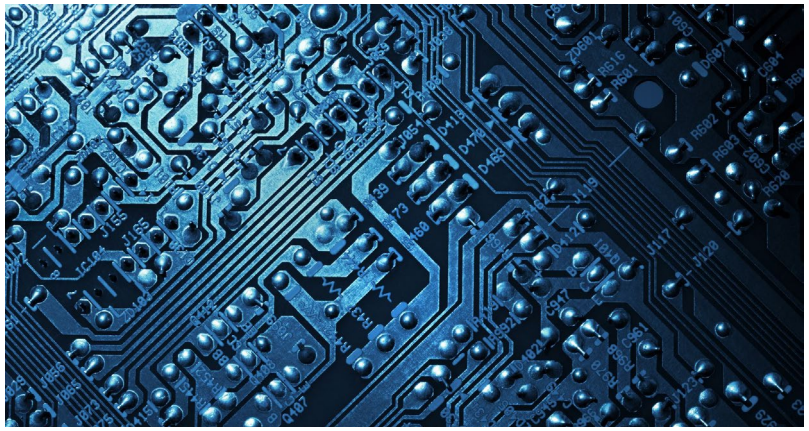
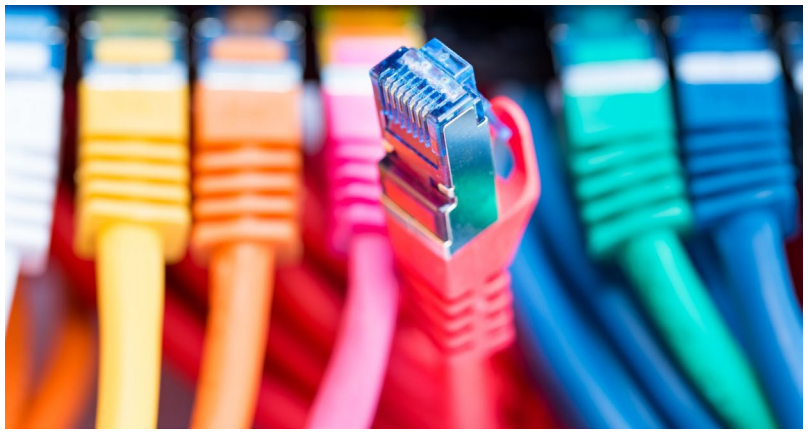
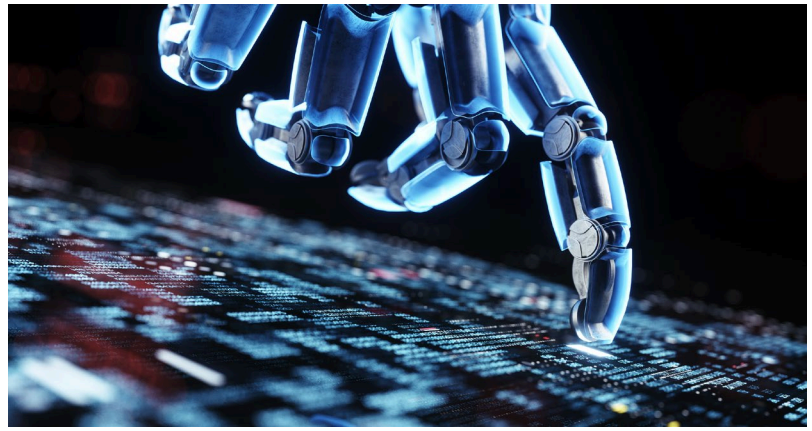
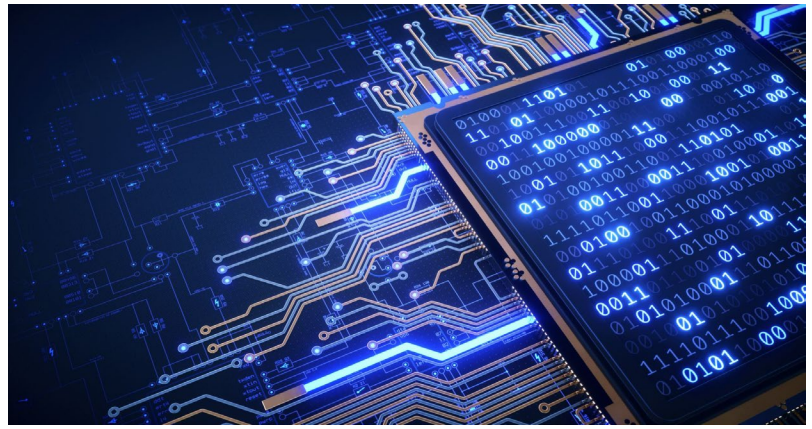








Mississippi Office of Homeland Security
State and Local Cybersecurity Grant
2026 Grant Writing Session

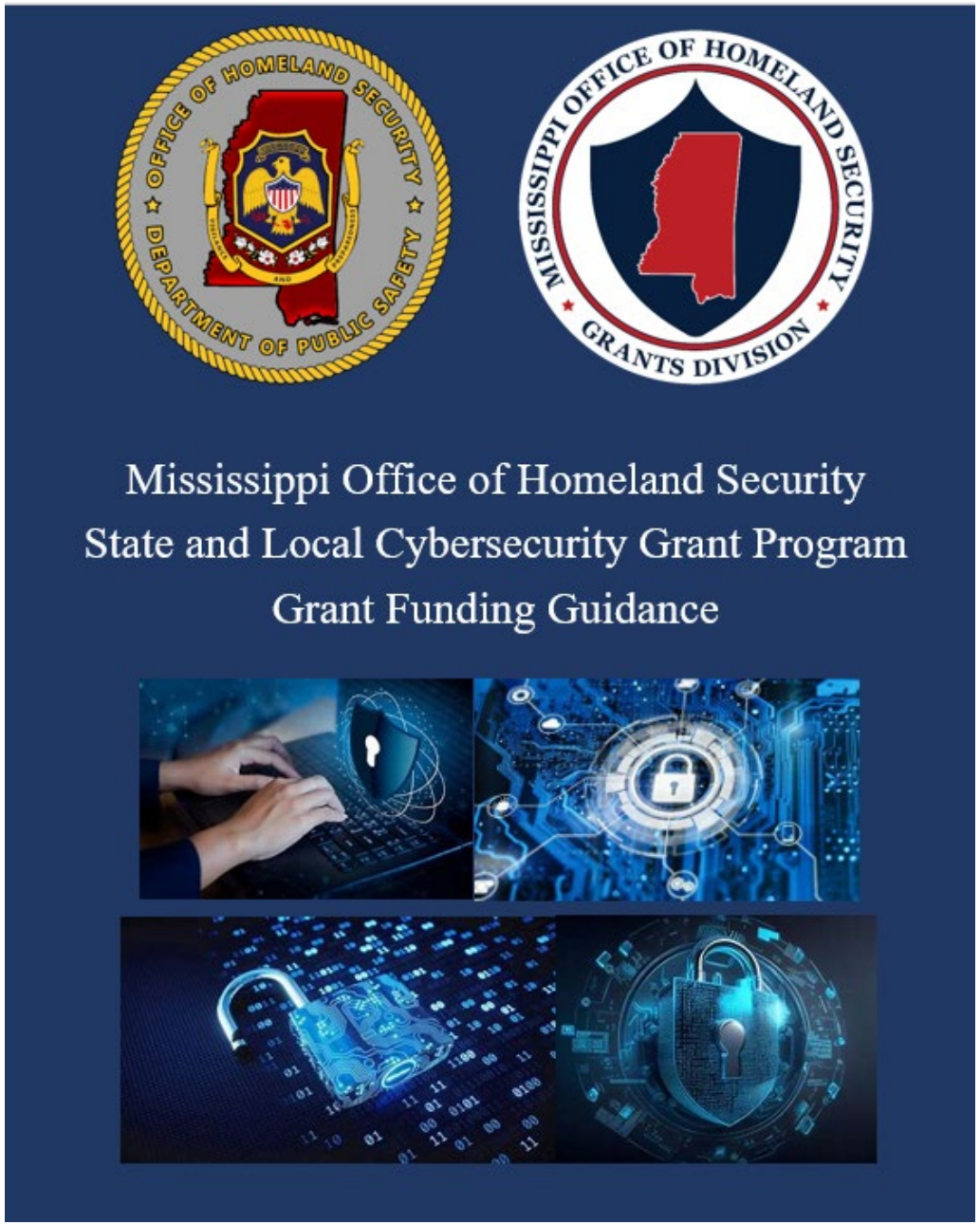
Welcome and Introductions

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

Bobby Freeman-MS Office of Homeland Security Cybersecurity Director

State and Local Cybersecurity Grant Program

Information about the Federal SLCGP Grant Program



In the State and Local Cybersecurity Grant Program Funding Guidance, information is provided to fill out the SLCGP 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 Grant Application	January 5, 2026
SLCGP Grant Application Release	January 15, 2026
Grant Writing Sessions (Virtual)	January 28, 2026 @ 9:00 a.m. February 10, 2026 @ 9:00 a.m.
Application Deadline	February 27, 2026, by 5:00 p.m.
Application Review Period	March – April 2026 Initial Risk/Financial Assessment Review (March) Cybersecurity Review (March) Executive Award Review (March) FEMA Approvals (April)
Award Announcement	May 15, 2026 (Tentative)
Grant Orientation	May 2026
Grant Awards Released	At Implementation Meetings (Tentative)
Grant Packets Due	June 15, 2026 (Tentative)
Grant Performance Period	June 1, 2026-November 30, 2027

