Maryland FFY2022 SLCGP Project Applications & Budget Narrative Instruction Manual[1]

TABLE OF CONTENTS

GENERAL INFORMATION

I. **SLCGP Manual 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"). Awards will go to the best applicants to bring them to baseline cybersecurity capabilities level or help them achieve advanced capabilities.

The Maryland Cyber Planning Committee has developed two programs to distribute the funds:

1. A reimbursable Sub-grant program where eligible entities can apply for funding for their projects.
2. A shared services Information Security Officer (ISO) program managed by the Department of Information Technology's Office of Security Management.

---

[1] Applicants are encouraged to review State and Local Cyber Grant Program

Maryland
DEPARTMENT OF
EMERGENCY MANAGEMENT

Russell J. Strickland | Secretary

Maryland
DEPARTMENT OF
INFORMATION TECHNOLOGY

Katie Savage | Secretary

Wes Moore | Governor
Aruna Miller | Lt. Governor

State and Local
Cybersecurity Grant Program

This Manual provides instructions for both the Sub-grant and ISO Program application. Please find the corresponding sections below for both programs.

II. Goals and Objectives

CISA developed a series of overarching goals and objectives for the SLCGP based on input from state, local, and territorial stakeholders, and consideration of national priorities, frameworks, and the national cyber threat environment:

1. Implement cyber governance and planning;
2. Assess and evaluate systems and capabilities;
3. Mitigate prioritized issues; and
4. Build a cybersecurity workforce

Using these goals & objectives as guidance, The Committee has determined project categories that will bring Maryland to baseline cybersecurity capabilities level or help the state achieve advanced capabilities. The Committee has also established a relationship with Maryland's Department of Information Technology to develop a shared services program that satisfies a priority of the grant program.

Maryland DEPARTMENT OF EMERGENCY MANAGEMENT

Russell J. Strickland | Secretary

Maryland DEPARTMENT OF INFORMATION TECHNOLOGY

Katie Savage | Secretary

Wes Moore | Governor

Aruna Miller | Lt. Governor

State and Local
Cybersecurity Grant Program

SLCGP SUBGRANT PROGRAM PROJECT PROPOSAL TEMPLATE INSTRUCTIONS

Follow the instructions below on how to complete the SLCGP Project Proposal Application that must be submitted as part of the application for funding. It is the responsibility of the applicant to ensure that the application package has been received in its entirety. Incomplete applications will be considered ineligible for review by the Committee. Applicants are eligible to apply for both the sub-grant program and the shared services program.

Project Title:

Include a title for the proposed project so that the Committee will have a brief, clear understanding of what will be supported under this project.

- For Example: Purchase and Implementation of MFA Tokens Project for Quaker County

Funding Amount:

Indicate the total amount requested for the project. In addition to inserting the total funding amount in this section, the application also requires a completed detailed budget narrative and budget justification sheet. For more information on this requirement, see section "SLCGP Budget Narrative Template Instructions".

- Funding Request Example: $80,000.00

Requesting Jurisdiction:

The Jurisdiction must include County, city, and/or town being applied for and must report if the applicant is an institution of public health, or education if applicable

- **Example**: Baltimore County, 21234 (or) Harford County Local Health Department, 21014

Information Technology/Operational Technology Question:

For the purpose of this application, operational technology is defined as "hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events."

Maryland
DEPARTMENT OF EMERGENCY MANAGEMENT

Russell J. Strickland | **Secretary**

Maryland
DEPARTMENT OF INFORMATION TECHNOLOGY

Katie Savage | **Secretary**

Wes Moore | **Governor**
Aruna Miller | **Lt. Governor**

State and Local
Cybersecurity Grant Program

Please answer the question regarding Operational Technology (OT)or Information Technology (IT) projects.

- Is the sub-grant application you are submitting for an Operational Technology (OT)or Information Technology (IT) project?

Start Month/Year and End Month/Year:

The period of performance as determined by the State Administrative Agency (SAA) is: **Please use 12/1/22-11/30/26.**

Contact Information

Please provide the contact information for the following individuals:

- Project Manager Name, Email and Telephone Information.
- Financial Contact Name, Email and Telephone Information. This individual is responsible for managing the project budget and ensuring that the grant expenditures will be tracked and segregated from other expenditures.
- Administrative Contact Name, Email and Telephone Information. This individual is responsible for completing and submitting programmatic and financial progress reports.
- Approving Authority (Project Sponsor) Contact, Email and Telephone Information (if a different individual from the Project Manager).

