



Mississippi Office of Homeland Security State and Local Cybersecurity Grant Program Grant Funding Guidance



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

Application packets will be available at the Mississippi Office of Homeland Security website <https://www.homelandsecurity.ms.gov/>. Grant Applications received after the due date **will not** be accepted for the allocation of funds, but it **may** be considered if funds become available within one (1) year.

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 Information:

The State and Local Cybersecurity Grant Program (SLCGP) was created in 2022 through the Infrastructure Investment and Jobs Act (IIJA) by the federal government to award grants to eligible entities to address cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, state, local, or tribal governments.

The SLCGP provides funding to state, local, tribal, and territorial (SLTT) governments to address cybersecurity risks and cybersecurity threats to SLTT-owned or operated information systems. The overarching goal of the program is to assist SLTT governments in managing and reducing systemic cyber risks. The four main objectives of the program for which all projects at the state and local level must fall into are below:

- **Objective 1:** Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.
- **Objective 2:** Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
- **Objective 3:** Implement security protections commensurate with risk.
- **Objective 4:** Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

Before funding can be distributed to states and eligible sub-entities, the Homeland Security Act of 2002, as amended by the Bipartisan Infrastructure Law requires grant recipients (States) to develop a Cybersecurity Plan, establish a Cybersecurity Planning Committee to support development of the Plan, and identify projects to implement utilizing SLCGP funding.

To comply with federal guidance, the Mississippi Office of Homeland Security and the Mississippi Department of Information Technology Services (MOHS/ITS), acting in its role as the designated State Administrative Agency (SAA) for this program, began working with the established Statewide Cybersecurity Committee in 2022 to prioritize the following activities to meet SLCGP grant requirements:

- Establish a Cybersecurity Planning Committee.
- Develop a state-wide Cybersecurity Plan, unless the recipient already has a state-wide Cybersecurity Plan and uses the funds to implement or revise a state-wide Cybersecurity Plan.
- Identify and support projects that meet the objectives documented in the plan.

SLCGP Funding:

The SLCGP funding available is dependent on the fiscal year. Currently, there are three (3) fiscal years of funding available to Mississippi eligible entities. For grant years 2022 and 2023, the MOHS was able to secure cost waivers that would allow for all grant funds to be awarded without matching requirements. The MOHS is still currently waiting for the waiver determination of 2024 funds. At this time, MOHS plans to cover all matching funds with soft match amounts, so that local entities may be able to apply and be awarded without a matching cost burden.

Grant Funding Eligibility:

The State of Mississippi is the sole eligible entity with the ability to submit SLCGP applications to DHS/FEMA.

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.

State Agencies: Under the SLCGP, the State Administrative Agency (SAA) **may retain no more than 20 percent of funding** for expenditures made by the state on behalf of the local unit(s) of the government. Funding outside of the 20 percent may occur **only** with the written consent of the local unit(s) of government and the approval of DHS/FEMA.

Ineligible Entities: Ineligible entities are those entities that do not meet the definition criteria, as listed above, to include private businesses/corporations and non-profit entities. Non-Profit entities can include those entities that hold a 501(c)(3) designation status and/or houses of worship.

Memorandum of Understanding (MOU): The Mississippi Office of Homeland maintains all MOU’s indicating written consent of the local unit(s) of government. All MOU’s must be submitted to FEMA, approval and the award will be at the discretion of FEMA’s approval, if funding is allocated.

- Grant Application requests are **not** a guarantee for funding. Grants may be funded in the whole or partially funded. All funding considerations will be based on need and how the project fulfills the needs of the MOHS priorities and programs.
- The total amount of funding is limited to the amount received by FEMA, national priorities, and the requirements of the grant.
- Prioritize funding requests for items that **meet the needs** of the grant and applicant’s department. Awards will be given to projects with the needs identified in the Application.
- All funding requests must be reasonable and allowable.

What can I apply for?