Federal Award Overview:

Department of Homeland Security

State and Local Cybersecurity Grant Program

Assistance Listing Number (Formerly CFDA) 97.137

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 2022-2025 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: $1,644,657.00

Total: $16,592,346.00 Total Funds

Important Application Information

Application Deadline:

All SLCGP applications and supporting documentation must be received by the Mississippi Office of Homeland Security offices by **February 27, 2026, by 5:00 p.m.**

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 a Memorandum of Understanding
- Submitted a Consent Form
- Batch 1, Batch 2 and Batch 3 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.

Follow all local; state and federal guidance for funds.

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 (if applicable)
- 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 4-7 *Potential Allowable SLCGP Projects

Allowable SLCGP Grant Items:

Allowable Costs may include the following funding areas:

- Contractual Services
- Equipment
- Commodities/Supplies
- Training
- Other Items

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.

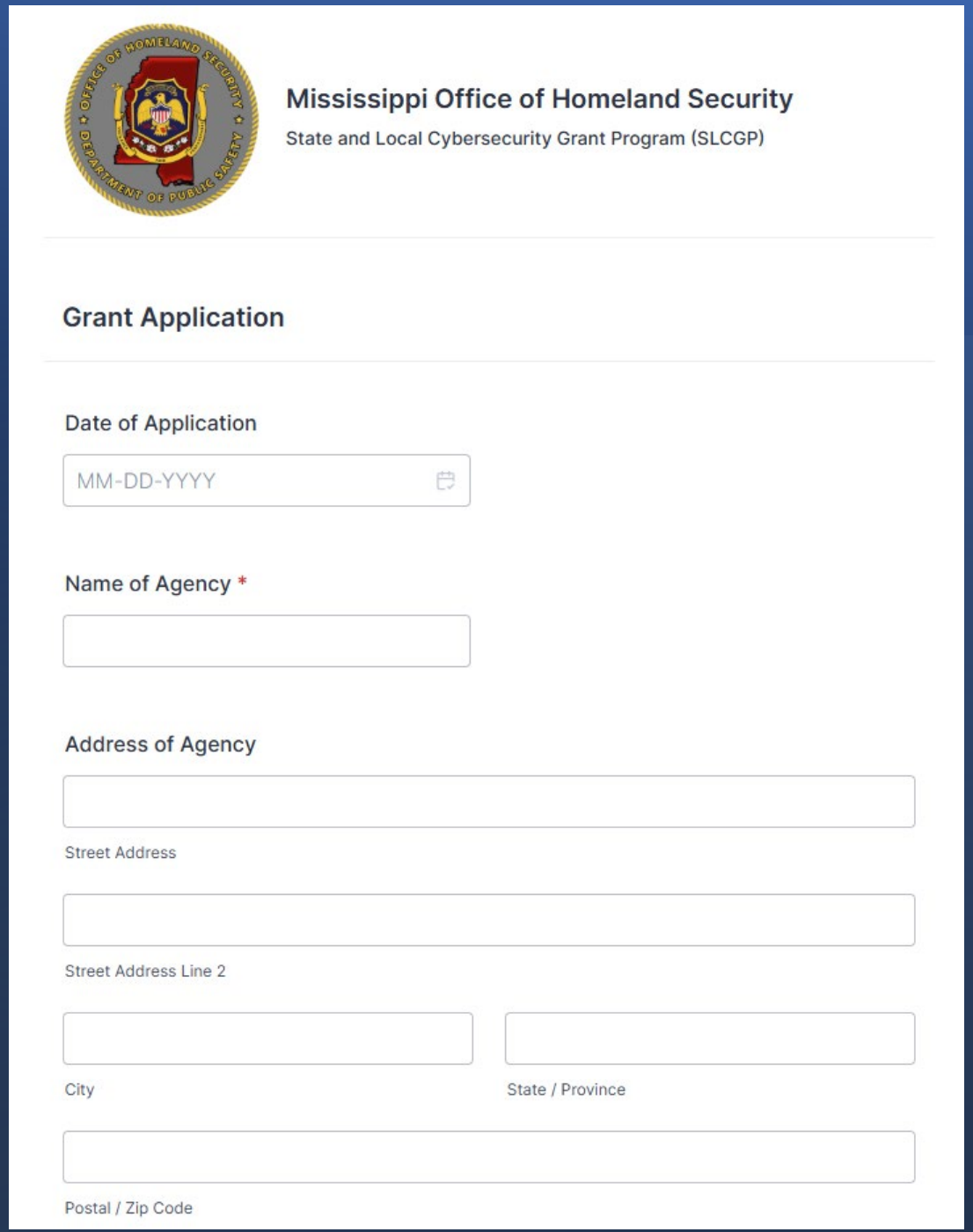
All items MUST be NEW planned items. Items can not have already purchased for the entity. Can not replace already purchased items with local funds and replace with federal funds.

