

STATE AND LOCAL CYBERSECURITY GRANT PROGRAM (SLCGP)

FY 2024 APPLICATION WORKSHOP



MISSOURI DEPARTMENT OF PUBLIC SAFETY(DPS) OFFICE OF HOMELAND SECURITY(OHS) SLCGP NOTICE OF FUNDING OPPORTUNITY(NOFO)

We are pleased to announce the funding opportunity for the FY 2024 State and Local Cybersecurity Grant Program (SLCGP) is open **October 18, 2024 – December 4, 2024 5:00 p.m. CST**

This funding opportunity is made available through the Missouri Department of Public Safety's, electronic WebGrants System, accessible online: <https://dpsgrants.dps.mo.gov>

- The Notice of Funding Opportunity (NOFO) can be accessed at the following link under Grant Applications and Forms:
<https://dps.mo.gov/dir/programs/ohs/grantstraining/>
- The NOFO contains information regarding the purpose/objectives of the program, eligibility, application requirements, allowable/unallowable costs, etc.

STATE AND LOCAL CYBERSECURITY GRANT PROGRAM (SLCGP)

- Our nation faces unprecedented cybersecurity risks, including increasingly sophisticated adversaries, widespread vulnerabilities in commonly used hardware and software, and broad dependencies on networked technologies for the day-to-day operation of critical infrastructure
- Cyber risk management is further complicated by the ability of malicious actors to operate remotely, linkages between cyber and physical systems, and the difficulty of reducing vulnerabilities

STATE AND LOCAL CYBERSECURITY GRANT PROGRAM (SLCGP)

- Considering the risk and potential consequences of cyber incidents, strengthening the cybersecurity practices and resilience of state, local, and territorial (SLT) governments is an important homeland security mission and the primary focus of the SLCGP
- Through funding from Infrastructure Investment and Jobs Act (IIJA), also known as the Bipartisan Infrastructure Law (BIL), the SLCGP enables Department of Homeland Security (DHS) to make targeted cybersecurity investments in state and local government agencies, thus improving the security of critical infrastructure and improving the resilience of the services state and local governments provide their community

STATE AND LOCAL CYBERSECURITY GRANT PROGRAM (SLCGP)

Missouri Cybersecurity Planning Committee

■ Vision:

To make Missouri safe, robust, and resilient, by strengthening Missouri's economic and public safety, while securing the confidentiality, integrity, and availability of Missouri's data

■ Mission:

To secure Missouri networks and data by providing governance and a framework to reduce cybersecurity risk by implementing national cybersecurity best practices

SLCGP KEY DATES

October 18, 2024:	SLCGP funding opportunity opens in WebGrants https://dpsgrants.dps.mo.gov/
December 4, 2024:	SLCGP applications due in WebGrants 5:00 pm CST <i>WebGrants will not accept any applications after this time</i>
December 2024/January 2025:	Cybersecurity Planning Committee application review/scoring
February 1, 2025:	Projected Project Start Date
January 31, 2028:	Projected Project End Date

OBJECTIVES

- The goal of the SLCGP is to assist state and local governments with managing and reducing systemic cyber risk
- Four Objectives
 - 1) 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
 - 2) Objective 2: Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments
 - 3) Objective 3: Implement security protections commensurate with risk
 - 4) Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility

Requested projects must align to at least one of the four objectives

OBJECTIVES

- **Objective I:** 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
 - Sub-objective 1.1 Establish cybersecurity governance structures and implement a program to evaluate maturity of the cybersecurity program aligned to Cybersecurity Performance Goals established by Cybersecurity and Infrastructure Security Agency (CISA) and the National Institute of Standards and Technology (NIST)
 - Sub-objective 1.2 Develop, implement, or revise, and test cybersecurity plans, including cyber incident response plans, with clearly defined roles and responsibilities
 - Sub-objective 1.3 Asset (e.g., devices, data software) protections and recovery actions are prioritized based on the asset's criticality and business value

Sub-objective Outcomes are listed in Appendix A of the FY 2024 SLCGP NOFO

OBJECTIVES

- **Objective 2:** Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments
 - Sub-objective 2.1 Physical devices and systems, as well as software platforms and applications, are inventoried
 - Sub-objective 2.2 Cybersecurity risk to the organization's operations and assets are understood
 - Sub-objective 2.3 Vulnerability scans are performed, and a risk-based vulnerability management plan is developed and implemented
 - Sub-objective 2.4 Capabilities are in place to monitor assets to identify cybersecurity events
 - Sub-objective 2.5 Processes are in place to action insights derived from deployed capabilities