If Applicants have questions regarding the allowable or unallowable use of funding or need assistance in completing the Application, please contact mohsgrants@dps.ms.gov. Applicants may also visit the FEMA website and review the Notice of Funding Opportunity to review all grant funding guidelines for this grant opportunity. Please see the link below: <https://www.fema.gov/grants/preparedness>

Allowable Grant Items:

Please see the State and Local Cybersecurity Grant Program- Notice of Funding Opportunity for additional information on allowable grant costs. The list below is not exhaustive, therefore, if Applicants have any additional questions, please reach out to mohsgrants@dps.ms.gov. Applicants may also visit the FEMA website and review the federal Notice of Funding Opportunity to review all grant funding guidelines for this grant opportunity. Please see the link below: <https://www.fema.gov/grants/preparedness>

Allowable Costs may include the following funding areas:

- Contractual Services
- Equipment
- Commodities/Supplies
- Other

The following chart shows examples of potential projects areas that could be considered for funding.

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. <ul style="list-style-type: none"> • 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.

Equipment-Allowable Costs: SLCGP equipment is intended to be used to address entities' cybersecurity risk, gaps and vulnerabilities. All equipment must be listed on the FEMA Authorized Equipment List (AEL). The FEMA AEL may be found at: <https://www.fema.gov/grants/tools/authorized-equipment-list>. Equipment not listed on the AEL will not be awarded.

The following examples are allowable FEMA AEL equipment items, that can be included but are not limited to the following items. The equipment requested should enhance the project and increase capabilities for the entity.

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.

04HW-01- INHW	Hardware, Computer, Integrated	Computer hardware and operating system software designated for use in an integrated system allowable under the indicated grant programs. Such systems include detection, communication, cybersecurity, logistical support and Geospatial Information Systems. This item may include networking hardware (routers, wireless access points, etc. servers, workstations, notebook computers, and peripherals such as printers and plotters procured with an allowable system and necessary for its implementation.
04HW-03- NETD	Components, Networking, Deployable	Networking devices such as routers, switches, and wireless access points that are designed for forward deployment during incident response. These devices may include functionality such as Power over Ethernet (PoE) or uninterruptible power supplies (UPS). Units may combine functionality, such as a satellite IP modem, wireless, and wired connections, or a router that also provides PoE for hardwired connections and has built-in UPS. These components are often ruggedized or otherwise designed for field deployment (including mesh networking) and are intended to assist in rapid deployment of wired and wireless network capability for incident command centers and other forward deployment activities.
04SW-04- NETW	Software, Network	Software for networking, monitoring network performance and/or maintaining configuration. This functionality may also be obtainable via subscription as a cloud-based service using a web browser interface, as opposed to purchasing software. However, special security considerations apply for data stored remotely. See 04AP-11-SAAS for further information.
05AU-00- TOKEN	System, Remote Authentication	System used to provide enhanced remote authentication, usually consisting of a server, some synchronization scheme, and a device, token, or smartphone application.
05EN-00- ECRP	Software, Encryption	Encryption software for protecting stored data files or email messages.
05EN-00- ETRN	Encryption, Data Transmission	A class of network access solutions, usually for remote access, that provide encrypted user access. May be used for remote access, point to point, or link encryption. Includes virtual private networks, and encrypted transmission modes such as SSH and SSL.
05HS-00- FRNS	Software, Forensic	Application suites that allow in-depth analysis of hosts based on operating system and file systems. Software of this type

		<p>may be used by law enforcement officers, government/corporate investigators and consultants to investigate the aftermath of computer-related crimes. Forensics software generally includes disk analysis tools, tools for the recovery of deleted files, and integrated database support to mark files and data of interest to investigators.</p> <p>This functionality may also be obtainable via subscription as a cloud-based service using a web browser interface, as opposed to purchasing software. See 04AP-11-SAAS for further information.</p>
05HS-00-MALW	Software, Malware/Anti-Virus Protection	Software for protection against viruses, spyware, and malicious code. May be obtained for individual hosts or for entire network segments.
05HS-00-PFWL	System, Personal Firewall	Personal firewall for operation on individual devices. Usually a software solution, but appliances are also available. See also: 05NP-00-FWAL.
05NP-00-FWAL	Firewall, Network	Firewall (software or standalone appliance) for use in protecting networks. See also 05HS-00-PFWL.
05NP-00-HONY	Honeypot	System or software used as a vulnerable decoy to lure and detect attackers.
05NP-00-IDPS	System, Intrusion Detection/Prevention	Intrusion Detection and/or Prevention System (IDS, IPS) deployed at either host or network level to detect and/or prevent unauthorized or aberrant behavior on the network. Software and hardware (appliance) solutions exist. This replaces item 05NP-00-IDS and incorporates more recent prevention technology.
05NP-00-MDMS	System, Mobile Device Management (MDM) or Enterprise Mobile Management (EMM)	Tools to facilitate the administration of mobile devices such as smartphones, tablets, and laptops
05NP-00-SCAN	Tools, Vulnerability Scanning	Tools designed to identify security vulnerabilities on networks, databases, web applications or individual hosts on target networks.
05NP-00-SIEM	System, Security Information and Event Management (SIEM)	Software or appliance that gathers data from multiple security sources such as firewalls, intrusion detection systems, malware protection systems, etc. to provide log file consolidation and event correlation capability in support of network security operations.

