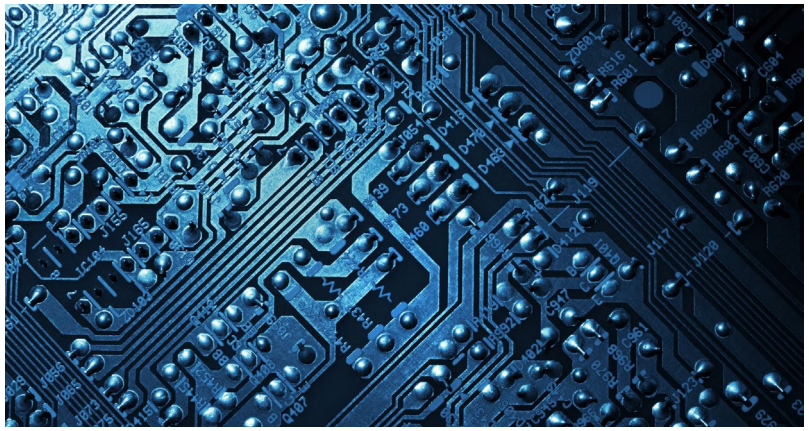
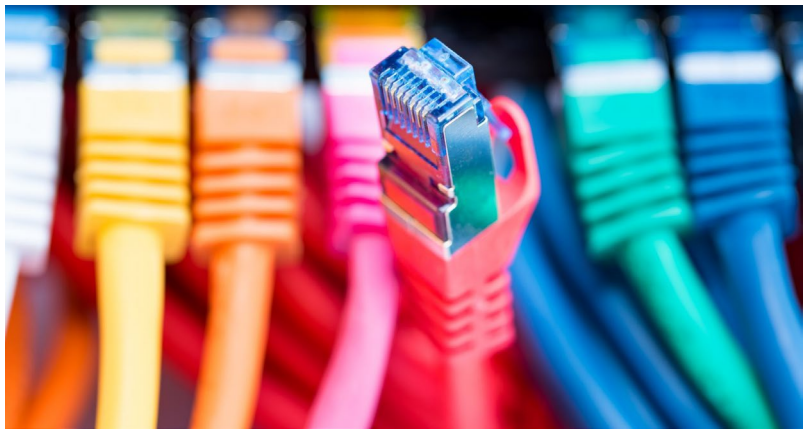
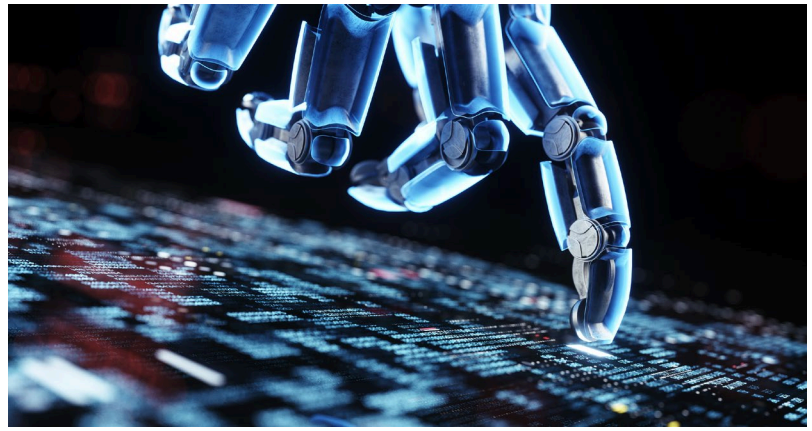
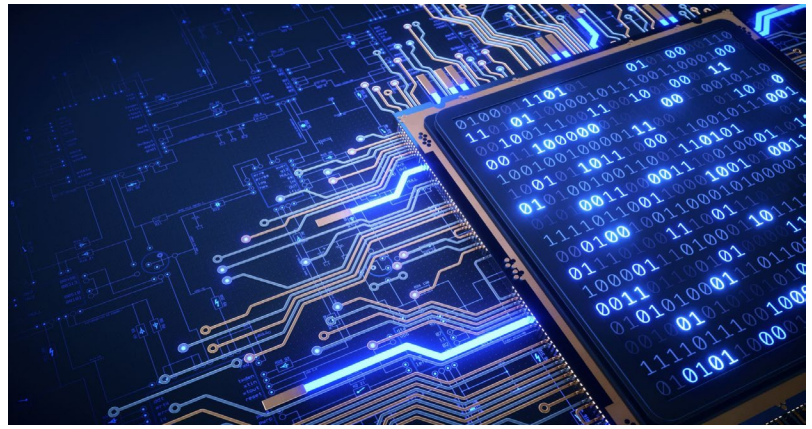