Sub-objective Outcomes are listed in Appendix A of the FY 2024 SLCGP NOFO

OBJECTIVES

- **Objective 3:** Implement security protections commensurate with risk
 - Sub-objective 3.1 State and local agencies adopt fundamental cybersecurity best practices
 - Sub-objective 3.2 Reduce gaps identified through assessment and planning process and apply increasingly sophisticated security protections commensurate with risk

Sub-objective Outcomes are listed in Appendix A of the FY 2024 SLCGP NOFO

OBJECTIVES

- **Objective 4:** Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility
 - Sub-objective 4.1 Train personnel to have the fundamental knowledge and skills necessary to recognize cybersecurity risks and understand their roles and responsibilities within established cybersecurity policies, procedures, and practices
 - Sub-objective 4.2 Organization has adopted the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework

Sub-objective Outcomes are listed in Appendix A of the FY 2024 SLCGP NOFO

STATE PRIORITIES

- Missouri has established eight priority areas for FY 2024
 - The eight priority areas are cybersecurity best practices
 - 1) Implement multi-factor authentication
 - 2) Implement enhanced logging
 - 3) Data encryption for data at rest and in transit
 - 4) End use of unsupported/end of life software and hardware that are accessible from the internet
 - 5) Prohibit use of known/fixed/default passwords and credentials
 - 6) Ensure the ability to reconstitute systems (backups)
 - 7) Actively engage in bidirectional sharing between CISA and SLT entities in cyber relevant time frames to drive down cyber risk
 - 8) Migration to the .gov internet domain
- **Projects that align to State Priorities will receive additional points during the application scoring process**

FY 2024 ANTICIPATED FUNDING

- The Federal Notice of Funding Opportunity has estimated funding levels for the FY 2024 SLCGP for Missouri at **\$5,805,583**
- Three funding sources available for FY 2024 SLCGP:
 1. Rural – funds dedicated for entities encompassing a population of less than 50,000 people and/or has not been designated in the most recent decennial census as an “urbanized” area by the Secretary of Commerce
 - a. 25% of SLCGP funds must be provided to rural areas
 2. Non-Rural – funds dedicated for entities encompassing a population of greater than 50,000 people and/or has been designated in the most recent decennial census as an “urbanized area” by the Secretary of Commerce
 3. State – funds dedicated for state agency applicants

MAXIMUM AWARD

- The maximum award available is \$200,000 Federal share per applicant agency
- Applicant agencies are only allowed to submit **one project and objective per application**
 - A maximum of four applications, not to exceed \$200,000 cumulatively, will be allowed per applicant agency

MATCH REQUIREMENTS

- 30% Cost Share Requirement
 - Hard (Cash)
 - Soft (In-Kind) – If awarded, supporting documentation must be submitted to document match expenses
- Subrecipient contributions must be verifiable, reasonable, allocable, and necessary, and otherwise allowable under the grant program, and in compliance with all applicable federal requirements and regulations

MATCH REQUIREMENTS

- **Step 1:** Calculating Total Project Costs based on Federal Costs & Federal Share Percentage

$$\frac{\text{Federal Award Amount}}{\text{Federal Share Percentage}} = \text{Total Project Costs}$$

- **Step 2:** Calculating Subrecipient's Share Percentage

$$\text{Subrecipient's Share Percentage} \times \text{Project Costs} = \text{Required Match}$$

- **Example 1:** $\frac{\$100,000}{70\%} = \$142,857.14$ Total Project Costs

$$30\% \times \$142,857.14 = \$42,857.14 \text{ Subrecipient Cost Share}$$

- **Example 2:** $\frac{\$200,000}{70\%} = \$285,714.29$ Total Project Costs

$$30\% \times \$285,714.29 = \$85,714.29 \text{ Subrecipient Cost Share}$$

ELIGIBLE APPLICANTS

- Local governments as defined in 6 U.S.C. section 101(13)
 - A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments, regional or interstate government entity, or agency or instrumentality of a local government
 - A rural community, unincorporated town or village, or other public entity
- State units of government

NATIONWIDE CYBERSECURITY REVIEW (NCSR)

- To be eligible to receive SLCGP funding, the applicant agency must have completed the 2024 Nationwide Cybersecurity Review (NCSR).
 - The NCSR must be completed and results received at the time of application submission
 - The NCSR Completion Certificate MUST be uploaded in the Named Attachments Form of the application!
- The NCSR is a free, anonymous, annual self-assessment designed to measure gaps and capabilities of a state and local government's cybersecurity programs. It is based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework and is sponsored by DHS and the MS-ISAC. ****Please note: New user accounts will be created within 2-4 business days of completing the registration form. It may take approximately 4-6 hours to complete the NCSR and the agency should allow up to two weeks to receive the results. If your agency has previously completed the NSAR, majority of the responses will be pre-populated and responses can be updated as applicable. PLEASE ENSURE YOU COMPLETE THE NCSR IN ADVANCE OF THE APPLICATION DEADLINE****
 - [NCSR FAQs](#)
 - [NCSR One Page Overview](#)
 - [NCSR General User Guide](#)
 - [NCSR Assessment Demo](#)
 - [NCSR Completion Certificate Instructions](#)
- Requested project must align to closing gaps and/or strengthening capabilities identified in the agency's cybersecurity risk assessment
- If an applicant agency is selected to receive FY 2024 SLCGP funds, the NCSR must be completed annually, throughout the grant period of performance