Prohibited SLCGP Grant Items:
Funding Guidance: Page 9

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

MM-DD-YYYY

Name of Agency *

Address of Agency

Street Address

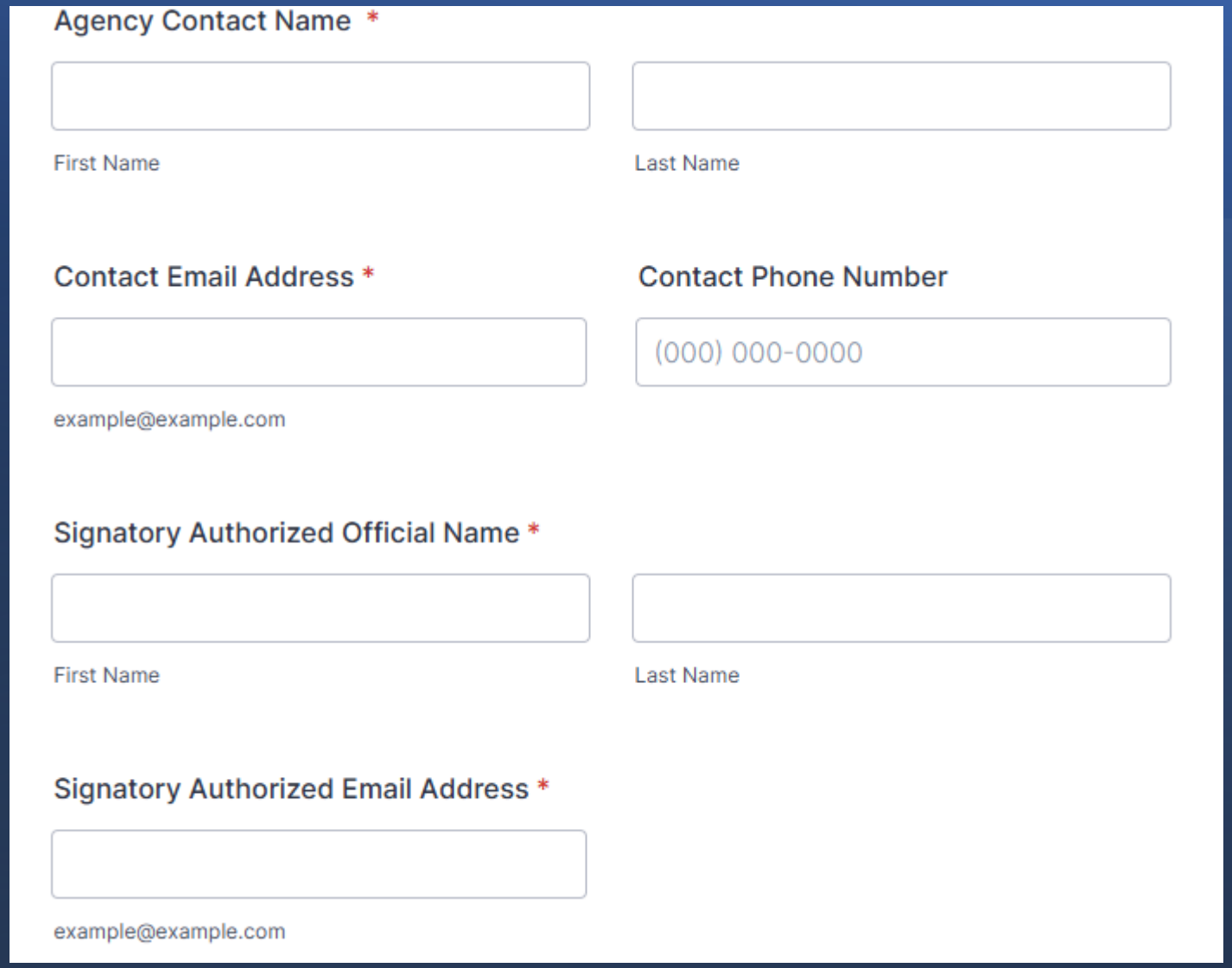
Street Address Line 2

City

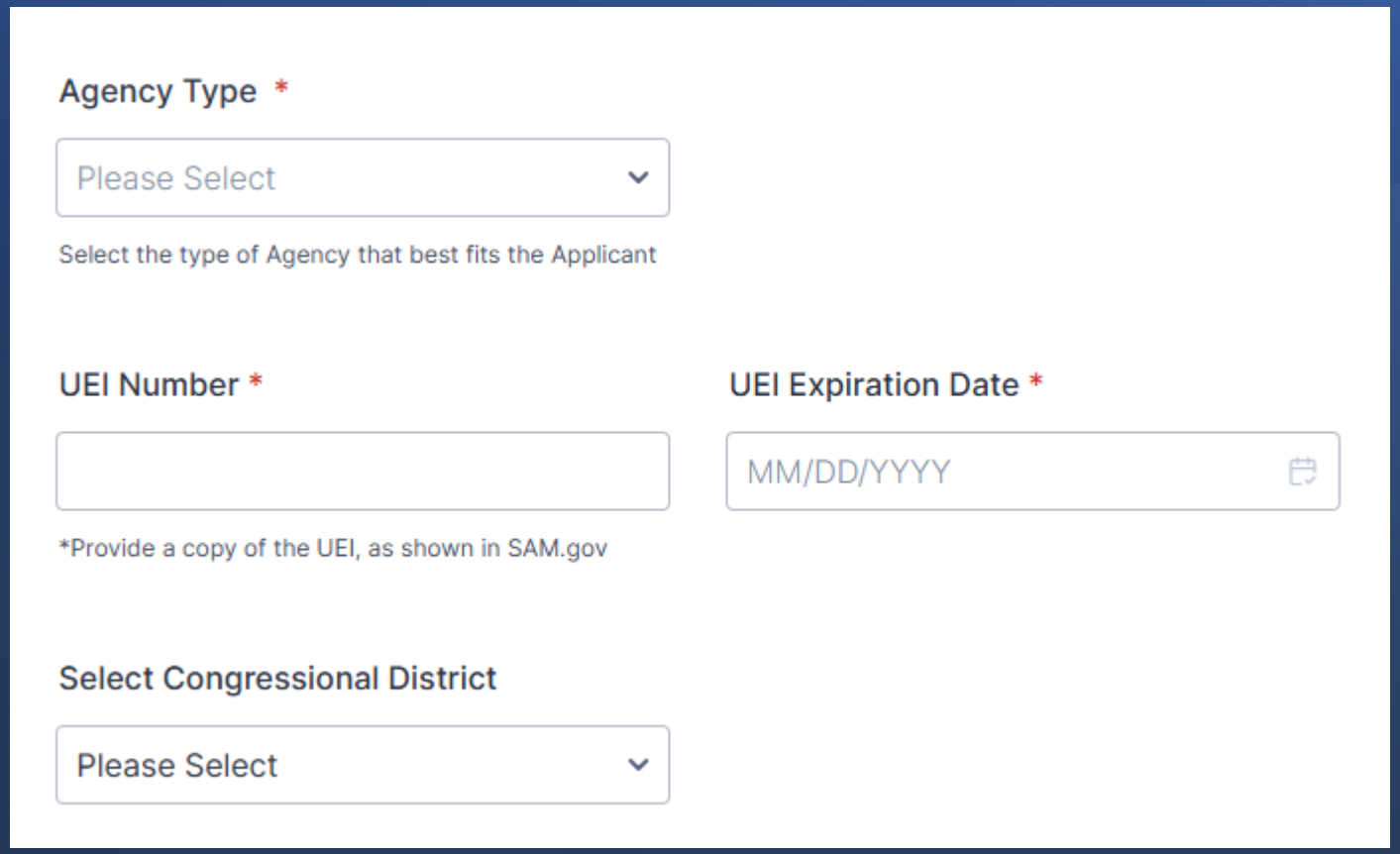
State / Province

Postal / Zip Code

Information and Contact Page



Contact Information and Signatory Authorized Official



Agency Type
UEI Number
UEI Exp. Date
Congressional District

NIMS COMPLIANCE

As part of the SLCGP Grant Application process, each agency MUST provide a copy of the NIMS Compliance certifications. The NIMS Certifications 100, 200, 700, and 800 for one agency member. If an agency member needs to complete this training, they can visit **FEMA's Training Website**.

Documentation MUST be Uploaded at the time of Application submission. *

Browse Files

Drag and drop files here

All documents must be submitted in PDF format. Submit NIMS compliance documents using the following naming format: [Agency Name] NIMS 100 (e.g., MOHS NIMS 100). Agencies may combine all NIMS certifications into a single PDF is preferred.

NIMS Compliance is required. Someone from your Agency will need to have NIMS Certifications 100; 200; 700 and 800.

Please upload documents within the "File Attachment Box"