		While some client-side software may be required, this functionality may also be obtainable via subscription as a cloud-based service using a web browser interface, as opposed to purchasing software. However, special security considerations apply for data stored remotely. See 04AP-11-SAAS for further information.
05PM-00-PTCH	System, Patch/Configuration Management	System to manage the update and installation of patches, applications, and/or operating systems utilized by an organization in order to maintain current "version control." This functionality may also be obtainable via subscription as a cloud-based service using a web browser interface, as opposed to purchasing software. However, special security considerations apply for data stored remotely. See 04AP-11-SAAS for further information.
05SM-00-ITAM	System, Information Technology Asset Management	Tools for maintaining and consolidating information about an organization's IT resources, including both hardware and software assets.

Additional Required Justifications for Specific Equipment:

Please provide additional information and justification for the items listed below. If additional justification is not provided for the items listed below, items **will not** be considered for review. **Please provide justification, as an additional attachment with the Application submission.**

- Items requested over \$75,000.00. Any items requested over \$75,000.00 will require additional justification **to be considered.** Provide the following:
 - How will this item increase the Homeland Security mission in your area?
 - How will this item reduce terrorism in your area?

Additional FEMA Approval: Some equipment requests may require additional approval from FEMA. MOHS may require additional information and detailed justifications for the request.

- Environmental and Historical Preservation Compliance: All projects that may have potential impact on the environment **will require** a FEMA Environmental Historic Preservation form. For more information, please see FEMA Policy 108-023-1.
 - Ground disturbances, new construction, modification/renovation of buildings (including the addition of cameras, security doors, etc.) will require an EHP form to be submitted.
 - Renovation of and/or modification including installation of security and communication equipment to buildings or structures that are fifty (50) years old or older.
 - Installation of security features such as doors, cameras, security locks, etc., will also require an EHP submission for FEMA approval.
 - Security enhancements to improve perimeter security or any other construction or renovations that change or expand the footprint of the facility.
 - Physical security enhancements including, but not limited to:
 - Lighting

- Fencing
- Closed Circuit Televisions
- Motion Detection
- Stationary/fixed License Plate Readers
- Barriers, doors, gates, and related security enhancements.

Unallowable Grant Costs:

The following items are considered unallowable by FEMA and/or the Mississippi Department of Homeland has deemed the items not permissible for funding. Applicants may also visit the FEMA website and review the Notice of Funding Opportunity to review all grant funding guidelines for this grant opportunity. Please see the link below, <https://www.fema.gov/grants/preparedness>

- 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.

- Unallowable Costs: SLCGP funds may not be used for the following.
 - Spyware.
 - Construction.
 - Renovation.
 - To pay a ransom.
 - For recreational or social purposes.
 - To pay for cybersecurity insurance premiums.
 - To acquire land or to construct, remodel, or perform alterations of buildings or other physical facilities.
 - For any purpose that does not address cybersecurity risks or cybersecurity threats on information systems owned or operated by, or on behalf of, the eligible entity that receives the grant or a local government within the jurisdiction of the eligible entity.
 - To supplant state or local funds; however, this shall not be construed to prohibit the use of funds from a grant under this NOFO for otherwise permissible uses on the basis that the SLT has previously used SLT funds to support the same or similar uses; and
 - For any recipient or subrecipient cost-sharing contribution.

- 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.

When Are Applications Due?

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.** Applications may be submitted before the deadline and early submission is encouraged. Applications received after the deadline date and time may not be considered eligible for consideration.

To facilitate processing, please submit Applications and supporting documentation via email to mohsgrants@dps.ms.gov.

What Do I Need to Do to Apply?

