State and Local Cybersecurity Grant Program

Information Session

10:00 AM - 11:00 AM

9/13/2024

Contents

- Housekeeping
- Background & Overview
- Applicant Eligibility Criteria
- Funding and Period of Performance
- Strategic Priorities
- Application Informational Guides
- Application Documents & Submission
- Grading Considerations
- Reporting Requirements
- General Requirements
- Questions

Housekeeping

- Please remain on mute until the Q&A section at the end of the presentation.
- Questions may be typed into the chat.
- Attendees can request a copy of this presentation by emailing slcgp.grant@maryland.gov and cc: taylor.munir@maryland.gov.

Background

The State and Local Cybersecurity Grant Program (SLCGP) is a federally funded grant program that is administered by the each US State.

The goal of the State and Local Cybersecurity Grant Program (SLCGP) is to help states, local governments, rural areas, and territories address cybersecurity risks and cybersecurity threats to information systems. The program enables DHS to make targeted cybersecurity investments in state, local, and territorial government agencies, thus improving the security of critical infrastructure and resilience of the services that state, local, and territorial governments provide to their communities.

Overview

The SLCGP funds granted to the State of Maryland will be distributed by the Maryland State and Local Cybersecurity Grant Program Planning Committee (“the Committee"). The Committee has developed a reimbursable Sub-grant program where eligible entities can apply for funding for their own projects. Funds will be granted to those who demonstrate the ability to put forward the most competitive projects, in alignment with the project application, and maintain federal and state grant compliance.

Application Eligibility Criteria

The eligible applicants are Maryland “Local governments” which include:

- A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments, regional or interstate government entity, or agency or instrumentality of a local government; or
- Rural as defined by FEMA which is, a rural community, unincorporated town or village, or other public entity. Per the Homeland Security Act of 2002, a “rural area” is defined in 49 U.S.C. § 5302 as an area encompassing a population of less than 50,000 people that has not been designated in the most recent decennial census as an “urbanized area” by the Secretary of Commerce.*
- Rural as classified by the Committee which is, any Maryland “Local Government” that can provide adequate evidence of their rural status such as a planning and zoning designation or mapping. Evidence should be submitted with the application package.*

*Rural jurisdictions have been given priority for funding

Funding and Period of Performance

- $6,514,533 granted to Maryland
- Grant is based on reimbursable funding

Event	Date(s)
Application Released	September 3rd, 2024
Information Session	September 13th, 2024
Applications Due	October 3rd, 2024 @ 11:59 PM EST
Review Process	October 2024
Awards Announced	November 2024
FEMA Review's Projects	November 2024
Period of Performance	~December 2024 - 30 September 2027

Strategic Priorities

The “Committee” has identified 5 investment priorities (referred to as project categories) for Maryland. Your proposed project and project budget should align with at least one of these project categories.

Project Category 1 (PC1): Adoption or enhancement of priority cybersecurity best practices

These priorities were developed by the State of Maryland, and are as follows:

1. Asset Discovery & Vulnerability Management
2. Multi-Factor Authentication (MFA)
3. End-Point Detection & Response (EDR)
4. Email Security (Secure Email Gateway (SEG)
5. Security Awareness Training

Strategic Priorities

The “Committee” has identified 5 investment priorities (referred to as project categories) for Maryland. Your proposed project and project budget should align with at least one of these project categories.

Project Category (PC2): Adoption or enhancement of general cybersecurity best practices

These priorities were developed by CISA, and are as follows:

1. Enhanced Logging
2. Data Encryption
3. End-of-use processes of software & hardware
4. Ability to Reconstitute back-ups
5. Migration to .gov domain
6. Implement the NIST CSF Framework
7. Implement the NIST cyber supply chain risk management practices
8. Making use of knowledge bases of adversary tools and tactics

Strategic Priorities

The “Committee” has identified 5 investment priorities (referred to as project categories) for Maryland. Your proposed project and project budget should align with at least one of these project categories.

Project Category 3 (PC3): Cybersecurity policy and governance - Jurisdictions may seek funding to support the development of cybersecurity policies and governance.

Examples include, but are not limited to: cyber incident response plans; acceptable use policies; continuity of operations plans; technology modernization processes; risk and/or threat assessments.

Strategic Priorities

The “Committee” has identified 5 investment priorities (referred to as project categories) for Maryland. Your proposed project and project budget should align with at least one of these project categories.

Project Category (PC4): Addressing specific jurisdictional cybersecurity needs - Recognizing that some jurisdictions may have specific or unique cybersecurity needs, jurisdictions may propose projects to address those needs. For example: addressing gaps in cybersecurity critical infrastructure specific to your entity/jurisdiction.

Project Category 5 (PC5): Cybersecurity workforce development - Jurisdictions may seek funding to support workforce recruitment and development needs using the NICE Cybersecurity Workforce Framework.

Supplanting vs. Supplementing

- “Supplement” means to add to; “supplant” means to replace. Therefore, federal regulations strictly prohibit supplanting as federal funds cannot replace state, local, or agency funds.
- I.e. using federal funds in the place of already budgeted or local or state funds.
- For example, if you have an MDR solution that you now have general funds allocated towards, you cannot use grant funds instead for the same solution.
- If however, by switching to the grant solution, you enhance a capability, or add value to the product/ project, that is supplementing

Application Informational Guides

Review the following documents prior to filling out your application documents:

- Maryland FFY2023 SLCGP Funding Guide
- Maryland FFY2023 SLCGP Project Application & Budget Narrative Instruction Manual
- Maryland FFY2023 SLCGP FAQs

These guides provide a detailed list of the required elements that must be included in your project proposal and other application documents.