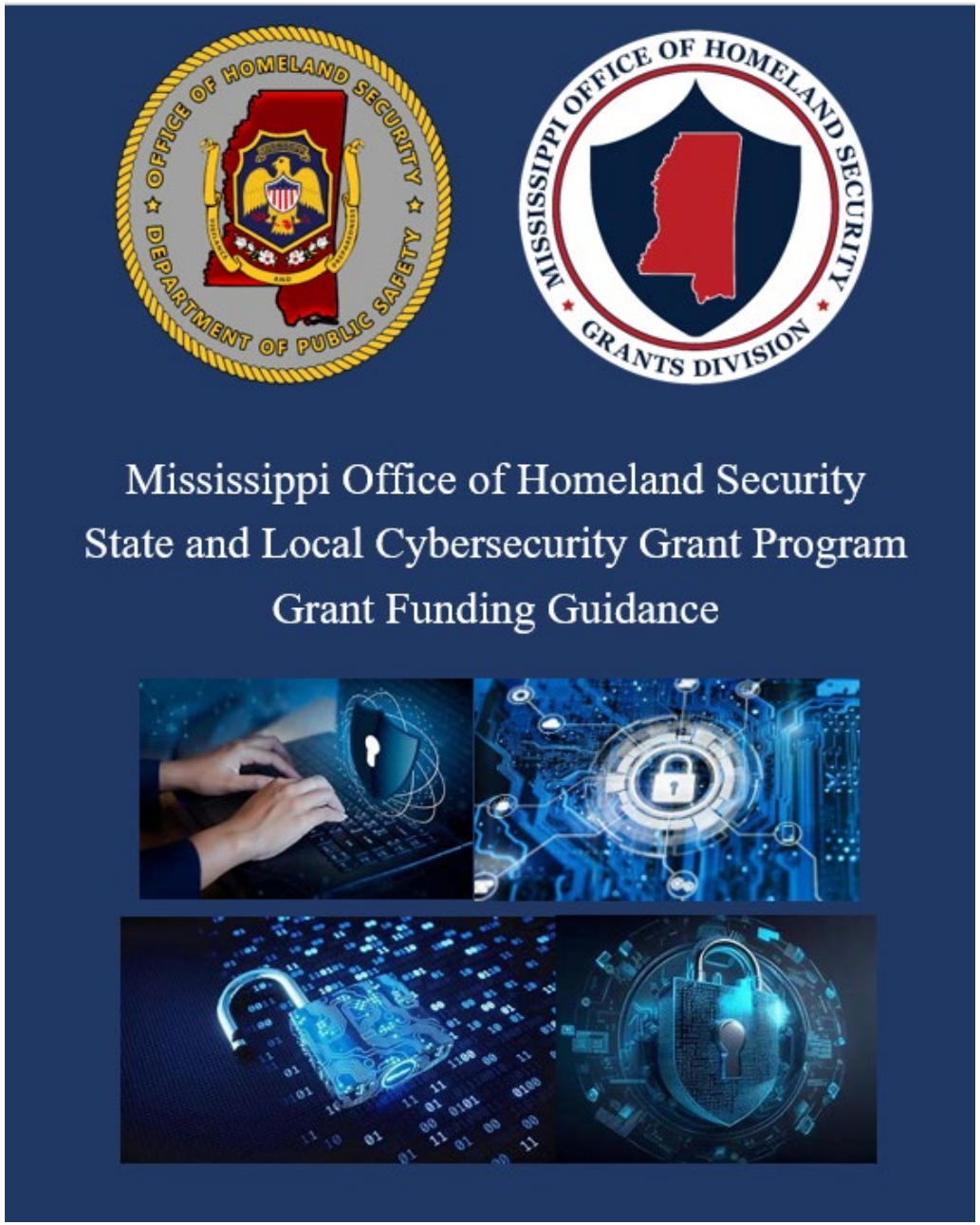


Mississippi Office of Homeland Security
State and Local Cybersecurity Grant
Grant Writing Session

Welcome and Introductions

Beth Loflin- MS Office of Homeland Security- Grants/Finance Director

Bobby Freeman-MS Office of Homeland Security Cybersecurity Director



In the State and Local Cybersecurity Grant Program Funding Guidance, information is provided to fill out the FY25 Grant Application.

Please read and follow the step-by-step instructions for each section.

Schedule for State and Local Cybersecurity Grant Program (SLCGP):

Key Announcements	Key Dates
Notice of Funding Release of FY25 Grant Funds	April 14, 2025
SLCGP Grant Application Release	May 1, 2025
Grant Writing Sessions (Virtual)	May 15, 2025 @ 10:00 a.m. May 22, 2025 @ 10:00 a.m.
Application Deadline	June 4, 2025, by 5:00 p.m.
Application Review Period	June 2025 Initial Risk/Financial Assessment Review (June) Cybersecurity Review (June/July) Executive Award Review (July)
Award Announcement	August 1, 2025 (Tentative)
Grant Orientation	August/September 2025
Grant Awards Released	At Implementation Meetings (Tentative)
Grant Packets Due and to be Returned to MOHS	October 15, 2025 (Tentative)
Grant Performance Period	September 1, 2025-August 31, 2026
Grant Closeout Deadline	November 1, 2026

Federal Award Overview:

Department of Homeland Security

State and Local Cybersecurity Grant Program

Assistance Listing Number (Formerly CFDA) 97.137

Federal Grant Period: 9/1/2022-8/31/2026

https://www.fema.gov/grants/preparedness/homeland-security

Program Objective:

The SLCGP is to assist **local** jurisdictions with the managing and reducing cyber risk for their agencies.