- The applicant must be eligible for funding.
- 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 compliant with NIMS Courses (100, 200,700 and 800). Applicants will be requested to show compliance, if awarded.
- Applicants must have a current and active Unique Entity Identification (UEI) number.
- Applicants must read and comply with 2 CFR 200.318 to 2 CFR 200.327 regulations.
- Applicants must have written procurement standards per 2 CFR 200.318(a).
- Applicants must have written conflict of interest standards per 2 CFR 200.318(c).
- Applicants read and understand 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.
- Applicants 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.
- The 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.

The following items must be submitted at the time of the Application, or the Application will be considered incomplete.

- Complete State and Local Cybersecurity (SLCGP) Application
- Agency Signatures
- UEI Certification, showing Active Date and UEI Number
- NIMS Certifications
- Most Recent Audit, if Applicable.
- Additional Justification, if applicable for the following items:
 - Items are over \$75,000.00

What If I Have Questions about the Grant Application?

The Mississippi Office of Homeland Security is always available to answer any questions regarding the Application packet and/or any grant questions.

Grant Writing Sessions:

The MOHS will hold two (2) virtual grant writing sessions to provide program updates, answer questions and assist in the development of the Applications.

Grant Writing Sessions for the State and Local Cybersecurity Grant Program

May 15, 2025 @ 10:00 a.m.
via Microsoft TEAMS

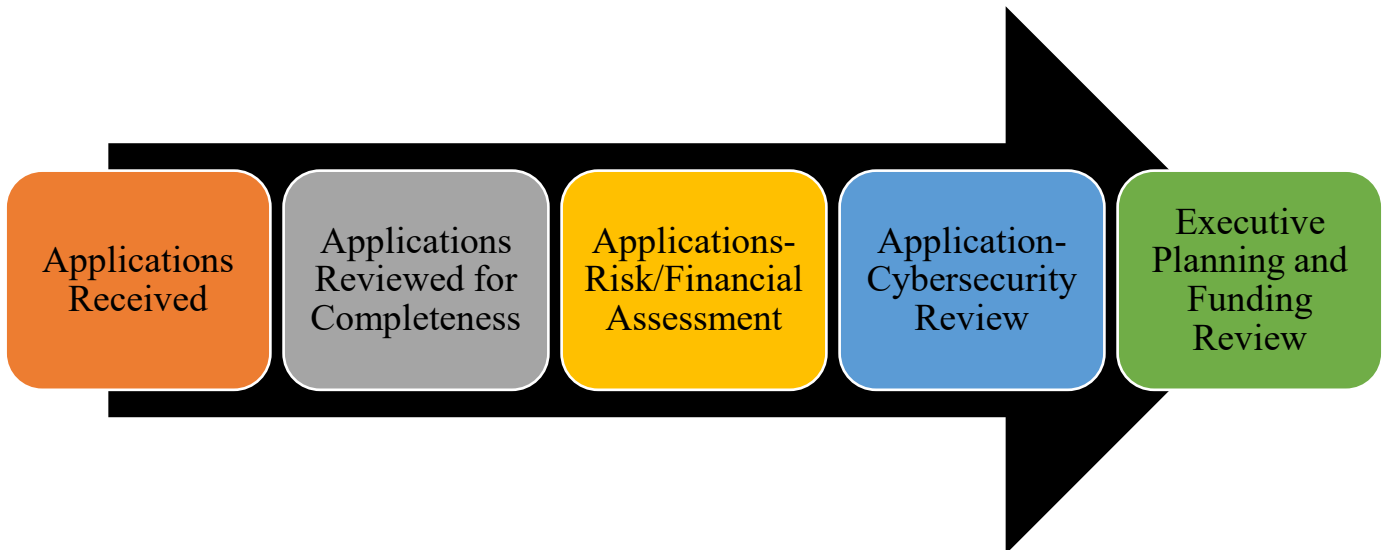
May 22, 2025 @ 10:00 a.m.
via Microsoft TEAMS

What Happens After the Application Is Submitted?

Each Application will go through a series of reviews for completeness, risk assessment, peer review, scoring and an executive planning and funding session. Please see below the stages of review for each Application that is received.