Please determine who will be the primary contact for application updates.

Associated Investment Justification(s):

Through the collaborative efforts of the Maryland State and Local Cybersecurity Grant Program Planning Committee ("the Committee") and the provided SLCGP NOFO issued by the U.S. Department of Homeland Security (DHS)/Federal Emergency Management Agency (FEMA)/Resilience/Grant Program Directorate (GPD), 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.

The Committee's identified project categories are as follows:
1. **Project Category 1 (PC1): Adoption or enhancement of priority cybersecurity best practices -** The Maryland Cybersecurity Planning

Maryland
DEPARTMENT OF
EMERGENCY MANAGEMENT

Russell J. Strickland | Secretary

Maryland
DEPARTMENT OF
INFORMATION TECHNOLOGY

Katie Savage | Secretary

State and Local
Cybersecurity Grant Program

Wes Moore | Governor
Aruna Miller | Lt. Governor

Committee has identified five baseline best practices that will significantly enhance the cybersecurity posture across the state. Due to the limited amount of funding available, jurisdictions are encouraged to propose projects that enable or enhance these five priority best practices.

These best practices are (1) Asset Discovery & Vulnerability Management; (2) Multi-Factor Authentication (MFA); (3) End-Point Detection and Response (EDR); (4) Email Security (such as Secure Email Gateway (SEG) solutions); and (5) Security Awareness Training.[2]

2. **Project Category (PC2): Adoption or enhancement of general cybersecurity best practices -** While not identified as Maryland's prioritized baseline cybersecurity best practices, jurisdictions can submit project proposals that support the adoption or enhancement of other general cybersecurity best practices.

   These best practices include, but are not limited to: Enhanced logging; data encryption; end-of-use processes of software and hardware; strong password management; ability to reconstitute systems (backups); migration to .gov domain; implementing the NIST Cybersecurity Framework; implementing NIST cyber supply chain risk management practices; and making use of knowledge bases of adversary tools and tactics.[3]

3. **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; and risk and threat assessments.

4. **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.

---

[2] For definitions of the best practices listed in Project Category 1 (PC1), please review the Maryland SLCGP Subapplication FAQs.
[3] For definitions of the best practices listed in Project Category 2 (PC2), please review the Maryland SLCGP Subapplication FAQs.

5. **Project Category 5 (PC5): Cybersecurity workforce development -** Jurisdictions may seek funding to support workforce recruitment and development needs using the NICE Cybersecurity Workforce Framework[4].

In this section, identify which Project Category aligns more closely with the proposed project. If there is also a secondary Project Category that the project aligns with, include that as well.

Associated Priorities:[5]

As stated in the" Associated Investment Justifications" section, due to the limited amount of funding available, jurisdictions are encouraged to propose projects that enable or enhance the Committee's identified priority best practices. The Committee has also identified general best practices that they encourage entities/jurisdictions to implement.

A. (Project Category 1) Priority best cyber security practices determined by the Committee as the most essential functions:
   1. Asset Discovery & Vulnerability Management
   2. End-Point Detection and Response (EDR)
   3. Multi-factor authentication (MFA)
   4. Email Gateway Security
   5. Security Awareness Training

B. (Project Category 2) General cybersecurity best practices which are described in the SLCGP plan as priorities, including but not limited to:
   1. Enhanced Logging
   2. Data Encryption
   3. End-of-use processes for software & hardware
   4. Prohibit the use of known/fixed/default passwords and credentials
   5. Ensure the ability to reconstitute systems (backups)

---

[4] For more information on the NICE Cybersecurity Framework view: https://niccs.cisa.gov/workforce-development/nice-framework
[5] Applicants are encouraged to review Section 10. C. PRIORITIES, of The Department of Homeland Security Notice of Funding Opportunity Fiscal Year 2022 State and Local Cybersecurity Grant Program Website title:FEMA
URL:https://www.fema.gov/fact-sheet/department-homeland-security-notice-funding-opportunity-fiscal-year-2022-state-and-local

Maryland
DEPARTMENT OF
EMERGENCY MANAGEMENT

Russell J. Strickland | Secretary

Maryland
DEPARTMENT OF
INFORMATION TECHNOLOGY

Katie Savage | Secretary

Wes Moore | Governor

Aruna Miller | Lt. Governor

State and Local
Cybersecurity Grant Program

6. Migration to the .gov domain

If the proposed project fulfills Maryland Project Category 1 or 2, please indicate which priorities your project will enable or enhance.