SLCGP Grant

These funds are provided as a four (4) year grant program from the federal agencies FEMA and CISA to State Agencies, such as the MS Office of Homeland Security.

MOHS Goals for the SLCGP Grant Program

Prioritize Grant Funds to be used in the most efficient and effective way!!!

1

Identify the **Problems** within the State.

2

Identify solutions for the **Problems** found within the State.

3

Provide funds (If possible) to areas with **Needs** that can be addressed.

Federal Appropriation

SLCGP Funds are from 2022-2024 Federal Appropriations

- Items within the Funding Guidance are subject to change, based on funding amounts; Federal Notice of Funding; Guidance and FEMA/DHS.

- The Application is an Application and **not** a Guarantee of any funding.

Federal Funding for SLCGP

The MOHS has received the following amounts so far for the SLCGP program.

- FY22: $3,273,651.00
- FY23: $6,639,551.00
- FY24: $5,034,487.00
- FY25: $1,750,000.00*

Total: $16,697,689.00* Total Funds for Program

Important Application Information

Application Deadline:

All SLCGP applications and supporting documentation must be received by the Mississippi Office of Homeland Security offices by **June 4, 2025, by 5:00 p.m. CST.**

Email to:
MOHSgrants@dps.ms.gov

Who can Apply?

- The applicant must not be listed on the suspended and debarred list.
- The applicant must not be listed on the Denied Parties List.
- The applicant must be NIMS complaint with NIMS Courses (100, 200,700 and 800).
- Applicants must have a current and active DUNS/Unique Entity Identification number.
- Applicant must read and comply with 2 CFR 200.318 to 2 CFR 200.327 regulations.