Grant Funding Request

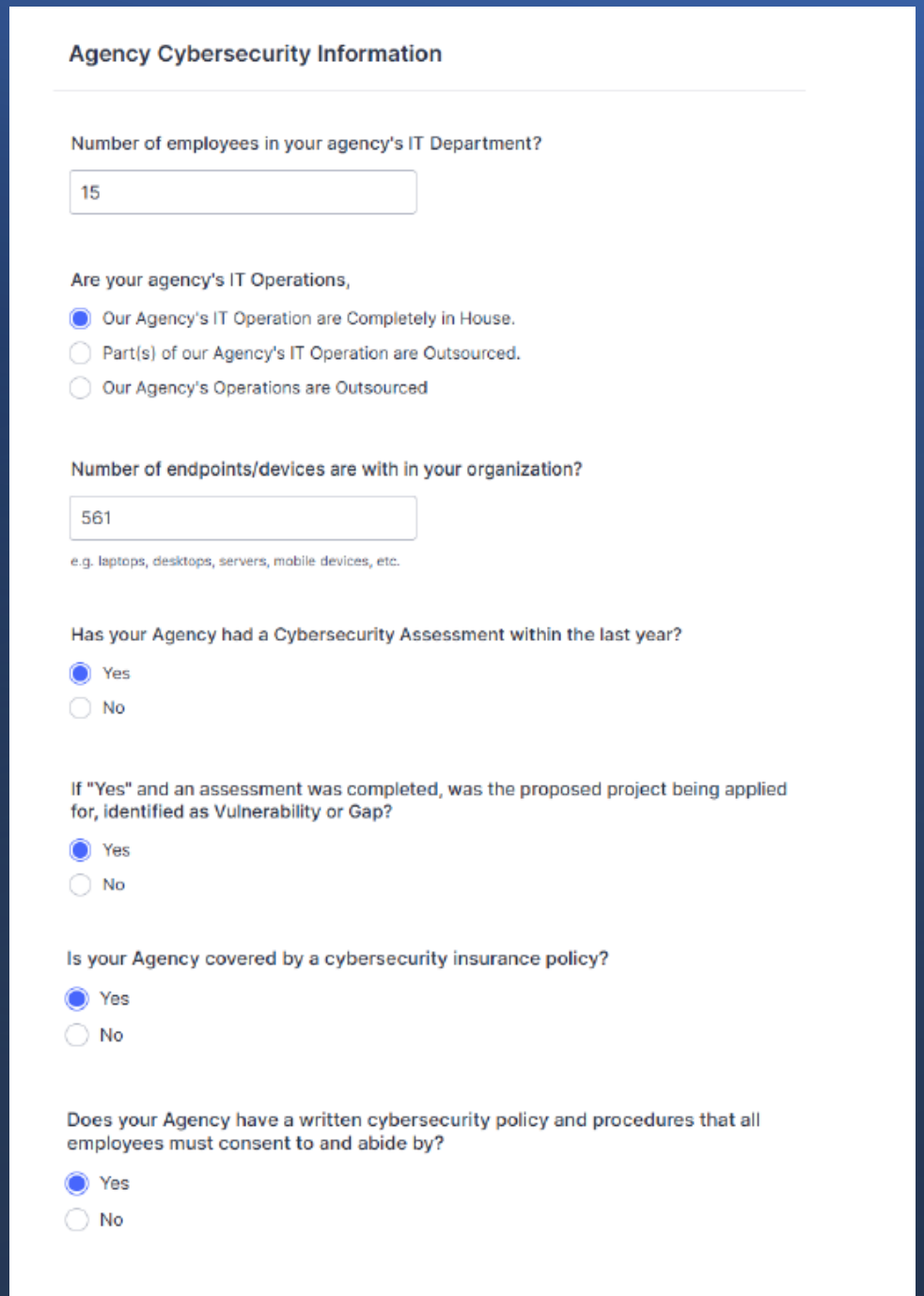
Grant Applicant Funding Request by Cost Category

	Amount Requested
Contractual Service	
Cybersecurity Equipment	
Training	
Other Expenses	

Total Application Funding Request:

$0

Problem Identification



Problem Identification

-Please Answer Each Question

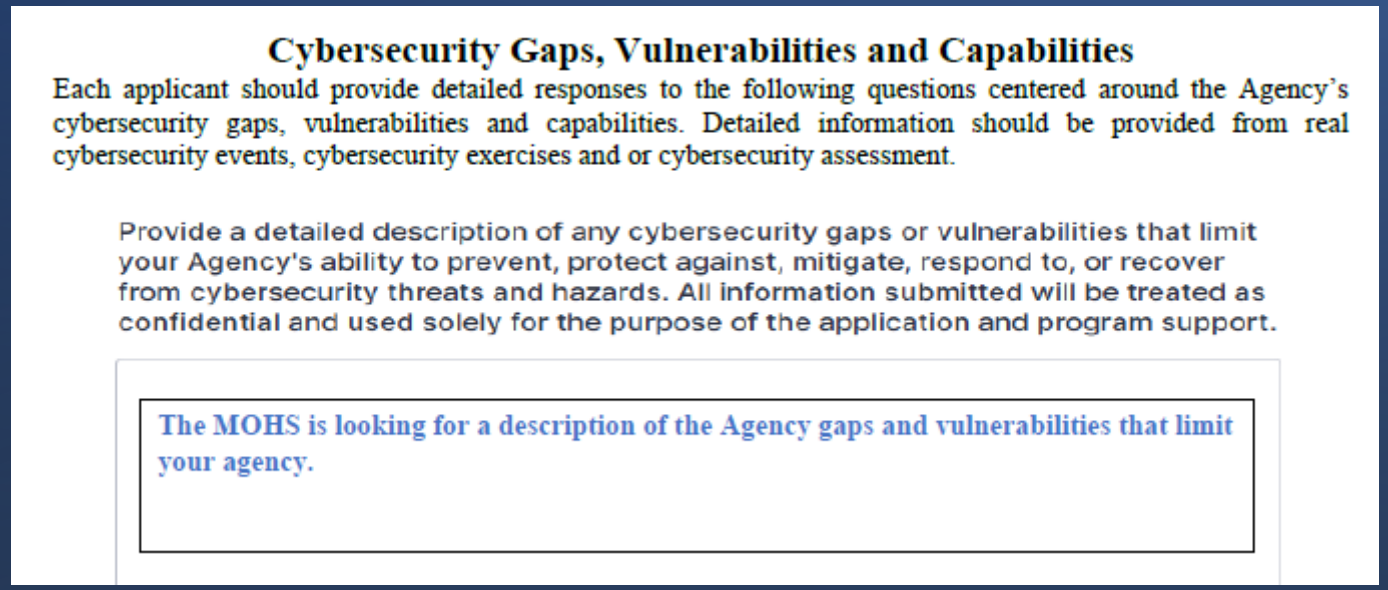
Proposed Project Description and Project Details

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

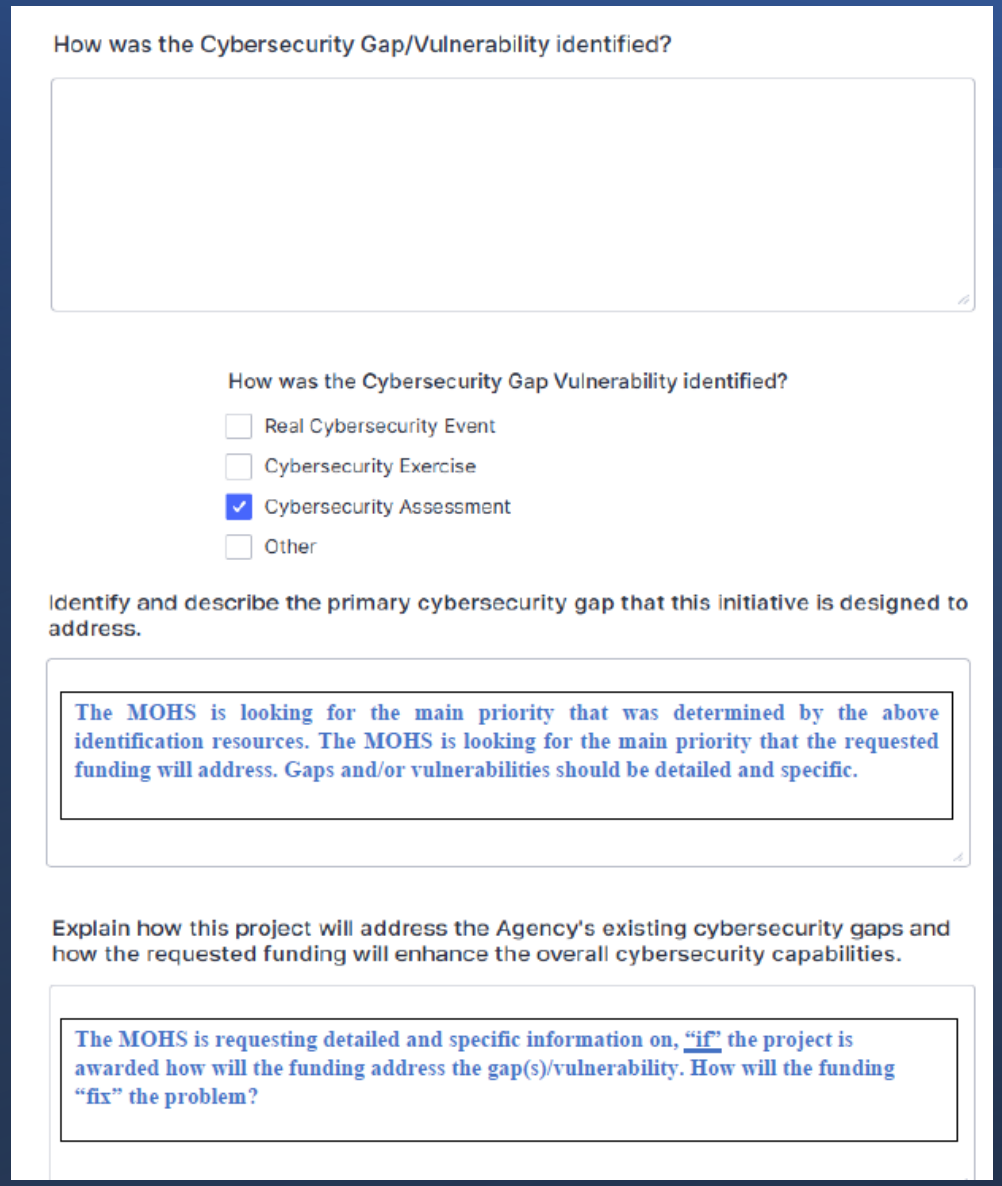
Each applicant should provide detailed responses to the following questions centered around the Agency's cybersecurity gaps, vulnerabilities and capabilities. Detailed information should be provided from real cybersecurity events, cybersecurity exercises and or cybersecurity assessment.