- For Example: Security Awareness Training

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 1.5.

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

SUB-GRANT APPLICATION REQUIREMENTS SECTION

I. Approving Local Authority

Please identify an approving local authority who is authorized by your entity to attest to the accuracy of the application submitted for the Maryland SLCGP subaward. This authority must also sign the mandatory Local Consent Form that must be submitted with this application.

Mandatory Forms Attestation & Required Certifications

1. **Mandatory Forms:** The following documents must be submitted as part of your proposal. Applications not submitted with this information will be considered incomplete and will not be reviewed by the Committee.

   By checking the box in this section for each document, the applicant is attesting that their application packet is submitted in its entirety.

2. **Availability of Additional Funding Sources & Duplication of Efforts Certifications:**

Please review and certify that the jurisdiction and/or governing body your entity belongs to does or does not have any funding opportunities or programs that would cover the needs of your project. If there is partial or complete funding available from another source, please explain why the grant funds would be needed to support the project on top of already available funds.

Please also certify that there is/are no other entities in their jurisdiction applying for funds to conduct that same project other than to intentionally enhance each other's projects. If there are other jurisdictions applying for funds to conduct that same project, please explain why the grant funds would be needed to support the project.

Compliance Requirements

Please review and certify the information in this section for your application:

- SAM: Compliance with SAM registration requirements and providing a UEI number. If you cannot get a UEI number in time to apply. Please inform slcgp.grants@maryland.gov and cc' Jesse Limmer when you submit your application.
- Subrecipients who are municipalities and local health departments must include a completed W-9 form with their application.
- Mailing Address & Check Mailing Address: Please provide the mailing address for your project and address for mailing any checks, if they need to be sent to your entity.
- Suspension, Proposed Suspension From Receiving Federal Award funds: Is the applicant submitter or any other employee or contractor participating in this project suspended, or otherwise excluded from or ineligible for participation in federal assistance programs or activities?
- Fiscal Responsibility: The applicant certifies that its entity's financial system is in accordance with generally accepted accounting principles.

Rural Alignment:

According to the Federal Health Resource and Services Administration, Rural jurisdictions are defined as having a population of less than 50,000 people (https://www.hrsa.gov/rural-health/about-us/what-is-rural). Furthermore, Maryland's

Maryland
DEPARTMENT OF
EMERGENCY MANAGEMENT

Russell J. Strickland | Secretary

Maryland
DEPARTMENT OF
INFORMATION TECHNOLOGY

Katie Savage | Secretary

State and Local
Cybersecurity Grant Program

State Office of Rural Health lists Maryland's rural jurisdictions. Based on this information, Maryland has 8 rural jurisdictions out of 24 total jurisdictions: Caroline, Dorchester, Garrett, Kent, Queen Anne's, Somerset, Talbot and Worcester. Maryland will ensure that 80% of SLCGP funds are passed down to local jurisdictions. If you're applying from one of the counties designated as "rural" please check the "Yes" box on the SLGCP Project Proposal Template. Then in the space below, explain what county you're applying from and how the selected Maryland Project Category is aligned with your county's needs.

Proposal Summary:

Must align with the project title, summarize the project's goals, and provide a high-level narrative of the project. As stated above, this section should clearly delineate how the project will build or sustain capabilities based on gaps found during the completion of Appendix A: Cybersecurity Capabilities Assessment[6].

Other important information that should also be included in this section:

- Title(s) and name(s) of those overseeing the project.
- Roles and responsibilities of those overseeing the project.
- Anticipated Impact: Briefly summarize the desired outcome that the proposed project will be achieved and how the project will build or sustain capabilities based on gaps found during the completion of the Appendix A: Cybersecurity Capabilities Assessment. Another way to answer this question is in the negative (i.e., what would happen if this project fails to receive funding?)
- Specify the groups that will benefit from the project, including if the project has incorporated equity considerations as defined in the Funding Guide..
- Describe involvement and expertise of relative partners, stakeholders, staff, contractors, and any other involved parties.
- Address any impacts of the project on the general public and include a plan for how to disseminate information or facilitate public involvement.
- Explain how the project ties to the Maryland Project Category(ies) selected.

Project Deliverables

---

[6] The Cybersecurity Capabilities Assessment and instructions for its completion can be found in Appendix A of the Maryland SLCGP Notice Of Funding Opportunity (NOFO).

This section describes the deliverables expected to be produced by the end of your project. Objectives should note the activities and/or deliverables that will be achieved and provide additional granularity against the description provided in the Project Summary section. Objectives are most easily related to project deliverables.