Who can Apply?

Must be a participant into the SLCGP Grant Program.

- Completed and Submitted Memorandum of Understanding to MOHS
- Completed and Submitted a Consent Form to MOHS
- Only Batch 1 and Batch 2 are eligible for Application Submission.

Who can Apply?

Eligible Entities: Eligible sub-entities able to apply for SCLGP funding include State, tribal, and local governments. "Local government" is defined in 6 U.S.C. § 101(13) as:

- A county, municipality, city, 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.

- An Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; and

- A rural community, unincorporated town or village, or other public entity.

Special Emphasis with Grant Applications that are considered RURAL Entities.
50,000 or less in population

What do I need to Apply?

- Applicant must have written procurement standards per 2 CFR 200.318(a).
- Applicant must have written conflict of interest standards per 2 CFR 200.318(c).
- Applicant read and understands that certain telecommunications and video surveillance services or equipment are prohibited from being purchased using grant funds. See 2 CFR § 200.216 and 2 CFR § 200.471.
- Applicant must take necessary steps to assure that minority businesses, women's business enterprises, and labor surplus area firms are used, when possible, per 2 CFR 200.321.
- Applicant agrees that this federal funding does not supplant (replace) state, local, and agency monies in their organization's budget for the requested items in this application.

What do I need to Apply?

The following MUST items must be submitted, or the application will be considered incomplete.

- Complete SLCGP Application
- Agency Signatures
- UEI Certification (Active) & UEI #
- Audit (Most Recent)
- NIMS Certification (100, 200, 700 & 800)
- Justifications (If Required)
    - Items over $75,000.00

Grant Fund/Project Selections

Grant Funds will be based on availability of funds with several important factors to consider:

- Risk/Vulnerability and Need of Jurisdiction
- SLCGP Cybersecurity Assessment Results
- Cost of Project
- Impact of Project

What Happens After Application is Submitted?

- Applications Received
- Applications Reviewed for Completeness
- Applications-Risk/Financial Assessment
- Application-Peer Review
- Executive Planning and Funding Review

Please Remember….

- **<u>Funding is limited. Funding is competitive. Funding is NOT a guarantee!!</u>**

- Please prioritize projects and requests. Awards will be made on the need identified, how the need will assist the State in the MOHS mission and if funds are available.

- Projects may be funded in whole or partially funded.

All applicants will receive a notice of award or notice of non-approval. All non-approval applications will be kept on file for (1) one year if funds become available. If funding becomes available, then a MOHS staff member will contact the agency to discuss opportunities.

Endpoint Detection & Response
Purchase subscriptions for Endpoint Detection and Response, Managed Detection and Response, and Extended Detection and Response licensing vendor selected utilizing entities established procurement policies and grant performance and spend period time frames. Subscriptions cannot go past August 2026.
Cybersecurity Assessments/Testing and Evaluation:
Purchase an independent Cybersecurity Assessment or Penetration Testing for the organization utilizing existing State of Mississippi negotiated contractors. Contractors can be found on the Department of Finance and Administration Website. Cybersecurity Assessments can be applied as a follow-up/progress to the original MOHS cybersecurity assessment. • Maturing assessments • Tabletop exercises • Cybersecurity exercises, testing for team capabilities and controls.
Multifactor Authentication Solutions (MFA)
Purchase authentication devices, MFA Software, or other systems/hardware supporting MFA such as Identity and Access Management systems.
Advanced Backup Solutions
Purchase backup software, cloud services, backup servers, storage devices, or other services that support recovery and reconstitution of entity backup data.
Migration to the .gov Domain
Pay for services that support the migration of the organization's domain to a .gov internet domain. Managed Service Provider services to pay support vendors to perform migration tasks to a .gov domain.
Managed Service Provider Costs to pay for Cybersecurity Services
Pay Managed Service Providers for cybersecurity services that mitigate risk, improve cyber resiliency, and perform cybersecurity work where an organization does not have onsite staff to support.

