities)?

\$

Equipment money allocation (How much of the funds are going to cybersecurity equipment cost)?

\$

Training money allocation (How much of the funds are going to cybersecurity training cost)?

\$

Exercise money allocation (How much of the funds are going to cybersecurity exercise cost)?

\$

Total Project Amount - \$ _____

Total Project Amount including 30% Cost Share - _____

How will the 30 % Cost Share be met (Hard or Soft match), pages 17-18 of NOFO?

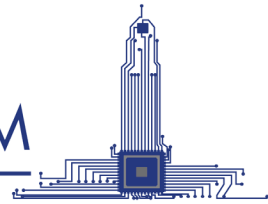
Please explain:

How much is going to Local Government (as defined by the NOFO)?

How much is going to Rural Communities (less than 50,000 population)?

Project Risks and Challenges:

STATE AND LOCAL CYBERSECURITY GRANT PROGRAM



Subrecipient Application Form

Specific Project Metric:

- *Example (Specific, Measurable, Time-bound, Aligned with SLCGP priorities):*
 - *Vulnerability Management:*
 - *Reduce the number of known, unpatched critical vulnerabilities in State and Local government information systems by 40% within 12 months, as measured by monthly vulnerability scans and remediation reports compared to the established baseline.*

Specific Project Milestones (up to 3 per project):

- *Example (Specific, Measurable, Achievable, Time-bound):*
 - *Vulnerability Management:*
 - *Description: Implement enhanced vulnerability management practices, including regular scanning, patch deployment, and remediation tracking.*
 - *Target Completion Date: 12 months*
 - *Performance Measure/Outcome: Achieve a 40% reduction in active vulnerabilities across covered systems compared to baseline assessments.*

Sustainability:

- *Please describe how the project and initiative will be sustained at the end of the grant funds*

Have these cybersecurity capabilities been included in future budgetary spending? Yes No

Does the Project support a previously awarded investment? Yes No

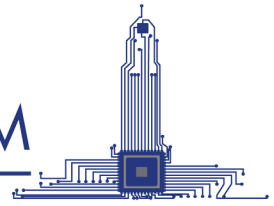
What Year? 2022 2023

Name of Chief Elected or Executive Official

Signature of Chief Elected or Executive Official

Date Signed:

STATE AND LOCAL CYBERSECURITY GRANT PROGRAM



Subrecipient Application Form