- Example: The project will deliver a series of workshops designed to assist local jurisdictions evaluate current emergency preparedness plans and other authoritative documents and formulate project concepts for future execution.

Project Metrics Summary

This section should include measurable milestones. Formats such as SMART (Specific, Measurable, Achievable, Realistic, Time-Bound) should be considered. This section should strongly align with the Appendix E: Measurable Milestones section. Also explain how periodic updates on the project's progress will be recorded to report to the Maryland State and Local Cybersecurity Grant Program Planning Committee during the life of the project.

- Example: Complete 7 drills related to project scope by 6/30/2024
- Example: Procure project all equipment no later than Q3 of 2024
- Example: Deliver 4 trainings related to project scope within 90 days of accepting subaward
- Example: Submit requests for reimbursement no later than 15 days from receipt

Project Sustainment Plan:

Applicants are expected to plan for project sustainment once they no longer have SLCGP funds. In this section, please explain your project sustainment plan after the period of performance ends. Also in this section, notate any other funding sources related to the successful completion of the proposed project that may assist with project sustainment.
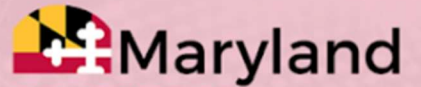
Certification of Application Information

The information, certifications, and representations in the application should be reviewed and signed by an authorized official of the recipient to attest to the

accuracy of the application.

SUB-GRANT SLCGP BUDGET NARRATIVE TEMPLATE INSTRUCTIONS

I. Budget Narrative Overview

The applicant must submit a Budget Narrative using the provided budget template that serves as a detailed line-item budget. This Narrative must include the:
- Budget Dashboard
- Budget Summary: Cost for personnel, fringe benefits, travel, contractual, and other expenses. Please include any reimbursement needs/dates.

II. Detailed Budget Narrative and Budget Justification:

- **Detailed Budget -** Applicants must submit a detailed line-item budget. Applicants should utilize the template provided. Line-item expenditures should be listed in the greatest possible detail. The budget must identify the total amount of funding requested, with a breakdown of amounts to be spent in the following budget categories: Personnel, Fringe Benefits, Travel, Equipment, Supplies, Contractual, Training, and Other. Budgets must be submitted in U.S. dollars and final grant agreements will be conducted in U.S. dollars.

  The following are allowable expenses for the funds granted by the State and Local Cybersecurity Grant Program:
  - Planning
    - Development, review and revision of cybersecurity plans
    - Other planning activities
  - Organization
    - Program Management
    - Operational Support
    - Hiring of personnel (training and exercise coordinators, program managers, planners)
  - Equipment, which includes:
    - Maintenance contracts/agreements
    - Warranty coverage
    - Licenses and user fees
    - Repair or replacement of equipment
    - Equipment upgrades
  - Exercises

- ○ Must use HSEEP concept[7]
- Training
- Management and Administration (M&A)
  - ○ M&A costs are allowable expenses for this grant. An eligible entity may use up to 5% of the SLCGP award for M&A purposes.
  - ○ M&A costs and activities are not operational costs; they are those costs and activities incurred in direct support of the grant or as a result of the grant and should be allocated across the entire lifecycle of the grant. They are directly related to managing and administering the award, such as financial management, reporting, and program and financial monitoring.

If the grant administrator(s) identify costs that are inconsistent with any of these requirements, these costs may be disallowed, and the grant administrator may recover funds as appropriate, consistent with applicable laws, regulations, and policies.

- **Budget Justification:** Applicants must submit a budget justification to accompany the detailed line-item budget. The purpose of the budget justification is to provide additional information for the detailed budget spreadsheet by justifying how the budget cost elements are necessary to implement project objectives and accomplish the project goals.

---

[7] For more information on the HEESP concept review: https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep

State and Local
Cybersecurity Grant Program

SLCGP ISO SHARED SERVICES APPLICATION INSTRUCTIONS

The information below will guide you through the application process for the Endpoint Detection and Response Shared Service Program. It is the responsibility of the applicant to ensure that the application package has been received in its entirety. Incomplete applications will be considered ineligible for review by the Committee.

I. **Shared Service Program Information**
    The shared services Information Security Officers (ISO) will be stationed within the Office of Security Management at the Department of Information Technology (DoIT) and will work collaboratively with various government entities to strengthen their information security posture.

    Through this program, applicants can apply to be considered for this Shared Service Program instead of receiving funding.