Provide a detailed description of any cybersecurity gaps or vulnerabilities that limit your Agency's ability to prevent, protect against, mitigate, respond to, or recover from cybersecurity threats and hazards. All information submitted will be treated as confidential and used solely for the purpose of the application and program support.

The MOHS is looking for a description of the Agency gaps and vulnerabilities that limit your agency.

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.

Gaps, Vulnerabilities and Capabilities



How was the Cybersecurity Gap/Vulnerability identified?

How was the Cybersecurity Gap Vulnerability identified?

- [ ] Real Cybersecurity Event
- [ ] Cybersecurity Exercise
- [x] Cybersecurity Assessment
- [ ] Other

Identify and describe the primary cybersecurity gap that this initiative is designed to address.

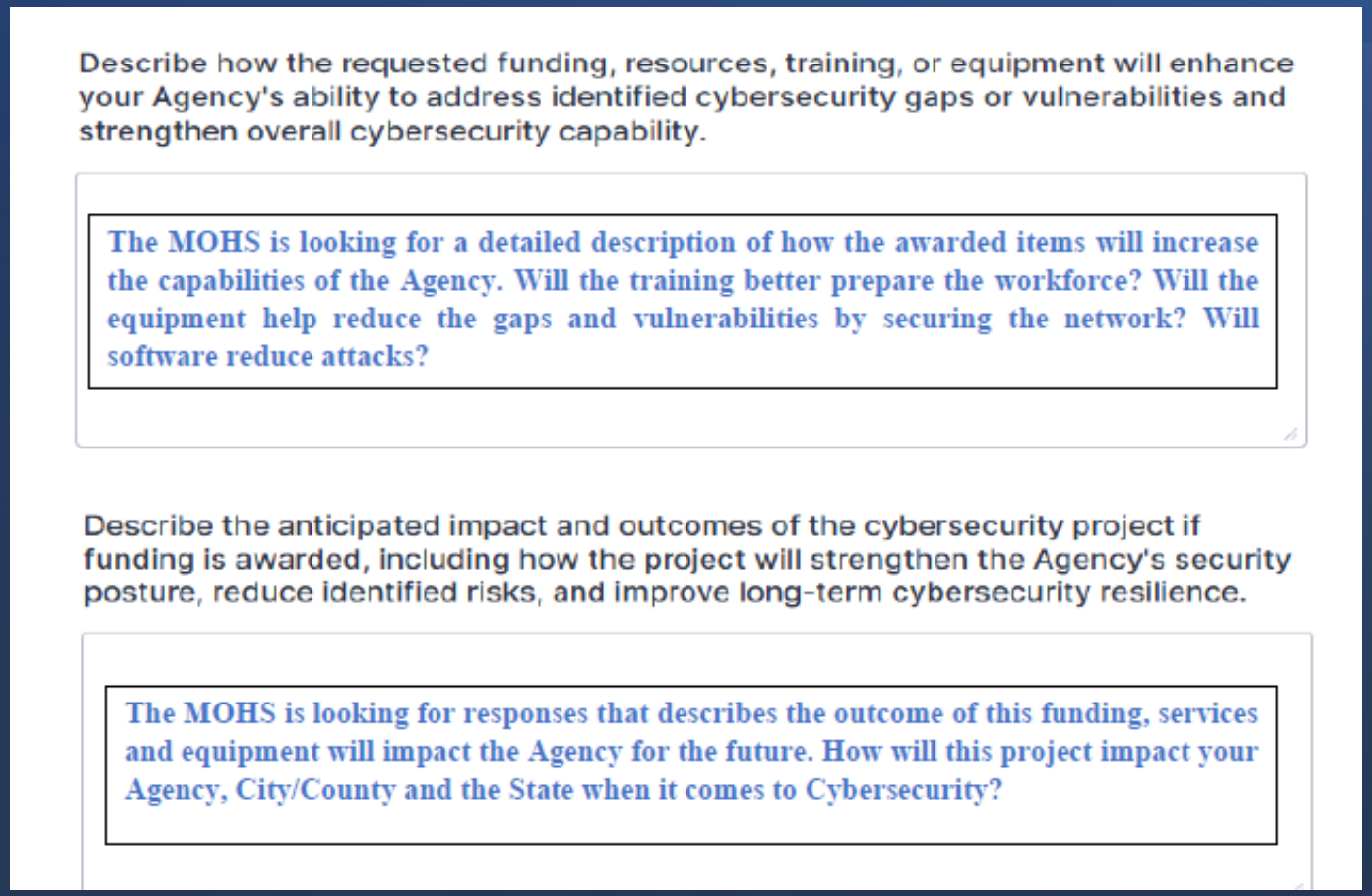
The MOHS is looking for the main priority that was determined by the above identification resources. The MOHS is looking for the main priority that the requested funding will address. Gaps and/or vulnerabilities should be detailed and specific.

Explain how this project will address the Agency's existing cybersecurity gaps and how the requested funding will enhance the overall cybersecurity capabilities.

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?

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.

Gaps, Vulnerabilities and Capabilities



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 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.

Applicants are required to address how the potential project will align with the State and Local Cybersecurity Grant Program (SLCGP) Grant Program Objectives. Please mark the OBJECTIVE that will best fit the Agency's 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

Contractual Services Budget

	Contractual Service	Amount of Contractual Service	Quantity of Contractual Service	Total of Contractual Service
Service 1				
Service 2				
Service 3				
Service 4				
Service 5				

Total for Contractual Services

$0

Please place the services within the provided chart, along with the Amount and Quantity.

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 5-8

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).

Equipment Budget

Cybersecurity Equipment Budget

	FEMA AEL	Description	EQ Cost	EQ Quantity	EQ Total
EQ 1					
EQ 2					
EQ 3					
EQ 4					
EQ 5					

Total for Cybersecurity Equipment

$0

Please include the AEL Number; Description; Costs and Quantity.

Training/Workforce Development

Training/Workforce Development Budget

	Training Name	Training Cost	Training Quantity	Training Total
Training 1				
Training 2				
Training 3				
Training 4				
Training 5				

Total for Training/Workforce Development Budget

$0

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

Explain how the requested trainings and certifications programs will reduce identified cybersecurity gaps or vulnerabilities and how they will enhance the Agency's overall capability to protect, detect, and respond to cyber threats.

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 Budget

	Item Name	Item Cost	Item Quantity	Item Total
Other Expense 1				
Other Expense 2				
Other Expense 3				
Other Expense 4				
Other Expense 5				

Total for Other Expenses Budget

$0

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.

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 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.

Would the Agency be able to implement the requested budget items without the support of the State and Local Cybersecurity Grant Program (SLCGP) funding, or are these investments dependent on grant assistance to move forward?

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.

Describe how the Agency will sustain and continue any goods, services, or capabilities acquired through federal grant funding once the Period of Performance has ended.

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?