Cybersecurity Awareness Training
Purchase subscriptions for cybersecurity awareness training for employees to better understand cyber threats, best practices, incident response, compliance, and policies. KnowBe4, Proofpoint, SANS Institute & Infosec IQ are examples of vendors providing security awareness training.
Cybersecurity Professional Training for IT/Security Staff
Purchase professional cybersecurity training for those responsible for mitigating risk and maintaining resiliency in the organization's environment. Example Trainings: CompTIA, CySA+, PenTest+ Certification Training, SANS Institute Enterprise Cloud Security Architecture, Certified Ethical Hacker, Security Training, and Certifications that will increase the skills and knowledge of systems and security.

SLCGP Funding Guidance. Page 5-6 *Potential Allowable SLCGP Projects (Not limited to these)

Allowable SLCGP Grant Items:

Allowable Costs may include the following funding areas:

- Contractual Services
- Equipment
- Commodities/Supplies
- Other

Unallowable SLCGP Grant Items:

Supplanting:

- Grant funds will be used to supplement existing funds and will not replace (supplant) funds that have been appropriated for the same purpose. Applicants or recipients may be required to supply documentation certifying that a reduction in non-federal resources occurred for reasons other than the receipt or expected receipt of federal funds.

All items MUST be NEW planned items. Items can not have already purchased for the entity.
Can not replace already purchased items with local funds and replace with federal funds.

Prohibited SLCGP Grant Items:
Funding Guidance: Page 10

Recipients and subrecipients of FEMA federal financial assistance are subject to the prohibitions described in section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (FY 2019 NDAA), Pub. L. No. 115-232 (2018) and 2 C.F.R. §§ 200.216, 200.327, 200.471, and Appendix II to 2 C.F.R. Part 200. Beginning August 13, 2020, the statute – as it applies to FEMA recipients, subrecipients, and their contractors and subcontractors – prohibits obligating or expending federal award funds on certain telecommunications and video surveillance products and contracting with certain entities for national security reasons.

Guidance is available at FEMA Policy #405-143-1 - Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services Additional Information and restrictions can be found in FEMA NOFO.

Let’s Write a Grant Application

Mississippi Office of Homeland Security

State and Local Cybersecurity Grant Program (SLCGP)

Grant Application

Date of Application			
Name of Agency			
Mailing Address			
City		**Zip Code**	
County			
Agency Contact Name			
Contact Phone Number			
Contact Email Address			
Signatory Authorized Offical Name			
(Name of Mayor, Board President, Commissioner, Head of Agency, etc.)			
Signatory Authorized Email Address			
UEI Number		**Expiration Date**	
**** Please provide a copy of UEI number and current status, as shown in SAM.gov.***			
Congressional District			

Information and Contact Page Funding Guidance Page13

Grant Applicant Funding Request By Cost Category	
Cost Category	**Amount Requested**
Contractual Services	$0.00
Equipment	$0.00
Training	$0.00
Other	$0.00
Total of Grant of Grant Amount Requested	**$0.00**

Allowable Cost Categories for SLCGP

Problem Identification

Problem Identification

Agency Cybersecurity Information					
How many employees are in your IT Department?					
Are IT operations, whole or part(s), outsourced?					
How many endpoints/ devices (e.g. laptops, desktops, servers, mobile devices) within your organization?					
Has your Agency conducted a Cybersecurity Assessment?	☐	Yes	☐	No	
If assessment was completed, was the proposed project being applied for, identified as a Vulnerability or Gap?	☐	Yes	☐	No	
Does your Agency currently have Cybersecurity Insurance?	☐	Yes	☐	No	
Does your Agency have written cybersecurity policies that all employees must consent and abide by?	☐	Yes	☐	No	

Agency Type:

Agency Type:					
☐	County	☐	Municipal	☐	School District
☐	Law Enforcement	☐	Fire Service	☐	Emergency Management Agency
☐	Hospital/ Medical Service	☐	Circuit Clerk	☐	Chancery Clerk
☐	Coroner	☐	Public Works	☐	Water District
☐	Tax Office	☐	State Agency	☐	Election Security
☐	Other: Please Place Description of Organization in Next Box.				