CYBERSECURITY PROGRAM

■ Missouri DPS/OHS Cybersecurity Program

- Applicant Agencies **MUST** subscribe to the Missouri Department of Public Safety (DPS)/Office of Homeland Security (OHS) Cybersecurity Program at the **time of application submission** to be eligible for funding
 - Subscribe by emailing securityintel@mshp.dps.mo.gov with your name, agency/entity, title, desk phone, work phone, and email address
 - Must participate in information sharing with federal, state, and local agencies (i.e., Missouri Department of Public Safety (DPS)/Office of Homeland Security (OHS), Missouri Information Analysis Center (MIAC), St. Louis Fusion Center, Kansas City Regional Fusion Center)

LAW ENFORCEMENT/FIRE ENTITY REQUIREMENTS

- To be eligible for SLCGP funding, the applicant agency must be compliant with the following statutes, as applicable and must maintain compliance throughout the grant period of performance:

- **Section 320.271 RSMo– Fire Department Registration**

Pursuant to [section 320.271 RSMo](#), All fire protection districts, fire departments, and all volunteer fire protection associations as defined in section 320.300 shall complete and file with the state fire marshal within sixty days after January 1, 2008, and annually thereafter, a fire department registration form provided by the state fire marshal.

- **Section 590.650 RSMo– Vehicle Stops Report**

Pursuant to [section 590.650.3 RSMo](#), (1) every law enforcement agency shall compile the data described in subsection 2 for the calendar year into a report to the attorney general and (2) each law enforcement agency shall submit the report to the attorney general no later than March first of the following calendar year.

NOTE: It is the responsibility of the applicant to verify the submission of this report with the Attorney General's Office prior to submitting an application. Failure to submit the Racial Profiling Report will result in the automatic denial of the application. A copy of such report does not need to be submitted with the application.

LAW ENFORCEMENT/FIRE REQUIREMENTS

■ **Section 590.700 RSMo – Written Policy on Recording of Custodial Interrogations**

Pursuant to [section 590.700.4 RSMo](#), each law enforcement agency shall adopt a written policy to record custodial interrogations of persons suspected of committing or attempting to commit felony crimes as outlined in subsection 2 of this section and shall certify adoption of such policy when applying for any grants administered by the Department of Public Safety.

NOTE: It is the responsibility of the applicant to ensure the prescribed written policy is in place prior to submitting an application.

■ **Section 43.544 RSMo – Written Policy on Forwarding Intoxication-Related Traffic Offenses**

Pursuant to [section 43.544.1 RSMo](#), each law enforcement agency shall adopt a policy requiring arrest information for all intoxication-related traffic offenses be forwarded to the central repository as required by [section 43.503 RSMo](#) and shall certify adoption of such policy when applying for any grants administered by the Department of Public Safety.

NOTE: It is the responsibility of the applicant to ensure the prescribed written policy is in place prior to submitting an application.

■ **Section 590.1265 RSMo – Police Use of Force Transparency Act of 2021**

Pursuant to [section 590.1265 RSMo](#) Use of force incidents reporting standards and procedures, publication of report data, analysis report. Each law enforcement agency shall report data submitted under subsection 3 of this section to the department of public safety. *For purposes of grant eligibility, law enforcement agencies will be considered non-compliant if they have not submitted Use of Force reports for three or more months in the past twelve months.*

LAW ENFORCEMENT/FIRE REQUIREMENTS

■ **Section 43.505 RSMo** – National Incident-Based Reporting System (NIBRS) *formerly Uniform Crime reporting (UCR)*

Pursuant to [section 43.505 RSMo](#) Uniform Crime Reporting system – duties of department – violations, penalty: Each law enforcement agency in the state shall: (1) Submit crime incident reports to the department of public safety on forms or in the format prescribed by the department' and (2) Submit any other crime incident information which may be required by the department of public safety. *For purposes of grant eligibility, law enforcement agencies will be considered non-compliant if they have not submitted MIBRS reports for three or more months in the past twelve months.*

NOTE: Show Me Crime Reporting provides a no cost option for agencies to comply with Section 43.505 RSMo. Agencies that are not currently compliant with Section 43.505 RSMo will not be eligible to apply until they have registered with Show Me Crime Reporting and have begun submitting MIBRS reports.