II. **Shared Service Description**

    Utilizing the SLCGP Year 1 funds, the State of Maryland will provide a Maryland Shared Information Security Officer (ISO) Program. This program is a specialized service, administered by the State, and funded through SLCGP grant funds.

    The purpose of the program is to provide dedicated ISOs to units of local government, including counties, municipalities, and public school systems. The program is designed to support units of local governments to conduct cybersecurity assessments in compliance with NIST CSF / NCSR and Maryland's Minimum Cybersecurity Standards created by the Maryland Department of Information Technology, conduct vulnerability assessments, external vulnerability scanning via CyHy, identify gaps from assessments and recommend the top 10 priorities, and help local units of government by consulting on how to reduce risk, improve security, cyber readiness and resilience, and hardening networks.

III. **Shared Service Application Description**
     To apply for the shared service program follow the prompts in the application. You'll be required to
     a. Select that you want to participate in the Shared Service Program (Applicants are eligible to apply for both Shared Service and the Sub-grant program)

b. Review and agree to the description of the program implementation
c. If applicable, signify how your project aligns with the Rural Jurisdiction pass-through consideration.
d. Complete the special Review and Certification section of the application

IV. Shared Service Application Elements

Grading Consideration

The Committee has determined that rural jurisdictions receive priority for this program and will be selected first during the program rollout.

Requesting Jurisdiction:

The Jurisdiction must include County, city, and/or town being applied for and must report if the applicant is an institution of public health, or education if applicable.

Size of Jurisdiction

Please provide the estimated size of your jurisdiction's population. (If you are a school, please include students and staff. If you are a county, please include the total population).

Operational Technology Question

Please explain if you are also applying for funds to address operational technology cybersecurity gaps, or other needs as a separate project within the Sub-grant Project Application.

Contact Information

Please provide the contact information for the following individuals:

- Project Manager Name, Email and Telephone Information.
- Financial Contact Name, Email and Telephone Information. This individual is responsible for managing the project budget and ensuring that the grant expenditures will be tracked and segregated from other expenditures.
- Administrative Contact Name, Email and Telephone Information. This individual is responsible for completing and submitting programmatic and financial progress reports.

- Approving Authority (Project Sponsor) Contact, Email and Telephone Information (if a different individual from the Project Manager).

Please determine who will be the primary contact for application updates.

General Questions

Please certify that you wish to participate in the ISO program, if you have had a third-party cybersecurity assessment conducted within the last 12 months, and if you require assistance with remediation efforts related to the security gaps identified from your last assessment.

ISO PROGRAM APPLICATION REQUIREMENTS SECTION

Mandatory Forms Attestation & Required Certifications

1. **Mandatory Forms:** The following documents must be submitted as part of your proposal. Applications not submitted with this information will be considered incomplete and will not be reviewed by the Committee.

   By checking the box in this section for each document, the applicant is attesting that their application packet is submitted in its entirety.

2. **Availability of Additional Funding Sources & Duplication of Efforts Certifications:**

   Please review and certify that the jurisdiction and/or governing body your entity belongs to does or does not have any funding opportunities or programs that would cover the needs of the ISP Program. If there is partial or complete funding or programs available from another source, please explain why the ISO program would be needed to support your entity on top of already available funds.

Compliance Requirements

Please review and certify the information in this section for your application:

- SAM: Compliance with SAM registration requirements and providing a UEI number. If you cannot get a UEI number in time to apply. Please inform

slcgp.grants@maryland.gov and cc' Jesse Limmer when you submit your application.

- Recipients who are municipalities and local health departments must include a completed W-9 form with their application.
- Mailing Address: Please provide the mailing address for your jurisdiction.
- Suspension, Proposed Suspension From Receiving Federal Award funds: Is the applicant submitter or any other employee or contractor participating in this project suspended, or otherwise excluded from or ineligible for participation in federal assistance programs or activities?
- Fiscal Responsibility: The applicant certifies that its entity's financial system is in accordance with generally accepted accounting principles.
- Local Consent Form (ISO Program Only): Jurisdictions that are chosen to participate in the ISO program must sign a consent form before implementation. The consent form will state that the jurisdiction will receive ISO services in lieu of funding. Please check yes to acknowledge that you understand this future requirement.

Approving Local Authority

Please identify an approving local authority who is authorized by your entity to attest to the accuracy of the application submitted for Maryland SLCGP ISO Application. This authority must also sign the mandatory Local Consent Form that must be submitted with this application.