Proposed Project Description and Project Details

Description and Details

Proposed Project Description and Project Details
Provide a detailed summary of the Project that the Agency will implement?
The MOHS is looking for a detailed summary of the project details and how the project will be implemented within the agency. Why does the agency need funds?

Provide as much information and details as possible when describing the planned project that will be implemented. If there is not enough room, please add in additional lines.

Gaps, Vulnerabilities and Capabilities

Cybersecurity Gaps, Vulnerabilities and Capabilities					
Provide a detailed description of any Cybersecurity gaps, vulnerabilities that hinder your agency's ability to prevent, protect, mitigate, respond to, and recover from cybersecurity threats and hazards. All information provided is confidential and will remain so, as part of this Application and for the support of the program.					
How was the Cybersecurity Gap/Vulnerability identified?					
☐	**Real Cybersecurity Event**	☐	**Cybersecurity Exercise**	☐	**Cybersecurity Assessment**
Clearly describe the Cybersecurity Gap(s)/Vulnerability of the Agency that is the main priority of the project?					
The MOHS is looking for the main priority that was determined by the above identification resources. The MOHS is looking for the main priority that the requested funding will address. Gaps and/or vulnerabilities should be detailed and specific.					

Please mark one of the three options on how the GAP/VULNERABILITY was identified.

Provide a description of the GAP/VULNERABILITY that is the main priority of the project.

Gaps, Vulnerabilities and Capabilities

Clearly describe how this project will address the Cybersecurity Gap(s)/Vulnerabilities and how funding will allow the Agency to improve the cybersecurity capability?
The MOHS is requesting detailed and specific information on, "if" the project is awarded how will the funding address the gap(s)/vulnerability. How will the funding "fix" the problem?
Describe how the requested funding, resources, training, or equipment will increase your Agency capabilities to address the Cybersecurity Gap(s)/Vulnerability?
The MOHS is looking for a detailed description of how the awarded items will increase the capabilities of the Agency. Will the training better prepare the workforce? Will the equipment help reduce the gaps and vulnerabilities by securing the network? Will software reduce attacks?
Describe the impact/outcome of the cybersecurity project, if awarded?
The MOHS is looking for responses that describes the outcome of this funding, services ad equipment will impact the Agency for the future. How will this project impact your Agency, City/County and the State when it comes to Cybersecurity?

Provide detailed descriptions to the questions for the following questions. Add as much detail as possible, if agency runs out of room, please add in additional lines.

Grant Objectives

Alignment with State and Local Cybersecurity Grant Objectives	
Applicants are required to address how the potential project will align with the State and Local Cybersecurity Grant Program Objectives. Please mark the Objective that will best fit the Applicant Project.	
☐	**Objective 1: Governance/Planning:** Develop and establish appropriate governance structures, as well as develop, implement, or revise cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.
☐	**Objective 2: Assessment and Evaluation:** Understand their current cybersecurity posture and areas of improvement based on continued testing, evaluation and structured assessments.
☐	**Objective 3: Mitigation:** Implement security protections commensurate with risk.
☐	**Objective 4: Workforce Development:** Ensure organizations personnel are appropriately training in cybersecurity, commensurate with responsibility.

Mark one or multiple objectives that best fit the planned project.

Grant Budget

Contractual Services

Type of Contractual	Amount of Service	Quantity of Service	Total
			$0.00
			$0.00
			$0.00
			$0.00
			$0.00
			$0.00
Total Contractual Service			**$0.00**

Contractual Services should be requested for one (1) year of service only. All expenses must be in accordance with current state and federal guidelines. Agency should be prepared to be able to continue contractual services after the end of the Grant Performance Period.