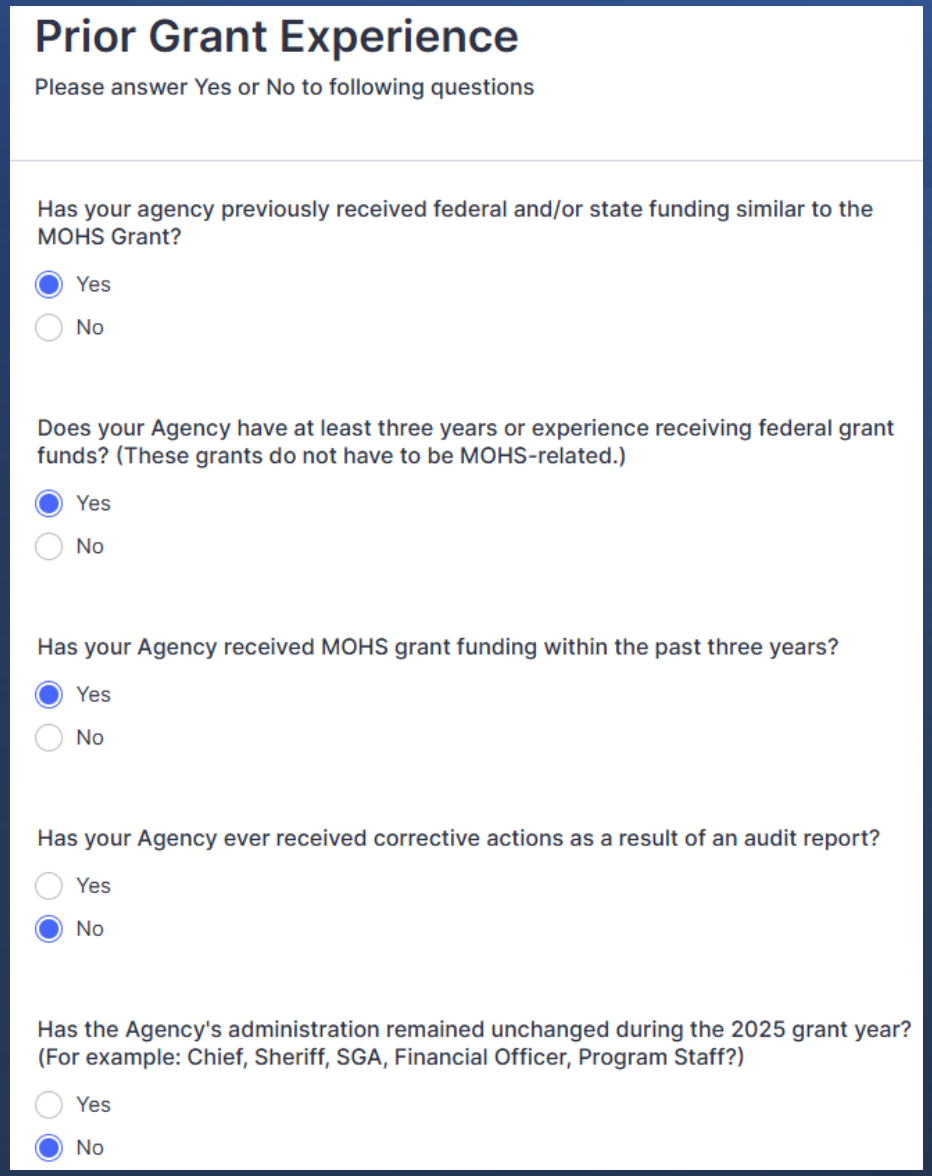
Has the Agency established a plan to sustain and advance cybersecurity improvements independently, without relying on State and Local Cybersecurity Grant Program (SLCGP) funding?

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?

Sustainability:

Provide as much detail as possible on the plans for the sustainability and future of the Cybersecurity program.

Prior Grant Experience:



Prior Grant Experience

Please answer Yes or No to following questions

Has your agency previously received federal and/or state funding similar to the MOHS Grant?

- (●) Yes
- ( ) No

Does your Agency have at least three years or experience receiving federal grant funds? (These grants do not have to be MOHS-related.)

- (●) Yes
- ( ) No

Has your Agency received MOHS grant funding within the past three years?

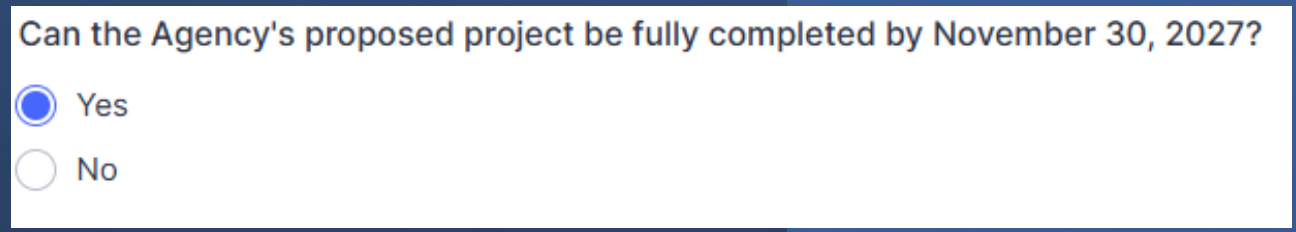
- (●) Yes
- ( ) No

Has your Agency ever received corrective actions as a result of an audit report?

- ( ) Yes
- (●) No

Has the Agency's administration remained unchanged during the 2025 grant year? (For example: Chief, Sheriff, SGA, Financial Officer, Program Staff?)

- ( ) Yes
- (●) No



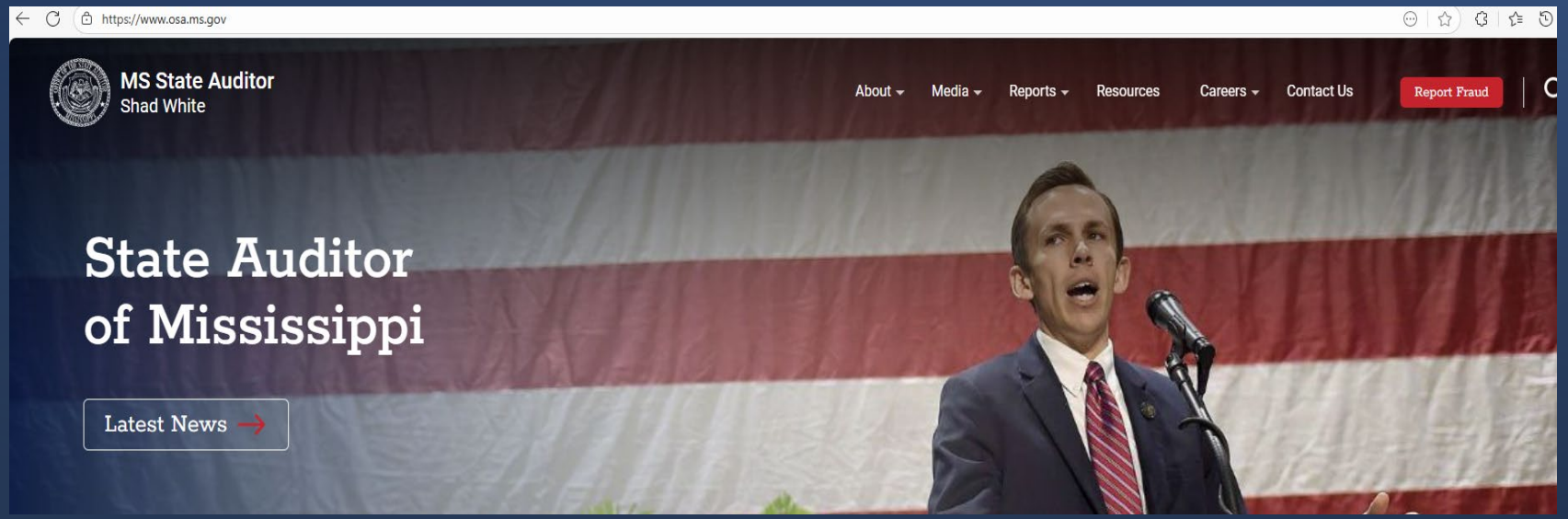
Can the Agency's proposed project be fully completed by November 30, 2027?