Please Remember:

- **Grants are based around the cybersecurity nexus, not IT/computer repair or programming.**
- **Funding is limited and grants are competitive.**



- Please prioritize projects and requests. Awards will be made in need of identifying how the need will assist the State in the MOHS mission and if funds are available.
- Fill out each section of the Grant Application in its entirety. Do not leave blank sections.
- Projects may be funded as a whole or partially funded.
- Please apply for what the agency NEEDS, not WANTS. If awarded, the Award will be made from approved items submitted with the Application. MODIFICATIONS will be limited during FY25.

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, MOHS staff will contact the agency to discuss opportunities.

If awarded during the review process, the Applicant will then become a Sub-Recipient and receive notice of an upcoming Grant Orientation meeting. The MOHS will provide updates of the grant, award packet information, grant forms, information on required reporting and closeout. A grant award packet will be sent to the sub-grantee for the review and the attainment of signatures from all authorized signatory officials.

Grant funds cannot be spent or requested until the Sub-Recipient has submitted all required award documentation. Costs/Expenses purchased before the executed agreement will be disallowed. Contracts entered before the period of performance begins will be disallowed.

Completing the Grant Application

Agency Applicant Information:

Applicant Details:

- Date: Date of Application Submission.
- Name of Agency: Full name of the Agency.
- Mailing Address: Full mailing address of the Agency.
- County of Agency: Name of the county where the Agency resides.
- Agency Contact Name: Name of the person that is responsible for filling out the Application.
- Agency Contact Phone Number: Phone number that can best reach the agency contact.
- Agency Contact Email Address: Email Address that can best reach the agency contact.
- Signatory Authorized Official Name: Name of the Mayor, Board President, Commissioner or Head of Agency.
- UEI Number: Twelve (12) Numeric and Digit code set up in SAMS.gov. Check with the finance clerk for this number.
- UEI Expiration Date: Date that the UEI Number is set to expire for the year.
- Congressional District: Congressional district where the agency resides.



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 Office Name			
<i>(Name of Mayor, Board President, Commissioner, Head of Agency, etc.)</i>			
Signatory Authorized Email Address			
UEI Number		Expiration Date	
<i>* Please provide a copy of UEI number and current status, as shown in SAM.gov.</i>			
Congressional District			

Grant Applicant funding Request by Cost Category:

- Contractual Services: List of the total amount requested for contractual services.
- Equipment: List of the total amount of equipment requested.
- Commodities/Supplies: List of the total amount requested for commodities/supplies.
- Training: List the total amount requested for training.
- Other: Any expenses that fall outside the other categories, should be included in the “Other” category.
- Total Grant Amount Requested: Add all sections for the total grant amount requested.

Grant Applicant Funding Request By Cost Category	
Cost Category	Amount Requested
Contractual Services	
Equipment	
Commodities/Supplies	
Training	
Other	
Total of Grant of Grant Amount Requested	

**Problem Identification & Description:
Agency Cybersecurity Information:**

Please provide responses to the following questions.

- 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?
- If assessment was completed, was the proposed project being applied for, identified as a Vulnerability or Gap?
- Does your agency currently have Cybersecurity Insurance?
- Does your Agency have written cybersecurity policies that all employees must consent and abide by?

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?	<input type="checkbox"/>	Yes	<input type="checkbox"/>	No
If assessment was completed, was the proposed project being applied for, identified as a Vulnerability or Gap?	<input type="checkbox"/>	Yes	<input type="checkbox"/>	No
Does your agency currently have Cybersecurity Insurance?	<input type="checkbox"/>	Yes	<input type="checkbox"/>	No
Does your Agency have written cybersecurity policies that all employees must consent and abide by?	<input type="checkbox"/>	Yes	<input type="checkbox"/>	No

Agency Type:

Mark the the type of Agency that best fits the Applicant.

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

Proposed Project Description and Project Details

Each applicant should provide a detailed description of the project details and how the project will be implemented by the Agency.

Proposed Project Description and Project Details
Provide a detailed summary of the Project that the Agency will implement?
<p style="color: blue; font-weight: bold;">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?</p>

Cybersecurity Gaps, Vulnerabilities and Capabilities

Each applicant should provide detailed responses to the following questions centered around the Agency’s cybersecurity gaps, vulnerabilities and capabilities. Detailed information should be provided from real cybersecurity events, cybersecurity exercises and or cybersecurity assessment.