Cybersecurity Equipment

AEL Number	AEL Equipment Title	AEL Description
04AP-04-RISK	Software, Risk Management	Software or systems that facilitate capture, quantification, and management of risk factors involved in specific tasks, environments, or programs. This functionality may also be obtainable via subscription as a cloud-based service, as opposed to purchasing software. However, special security considerations apply for data stored remotely. See 04AP-11-SAAS for further information.
04AP-11-SAAS	Applications, Software as a Service	Sometimes referred to as "on-demand software", SAAS applications run on the provider's servers, delivering functionality via the internet to any device having connectivity and the required browser or interface. Access to the application is obtained via a service subscription rather than outright purchase, with all updates and configuration requirements handled by the service provider. Some example SAAS applications include equipment tracking and maintenance, intra-application communication among client devices, and specialized software such as plume modeling. Note that purchasers of SAAS should consider the security aspects of the planned usage, particularly availability and the protection of sensitive information stored remotely. Internet connectivity is required to utilize SAAS applications unless specific failover measures such as a "hybrid cloud" are available. In addition, data is stored remotely on vendor equipment. Use of SAAS for mission critical applications should be thoroughly vetted before implementation.

SLCGP Funding Guidance.
Pages 6-9

All equipment must be on the FEMA Authorized Equipment List (AEL). You can find the AEL at https://www.fema.gov/grants/tools/authorized-equipment-list. Equipment MUST be for cybersecurity-based programs and activities. (See Funding Guidance for more information).

Training/Workforce Development

Training/Workforce Development
Professional cybersecurity training is allowable for those responsible for mitigating risk and maintaining resiliency in the organization's environment. Example Trainings: CompTIA, CySA+, PenTest+ Certification Training, SANS Institute Enterprise Cloud Security Architecture, Certified Ethical Hacker, Security Training, and Certifications that will increase the skills and knowledge of systems and security IT administration teams.

Training Name	Training Costs	Number of Person(s) to be Trained	Total Costs
			$0.00
			$0.00
			$0.00
			$0.00
			$0.00
Total Costs of Training/Workforce Development			**$0.00**

Please include a listing of any trainings or professional certification programs that the Agency will be seeking with grant funds. Please include Training Name, Costs, Number of person(s) to be training and the total costs.

Training/Workforce Development

How will the requested training/certifications program reduce the Gap(s)/Vulnerabilities and increase Agency capability?
The MOHS is looking for details on how this training will help the Agency. Training and Certifications should reduce the gap(s), vulnerabilities and create capabilities.

Other Expenses:

Other Expenses:			
If items are requested for the Agency do not fall into the above categories, please list those items into the following section. Please include the item name, item costs, quantity and the total costs.			
Item Name	**Item Costs**	**Item Quantity**	**Total Costs**
			$0.00
			$0.00
			$0.00
			$0.00
			$0.00
Total Costs of Other Expenses			**$0.00**

Include a detailed assessment of additional needs within the program area in which Applicants will be applying. Additional items listed in this category must have a detailed justification for requests. All expenses must be in accordance with current state and federal guidelines.

Total Amount of Request:

Total Amount Request for Cybersecurity Funds	**$0.00**

Please include a total of all budget sections for a total of the funding being requested.

Sustainability:

Federal funds awarded under the SLCGP should be considered as “one” time funding. Funds should be used to address the current priority of the Agency.

Sustainability:

Sustainability of Project
Would the Agency have the funding to implement the above requested budget requests without the use of the SLCGP funding?
The MOHS is looking for information on if funds were not available from this Award, would the Agency be able to fund the current project.
How will the Agency continue goods and services acquired using the federal grant funding after the award is closed?
The MOHS is looking for information on if the Agency will be able to continue the services, once the grant has ended. Will services be continued after the grant?
Has the Agency adopted a plan to ensure future improvements in cybersecurity without SLCGP grant funding?
The MOHS is looking for information on the Agency's future plans for Cybersecurity. Will there be follow-up assessments or potential request(s) for additional funding, if available? Will the Agency seek additional support from the jurisdiction or other routes for funding?