Application Documents & Submission

ALL Applicants Must Submit:

- Maryland FFY2023 SLCGP Subgrant Project Proposal Application
- Maryland SLCGP FFY2023 Additional Application Documents Packet
  - Budget Narrative and Justification
  - Appendix A: Cybersecurity Capabilities Assessment
  - Appendix E: Measurable Milestones

SOME Applicants Must Submit:

- Form W-9 (Required for Health Departments & Municipalities Only)
- Itemized Quote for Vendor or Contract Services (Required for Projects Including Vendor or Contract Services)
- Maryland Rural Classification Evidence (Required for an applicant requesting prioritized funding under the Maryland Rural Classification Eligibility Criteria)

Maryland FFY2023 SLCGP Subgrant Project Proposal Application

- General Project Information (Project Name, Amount requested, POC(s)
- Associated Project Category(s)
- Certifications (Prevention of Duplication of Efforts, Federal Award Funds Requirements, Fiscal Responsibility)
- Rural Jurisdiction Alignment Information (if applicable)
- Proposal Elements
  - Narrative
  - Project Deliverables
  - Project Metrics
  - Project Sustainment Plan

Maryland FFY2023 SLCGP Subgrant Project Proposal Application - Proposal Narrative

- Roles & Responsibilities of Project POCs
  - General Management
  - Financial Tracking and Reporting
- Geographic scope for project
- Alignment with Appendix A: Cybersecurity Capabilities Assessment
- Description of the involvement of relative partners, stakeholders, staff, contractors, etc.
- Impacts of the project on the public (if applicable)
- Connection between the proposed project and the Maryland Project Categories
- Are you enhancing or replacing an existing cybersecurity control? If yes, why?
- Incorporation of Equity, Inclusion, and Accessibility (if applicable) - more information is provided in the Funding Guide, page 12

Maryland FFY2023 SLCGP Subgrant Project Proposal Application - Proposal Deliverables & Metrics

Project Deliverables

- Anticipated outcomes after the period of performance
- Strategies for meeting project deliverables, including evidence from past performance on a similar project

Project Metrics (complete with Appendix E: Measurable Milestones)

- Identify the following:
  - How will you monitor the completion of project milestones and objectives?
  - How many people will benefit from the project?
  - How will you monitor how much of the allocated budget has been used and how much remains?
- SMART (Specific, Measurable, Achievable, Realistic, Time-Bound)

Maryland FFY2023 SLCGP Subgrant Project Proposal Application - Proposal Sustainment Plan

Project Sustainment Plan

- How will you sustain the project after the period of performance ends?

Maryland FFY2023 SLCGP Additional Application Documents Packet - Budget Narrative & Justification

Detailed instructions can be found in the “Project Applications & Budget Narrative Instruction Manual”.

Budget Dashboard

- POC(s) for financial tracking and reporting, general information, budget period of performance key dates

Federal

- Federal Budget Justification - Cost for personnel, fringe benefits, travel, contractual, and other expenses.
- Federal Budget Summary - **DO NOT FILL**

POETE

- POETE Budget Justification - Cost for planning, organization, equipment, training, and exercises.
- POETE Budget Summary - **DO NOT FILL**

Maryland FFY2023 SLCGP Additional Application Documents Packet - Appendix A & E

Appendix A: Cybersecurity Capabilities Assessment

- Detailed instructions can be found in the “Funding Guide”
- Evaluation of cybersecurity strengths and weaknesses
- Link results to project justification

Appendix E: Measurable Milestones

- Detailed instructions can be found in the “Project Applications & Budget Narrative Instruction Manual”.
- Tie Project Deliverables to key dates and checkpoints

Application Documents & Submission

Email completed forms to slcgp.grant@maryland.gov. Subject Line must be in this format: FY[funding year] SLCGP - [Sub-recipient Name] [Project Title] Application Forms

Example: FY[23] SLCGP - [MDEM]- [SLCGP Project] Application Forms

Step by Step Application Process can be found on the Maryland Department of Emergency Management, Cyber Preparedness Unit Webpage.

Grading Considerations

Because this is a competitive grant program, the committee has implemented a weighting system that ranks rural jurisdictions' applications highest by multiplying their final application score by:

- FEMA Rural Definition x 1.5
- Maryland Rural Classification x 1.4

The same practice will be applied to the project categories at the rates described below:

- Category 1 (Maryland's Priority Best Practices) x 1.3
- Category 2 (General Best Practices) x 1.1
- Category 3 (Cyber Security Governance) x 1
- Category 4 (Addressing specific needs) x 1
- Category 5 (Workforce development) x 1

Reporting Requirements

Subrecipient Quarterly Status Reports (QSRs) -The pass-through entity (MDEM) will provide a template for the subrecipients to utilize and will allow subrecipients to report on:

- Expenditures and Obligations
- Brief narrative of overall project(s) status;
- Summary of project expenditures;
- Description of any potential issues that may affect project completion; and
- Data collected for any additional Committee performance measure requirements.

Closeout Reporting - Subrecipients must utilize the final QSR to:

- Provide a final progress report detailing all accomplishments, including a narrative summary of the impact of those accomplishments throughout the period of performance; and
- Other documents as required by the Committee, or the pass-through entity (MDEM).

General Requirements

- Applicants must participate in or adhere to CISA Cyber Hygiene Services
  - Web Application Scanning is an “internet scanning-as-a-service.” This service assesses the “health” of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and government best practices and standards.
  - Vulnerability Scanning evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts.
- Must complete the Nationwide Cybersecurity Review (NCSR) annually

Questions & Next Steps

- Please unmute or raise your hand if you have questions.
- This presentation will be posted to the website.

Website link for Application Documents and More Information

Thank you!

For questions on today's presentation, please reach out to:

SLCGP Grant Administrator

slcgp.grant@maryland.gov

Taylor Munir

Taylor.munir@maryland.gov