Cybersecurity Gaps, Vulnerabilities and Capabilities					
<i>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.</i>					
How was the Cybersecurity Gap/Vulnerability identified?					
<input type="checkbox"/>	Real Cybersecurity Event	<input type="checkbox"/>	Cybersecurity Exercise	<input type="checkbox"/>	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.

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 and 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?

Alignment with State and Local Cybersecurity Objectives

As part of the SLCGP, each project must address one of the four (4) cybersecurity objectives for the program. Please review the definitions with each objective and place a mark on the objective that fits your project the best.

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.

<input type="checkbox"/>	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.
<input type="checkbox"/>	Objective 2: Assessment and Evaluation: Understand their current cybersecurity posture and areas of improvement based on continued testing, evaluation and structured assessments.
<input type="checkbox"/>	Objective 3: Mitigation: Implement security protections commensurate with risk.
<input type="checkbox"/>	Objective 4: Workforce Development: Ensure organizations personnel are appropriately training in cybersecurity, commensurate with responsibility.

SLCGP Grant Budget Request:

Each applicant should review the Agency Gap(s)/Vulnerabilities to request the budget fund requests that will fit the agencies **NEED**. Funding is **VERY** limited and should be requested based on need and priority of the request. All information provided in the Grant Budget Request sections is a request. There are no guarantees for funding. Funding may be partial or adjusted to coincide with grant funding available. All items requested **MUST** be justifiable by the cybersecurity gap, vulnerability and to increase capability.

Contractual Services: Include a detailed assessment of contractual services within the program area in which Applicants will be applying. Also, include a cost estimate for all contractual needs (rental, shipping costs, etc.). All expenses must be in accordance with current state and federal guidelines. **One (1) year of funding is allowable. Multiple years for services will not be considered.**

CONTRACTUAL SERVICES			
<i>Contractual Services should be requested for one (1) year of service only. All expenses must be in accordance to current state and federal guidelines. Agency should be prepared to be able to continue contractual services, if future awards or services are not approved.</i>			
Type of Contractual	Amount of Service	Quantity of Service	Total
			\$0.00
			\$0.00
			\$0.00
			\$0.00
			\$0.00
TOTAL CONTRACTUAL SERVICES			\$0.00

Cybersecurity Equipment: All Equipment must be allowable, reasonable and must be essential to the closing of the preparedness gap. All equipment must be included on the FEMA Authorized Equipment List. Unallowable equipment is provided above within the Funding Guidance. (See guidance above for more information). AEL Numbers **must be included** in the Application. Funding must be tied to Equipment must be essential to the program. The FEMA AEL List can be located at the following link: <https://www.fema.gov/grants/tools/authorized-equipment-list>

*If Equipment requires additional justification for consideration, please provide with the Application at the time of submission. If equipment requires additional justification and is not provided, the items may not be considered or items may be awarded at reduced program allocations, such as mobile radios.

**If additional spaces are needed for equipment, please add an additional page to the Application.

Cybersecurity Equipment				
<i>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 <u>MUST</u> be for cybersecurity based programs and activities. (See Funding Guidance for more information).</i>				
FEMA AEL Number:	Description of Equipment:	Item Cost	Quantity	Equipment Total:
				\$0.00
				\$0.00
				\$0.00
				\$0.00
				\$0.00
				\$0.00
				\$0.00
				\$0.00
Total Cost of Equipment				\$0.00

Training/Workforce Development: 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			
<i>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.</i>			
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

If training/workforce development training is being requested for the Agency, please describe how the training/certification program will reduce gaps(s)/vulnerabilities and increase Agency capability.

<p>How will the requested training/certifications program reduce the Gap(s)/Vulnerabilities and increase Agency capability?</p>
<p>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.</p>

Other Expenses: 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.

Other Expenses:			
<i>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.</i>			
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

Total Amount Request for Cybersecurity Funds: Please include a total of all budget sections for a total of the funding being requested.

Total Amount Request for Cybersecurity Funds	\$0.00
---	---------------

Sustainability of Project

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. Provide detailed responses to the following questions.

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:

Please mark Applicants' responses by a Yes or No response. Complete all sections.

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

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 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.

AGENCY AUDIT	
<p>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.</p>	
<input type="checkbox"/>	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.
<input type="checkbox"/>	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.

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 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.