- (●) Yes
- ( ) No

Agency Audit:

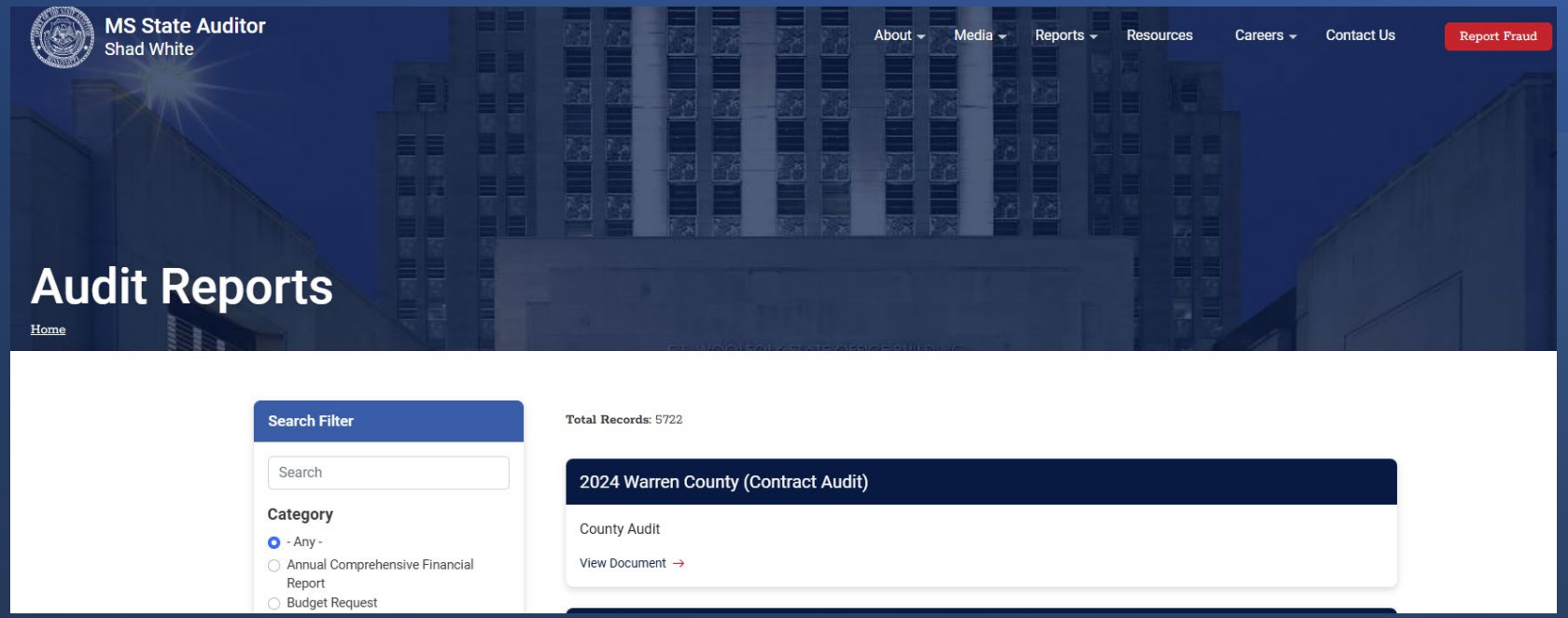
Easy Way to find Audits…….

Visit the Mississippi State Auditor's Website.



Go to the Reports Tab on the front page. Drop Down Box will give you option. Pick **Audit Reports**.

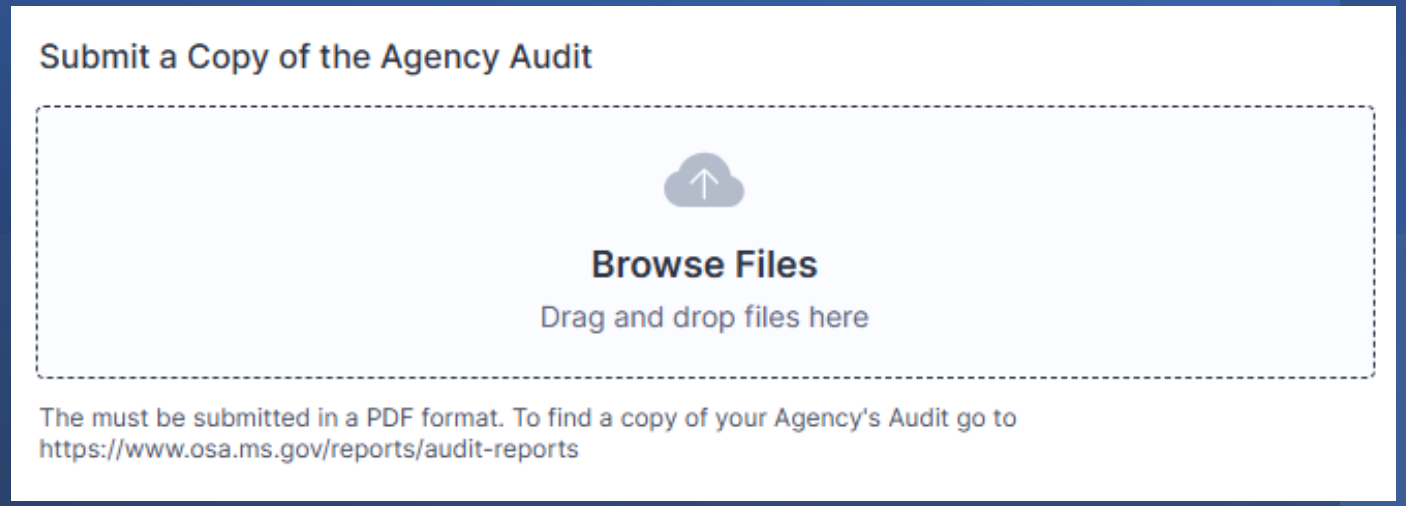
Agency Audit:



Type in City/County or School District into the Search Section.

Once results are found, the agency can them save the most recent audit for their file, as well as be able to submit the audit to meet the MOHS grant requirement.

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.

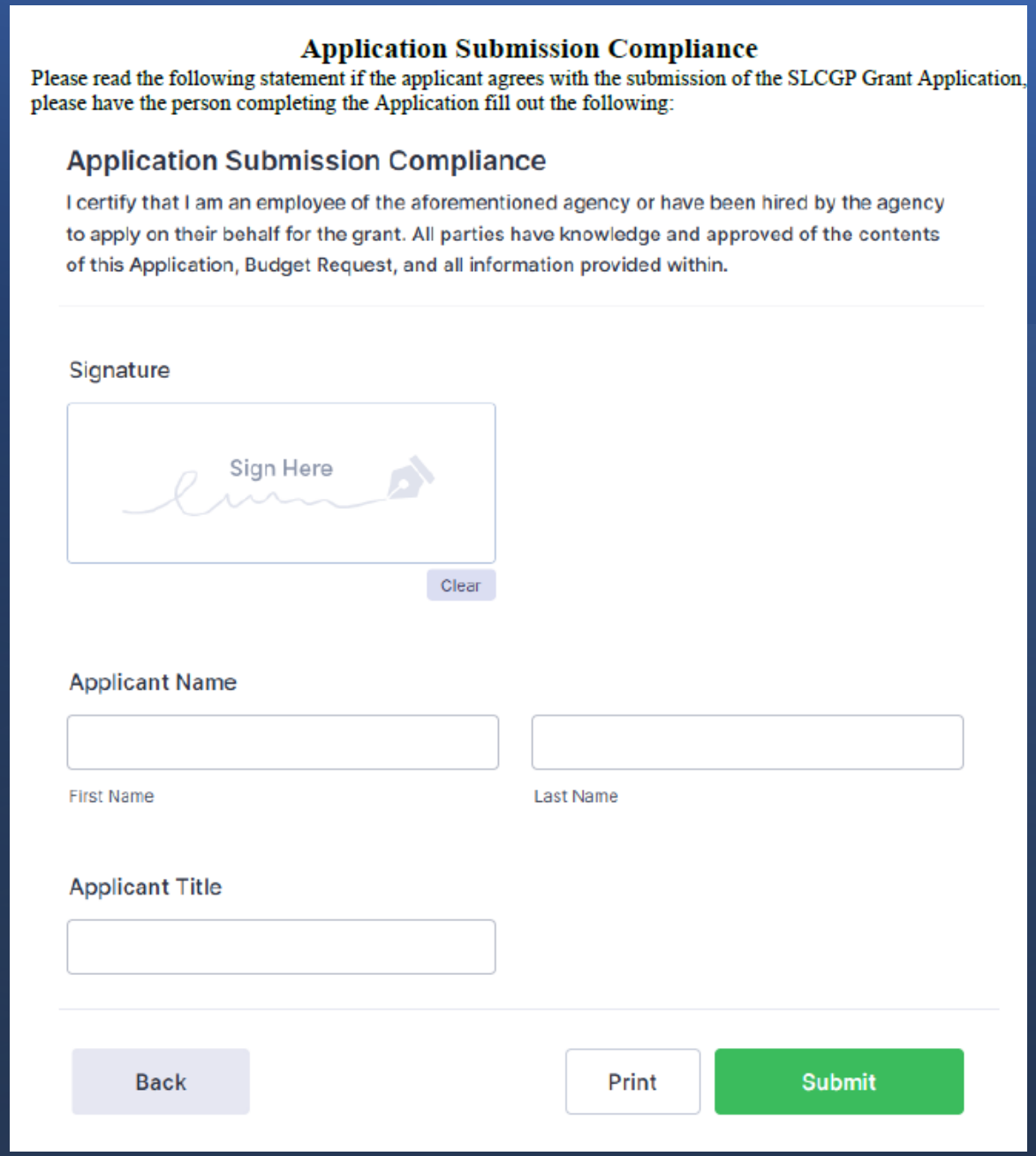
Agency Audit:

I certify that the Applicant's associated city/county/organization does NOT expect, to be required to have an audit performed under 2CFR Part 200, Subpart F, for the above listed program.