Prior Grant Experience:

PRIOR GRANT EXPERIENCE		
Please answer YES or NO to the following questions.		
	YES	**NO**
Has your agency received federal and/or state grants similar to the MOHS Grant?	☐	☐
Does your agency have at three (3) years of receiving federal grant funds? Does not have to be MOHS related.	☐	☐
Has your agency received MOHS Grant funds within the past three (3) years?	☐	☐
Has your agency ever received any corrective actions from a Audit Report?	☐	☐
Has the agency administration remained unchanged during the 2024 grant year? For example: (Chief, Sheriff, SGA, Financial Officer, Program Staff)	☐	☐
Can this project be completed by August 30, 2026?	☐	☐

Agency Audit:

AGENCY AUDIT	
Non-federal organizations, which expend $1,000,000.00 or more in federal funds during a fiscal year, will be required to have an audit performed in accordance with 2 CFR Part 200, Subpart F. Applicant **MUST** provide a copy of their latest audit report, if Applicant meets the funding threshold. Attach a copy of the latest audit to this Application.	
☐	I certify that the Applicant's associated city/county/organization does **NOT** expect, to be required to have an audit performed under 2 CFR Part 200, Subpart F, for the above listed program.
☐	I certify that the Applicant's associated city/county/organization, **WILL BE** required to have an audit performed under 2 CFR Part 200, Subpart F. A copy of the audit report **MUST** be attached at the time of Application submission.

Non-federal organizations, which expend $1,000,000.00 or more in federal funds during a fiscal year, will be required to have an audit performed in accordance with 2 CFR Part 200, Subpart F. Applicant **MUST** provide a copy of their Applicants latest audit report, if applicant meets the funding threshold. If an agency is applying as a sub-agency of a municipality or county, please include the municipality or county's latest audit report. Attach a copy of the latest audit at the time of the Application submission.

If an agency is required to submit an audit, but is not submitted with the Application, the Application will be considered incomplete.

Application Submission Compliance

Please read the following statement if the applicant agrees with the submission of the SLCGP Grant Application please have the person completing the Application fill out the following:

Application Submission Compliance	
I certify that I am an employee of the aforementioned agency or have been hired by the Agency to apply on their behalf for the Grant. All parties have knowledge and approved of the contents of this Application, Budget Request and all information provided within.	
Applicant Signature	Date
Applicant Name (Please Print)	Applicant Title

Before Submitting Application

BEFORE SUBMITTING THE SLCGP APPLICATION:

Have you included:

- State and Local Cybersecurity Grant Application:
  - All sections of the Application must filled be out. No blank spaces.
  - Double checked AEL/Equipment list and include allowable AEL Numbers.
  - Cost estimates will cover all areas of the budget request.

- Required Documentation is Provided at the time of the Application submission:
  - Unique Entity Identification Number
    - UEI Confirmation. As shown in Grants.gov
      - UEI Number
      - Current Status
  - Latest Audit (If Applicable)
  - Agency Cybersecurity Assessment: Agency should provide a copy of the most recent Cybersecurity Assessment. Assessment should be no older than (2) years old.

- NIMS Compliance Certifications
  - 100
  - 200
  - 700
  - 800

- Additional Justification Statement, if applicable for the following items:
  - Items are over $75,000.00

- Once completed and double checked.
  - Email the mohsgrants@dps.ms.gov, on or before **June 4, 2025**, at 5:00 p.m.

MOHS will provide an Approval or Non-Approval Letter to each Applicant on or before August 1, 2025

Before submitting the Application, be sure you have checked and reviewed all the requirements for submission.

Items Required for a COMPLETE Application Submission

If required items are missing with the submission, the Application will be tagged as **incomplete.**

Missing Information and Documentation could result in not being awarded or awarded reduced levels.

WHAT IS AWARDED IS AWARDED!!

SLCGP Grant Application Due to MOHS

Due June 4, 2025
By 5:00 p.m.

Questions