State and Local Cybersecurity Grant Program Application

Organizational Overview

Organizational Information

Name of Applicant Organization (as shown in WVOASIS):

Physical Address (as shown in WVOASIS):

Federal Employer Identification Number (FEIN):

Unique Entity Identifier (UEI, this must be obtained before federal funds can be awarded):

WVOASIS Number:

Organization Type:

□ County
□ Elections
□ Emergency Management
□ Higher Education
□ Municipality
□ Public Education
□ 911 Center
□ Public Health
□ State agency

In a Rural County as per Grant Funding Definition (50,000 or less population in county)?

Estimated number of citizens served by the organization:

Full-Time employees of the organization:

Total Annual Budget for Organization/Government Unit:

Does the organization operate a water utility or sewer utility? Check the box for each utility organization operates: □Water Utility □Sewer Utility

Technical and Cybersecurity Posture Details

Allocated Technology Budget for Organization:

Full-Time, Dedicated IT Employees:

Part-Time, Dedicated IT Employees:

Are IT Services managed by Vendor/Contractor or In-House?

Network Infrastructure Owned or Leased?

Total Number of –

Workstations: Laptops:

Physical Servers: Virtual Servers:

Has this organization completed a cybersecurity assessment?

If not, when is your assessment scheduled:

Who will be conducting the assessment:

Does your organization have written security policies that all employees must consent to and abide by?

Does the organization currently have Cybersecurity Insurance?

Project Contact Information

Project Manager

Name and Title:

Email:

Telephone:

Address (if different from the organization):

Fiscal Officer

Name and Title:

Email:

Telephone:

Address (if different from the organization):

Project Details

Project Title:

Project Description:

Required Elements Addressed

(All projects must address at least one element, but can address multiple items)

□ 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 assessments and threat mitigation practices prioritized by risk.

□ Adopt and use best practices and methodologies to enhance cybersecurity.

□ Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including using the .gov internet domain.

□ Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.

□ Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by National Institute of Science and Technology (NIST) to identify and mitigate any gaps in the cybersecurity workforces.

□ Ensure continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.

□ Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources.

□ Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.

□ Leverage cybersecurity services offered by CISA and other official sources.

□ Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.

□ 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 to local governments.

Project Significance

Explain how this project enhances cybersecurity and why it covers the most significant risk(s) to mitigate for your organization:

Implementation Plan

Does this project support a previously awarded investment through SLCGP?

When do you anticipate the authorization for the project work to be obtained?

During what timeframe do you anticipate the actual project to be executed?

Please enter the three major milestones anticipated for the project below:

MILESTONE 1

MILESTONE 2

MILESTONE 3

Sustainability

Would the organization have the funding to implement the necessary cybersecurity protection measures without the use of the SLCGP funding?

How will the organization continue to pay for any goods and services acquired using the grant funding after the award is closed?

Has the organization adopted a plan to ensure future improvements in cybersecurity?

Budgetary Breakdown

Item	Qty.	Unit Price	Total	AEL#
			$ 0.00	
			$ 0.00	
			$ 0.00	
			$ 0.00	
			$ 0.00	
			$ 0.00	
			$ 0.00	
			$ 0.00	
			$ 0.00	
			$ 0.00	
			$ 0.00	
			$ 0.00	
			$ 0.00	
			$ 0.00	
			$ 0.00	
			$ 0.00	
			$ 0.00	
			$ 0.00	
			$ 0.00	
			$ 0.00	
			$ 0.00	
			$ 0.00	
			$ 0.00	
			$ 0.00	
			$ 0.00	
			$ 0.00	
			$ 0.00	
			$ 0.00	

GRAND TOTAL: $ 0.00

Do any of the listed items require installation (i.e. server rack bolted to floor or secured to wall)?

(If a project requires permanent installation, or the disturbance of walls, floors, etc., there will be additional information needed for FEMA before the project can move forward, so timely reporting of such instances will speed up the funding process, if selected.)