- [x] Yes
- [ ] No

I certify that the Applicant's associated city/county/organization WILL BE required, to be required to have an audit performed under 2CFR Part 200, Subpart F. A copy of the audit report MUST be submitted at the time of this Application Submission.

- [ ] Yes
- [ ] No



Application Signatures and Submission Box.

Please electronically sign the document, as well as put the printed name and title.

Before Submission, please double check your responses.

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 **February 27, 2026**, at 5:00 p.m.

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

NIMS Certifications (100; 200; 700 and 800)

National Incident Management System (FEMA)

Per FEMA, The National Incident Management System (NIMS) guides all levels of government, nongovernmental organizations and the private sector to work together to prevent, protect against, mitigate, respond to and recover from incidents.

NIMS provides stakeholders across the whole community with the shared vocabulary, systems and processes to successfully deliver the capabilities described in the National Preparedness System. NIMS defines operational systems that guide how personnel work together during incidents.

Certificates will be required as part of the HSGP Grant and will be requested for review during MOHS Monitoring.

- ICS-100: Introduction to the Incident Command System

  ICS 100, Introduction to the Incident Command System, introduces the Incident Command System (ICS) and provides the foundation for higher level ICS training. This course describes the history, features and principles, and organizational structure of the Incident Command System. It also explains the relationship between ICS and the National Incident Management System (NIMS).

- ICS-200: ICS for Single Resources and Initial Action Incidents

  IS200, Basic Incident Command System for Initial Response, reviews the Incident Command System (ICS), provides the context for ICS within initial response, and supports higher level ICS training. This course provides training on, and resources for, personnel who are likely to assume a supervisory position within ICS.

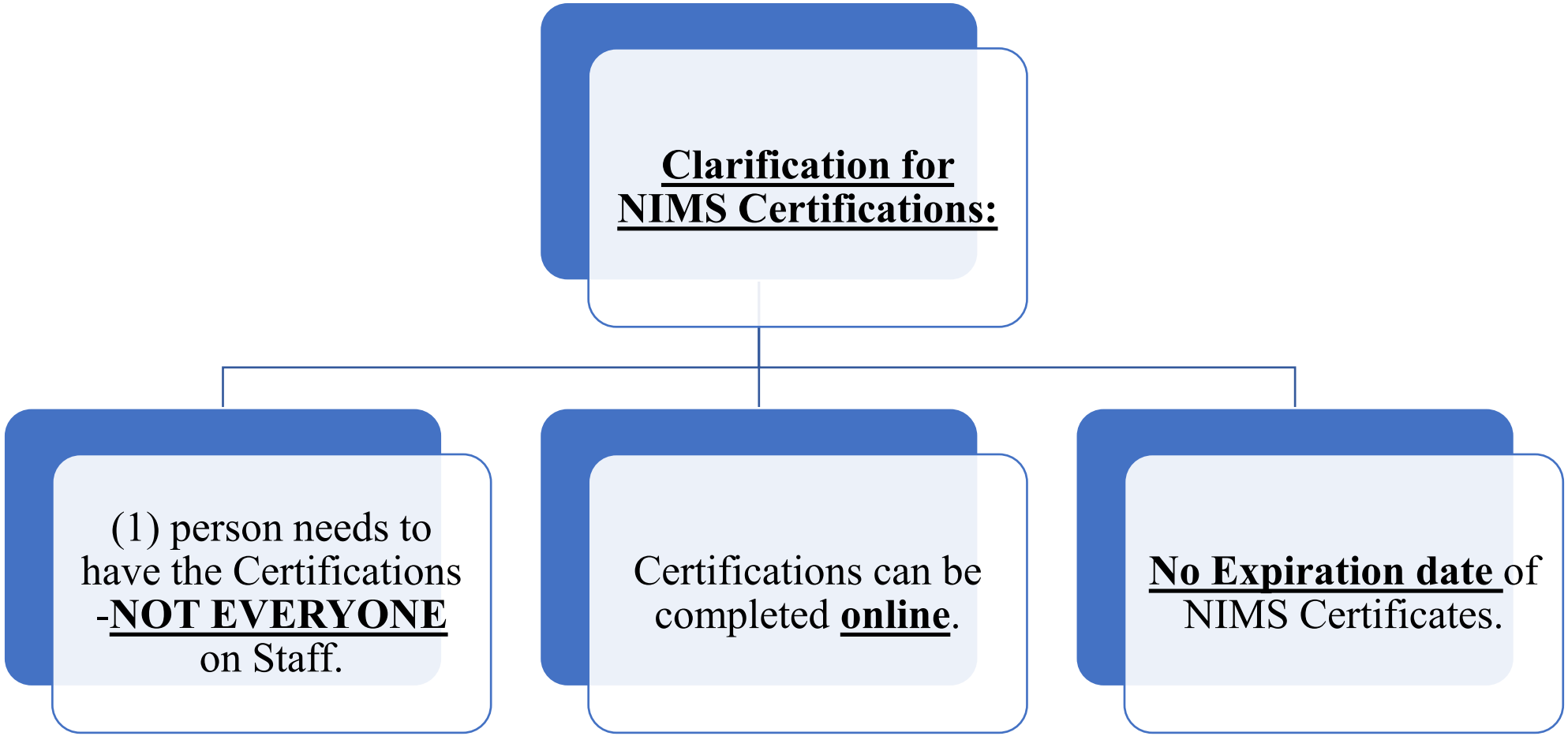
- IS-700: National Incident Management System, An Introduction

  This course provides an overview of the National Incident Management System (NIMS). The National Incident Management System defines the comprehensive approach guiding the whole community - all levels of government, nongovernmental organizations (NGO), and the private sector - to work together seamlessly to prevent, protect against, mitigate, respond to, and recover from the effects of incidents. The course provides learners with a basic understanding of NIMS concepts, principles, and components.

- IS-800: National Response Framework, An Introduction

  The goal of the IS-0800.d, National Response Framework, An Introduction, is to provide guidance for the whole community. Within this broad audience, the National Response Framework focuses especially on those who are involved in delivering and applying the response core capabilities.

NIMS Certifications (100; 200; 700 and 800)



Links for NIMS Certificates

FEMA - Emergency Management Institute (EMI) Course | IS-100.C: Introduction to the Incident Command System, ICS 100

FEMA - Emergency Management Institute (EMI) Course | IS-200.C: Basic Incident Command System for Initial Response, ICS-200

FEMA - Emergency Management Institute (EMI) Course | IS-700.B: An Introduction to the National Incident Management System

FEMA - Emergency Management Institute (EMI) Course | IS-800.D: National Response Framework, An Introduction

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!!

What Happens Next?

MOHS will review each application and start an internal Risk Assessment within the Grants/Finance Department.

Mississippi Cybersecurity Unit will review each application for a Peer Review.

At the end of the Reviews, the MOHS Executive Staff will review Applications and Budgets for Selection of Awards.

What Happens Next?

At the end of the Executive Review, a list of potential awards is developed.

MOHS prepared Request for Release of Funds and Approval documents for FEMA/CISA to review and approve.

Once FEMA/CISA approve potential projects, then the MOHS can notify all applicants of approvals or non-approvals.

What Happens Next?

Notifications will be submitted to ALL applicants for Award or Non-Award of grant funds.

Award Paperwork will be developed.

Implementation Meetings will be scheduled to go over Grant Logistics and program management.

SLCGP Grant Application Due to MOHS

Due February 27, 2026

By 5:00 p.m.

Questions