Describe the procurement method used to select the goods and services needed for this project:

Are these procurement methods documented and consistent with the requirements of State and Local laws and regulations?

Was the procurement method used adequate to comply with the requirements for full and open competition as per 2 CFR § 200.319?

Additional Requirements Under SLCGP

If funded, all sub-recipients are required to participate in a limited number of free services from CISA.

Cyber Hygiene Services

Vulnerability Scanning evaluates external network presence by executing continuous scans of public, static Internet Protocols for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts.

To register for this service, email vulnerability@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services – SLCGP" to get started. Indicate in the body of your email that you are requesting this service as part of the SLCGP. For more information, visit CISA's Cyber Hygiene Information Page.

Nationwide Cybersecurity Review (NCSR)

The NCSR is a free, anonymous, annual self-assessment designed to measure gaps and capabilities of a SLT's cybersecurity programs. It is based on the NIST Cybersecurity Framework and is sponsored by DHS and the MS-ISAC.

Eligible entities and their subrecipients are required to complete the NCSR, administered by the MS-ISAC, during the first year of the award/subaward period of performance and annually.

For more information, visit Nationwide Cybersecurity Review (cisecurity.org).

Membership in the Multi-State Information Sharing and Analysis Center (MS-ISAC)

The MS-ISAC receives support from and has been designated by DHS as the cybersecurity ISAC for SLT governments. The MS-ISAC provides services and information sharing that significantly enhances SLT governments' ability to prevent, protect against, respond to, and recover from cyberattacks and compromises. DHS maintains operational-level coordination with the MS- ISAC through the presence of MS-ISAC analysts in CISA Central to coordinate directly with its own 24x7 operations center that connects with SLT government stakeholders on cybersecurity threats and incidents. To register, please visit https://learn.cisecurity.org/ms-isac-registration. For more information, visit MS-ISAC (cisecurity.org).

Conditions and Assurances

The following bullets outline the federal and state requirements that any recipient of this fundings must comply, as appropriate, if they are selected to receive an award:

- □ The applicant has the legal authority to apply for the grant.
- □ The applicant/recipient will comply with all federal civil rights laws, including Title VI of the Civil Rights Act, as amended.
- □ The applicant/recipient may expend the grant funds only for the purposes and activities covered by the approved project description and budget. The applicant/recipient must obtain written approval for a project change.
- □ The applicant/recipient will comply with Title 2 Part 200 of the Code of Federal Regulations (2 CFR 200).
- □ If an audit is conducted, the applicant/recipient must submit a copy of the audit report to the state and to the Federal Audit Clearinghouse.
- □ The applicant/recipient must provide access to, and provide the right to examine all records, books, papers, documents, equipment, training, and/or exercises related to the sub-grant, and to relevant records of contractors.
- □ No official or employee or the applicant/recipient who performs any duties under the grant project may participate in an administrative decision with respect to the project if such a decision can be expected to result in any private/public benefit to the individual or individual's immediate family.
- □ Funds which the applicant/recipient supplies as match to the award must comply with the same grant requirements and expenditure guidelines as the federal funds.
- □ The applicant/recipient will submit all reports deemed reasonably necessary for monitoring, stewardship, and evaluation of programmatic and fiscal responsibilities.
- □ The applicant/recipient shall administer a system to control, protect, preserve, use, maintain, and dispose of any equipment acquired through the grant.

Please check the above boxes to indicate that you can comply with these requirements.

The official Conditions and Assurances for the SLCGP will be signed upon the issuance of an award.

Required Attachment Checklist

1. Mini-Risk Assessment
2. All Quotes acquired through the procurement process (at least two are necessary)
3. IT Strategy/Cybersecurity Plan documents (if applicable)
4. Other Assessment Summaries, if applicable (e.g. Water and Sewer Annual Risk Assessment)
5. Other supporting documents, as needed