<https://showmecrime.mo.gov/CrimeReporting/MIBRSRegistration.html>

■ **Section 590.030 RSMo** – Rap Back Program Participation

Pursuant to [section 590.030 RSMo](#), all law enforcement agencies shall enroll in the state and federal Rap Back programs on or before January 1, 2022 and continue to remain enrolled. The law enforcement agency shall take all necessary steps to maintain officer enrollment for all officers commissioned with that agency in the Rap Back programs. An officer shall submit to being fingerprinted at any law enforcement agency upon commissioning and for as long as the officer is commissioned with that agency. Each law enforcement agency shall certify compliance with [section 590.030 RSMo](#) when accepting any grants administered by the Department of Public Safety.

FUNDING RESTRICTIONS AND ALLOWABLE COSTS

- All costs must comply with:
 - Applicable statutes, rules and regulations, and policies
 - Notice of Funding Opportunity (NOFO)
 - Terms and conditions of the federal award
 - Uniform Administrative Requirements, Cost Principles, and Audit Requirements at 2 C.F.R. Part 200, the terms and conditions of the award.
- Five allowable expense categories:
 - Planning
 - Organization
 - Equipment
 - Training
 - Exercise

FUNDING RESTRICTIONS AND ALLOWABLE COSTS

■ Requested projects

- **MUST** strengthen state and local cybersecurity preparedness by focusing on cybersecurity measures to help manage state and local risk and enhance Missouri's cybersecurity posture
- **MUST** close gaps and strengthen capabilities identified in an agency's Nationwide Cybersecurity Review (NCSR) or other cybersecurity risk assessment
- **MUST** align with the Missouri Comprehensive Cybersecurity Plan (CCP) which can be located as an attachment in the WebGrants application
- **MUST** align with at least one of the FY 2024 SLCGP Objectives

FUNDING RESTRICTIONS AND ALLOWABLE COSTS

- Examples of allowable costs include but are not limited to planning, organization, equipment, training, and exercise costs for local end-user cybersecurity training and awareness campaigns, cybersecurity planning, monitoring, scanning, and protection solutions for equipment and networks, cybersecurity protection for critical infrastructure, and upgrading legacy technology

FUNDING RESTRICTIONS AND ALLOWABLE COSTS

■ Planning

- Funds may be used for planning activities that support the FY 2024 SLCGP objectives, Missouri Comprehensive Cybersecurity Plan (CCP), and closing gaps and strengthening capabilities in the applicant's in the applicant's NCSR

FUNDING RESTRICTIONS AND ALLOWABLE COSTS

■ Organization

■ Organizational activities include:

- Program management
- Development of whole community partnerships
- Structures and mechanisms for information sharing between the public and private sector
- Operational support

■ Personnel hiring, overtime, and backfill expenses are permitted under this grant to perform allowable SLCGP planning, organization, training, exercise, and equipment activities

■ Personnel expenses may include but is not limited to:

- Training and exercise coordinators
- Program managers and planners
- Cybersecurity navigators

****The grant subrecipient must demonstrate that the personnel will be sustainable once the program ends or funds are no longer available****

FUNDING RESTRICTIONS AND ALLOWABLE COSTS

■ Equipment

- SLCGP equipment is intended to be used to address cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, state and local governments
- Equipment must meet all applicable statutory, regulatory, and DHS/FEMA/DPS/OHS standards to be eligible
- Refer to FEMA's [Authorized Equipment List](#) for allowable equipment items
- Subrecipients are responsible for obtaining and maintaining all necessary certifications and licenses for the requested equipment
- Emergency communications systems and equipment must meet applicable [SAFECOM Guidance](#)
- Funds may be used to purchase maintenance contracts or agreements, warranty coverage, licenses, and user fees in support of a system or equipment
 - Contracts may exceed the period of performance if purchased incidental to the original purchase of the system or equipment
 - Stand-alone warranty or extending an existing maintenance contract on an already-owned piece of equipment or system, may not exceed the period of performance of the award
- Some items require prior approval from DHS/FEMA/DPS/OHS before obligation or purchase of the items. Please reference the grant notes for each equipment item to ensure prior approval is not required or to ensure prior approval is obtained if necessary

FUNDING RESTRICTIONS AND ALLOWABLE COSTS

■ Training

- Allowable training-related costs include the establishment, support, conduct, and attendance of training and/or in conjunction with training by other federal agencies.
- Training conducted should align to the Missouri Comprehensive Cybersecurity Plan (CCP) and address a performance gap identified through the NCSR and contribute to building a capability that will be evaluated through a formal exercise

FUNDING RESTRICTIONS AND ALLOWABLE COSTS

■ Exercise

- Exercises conducted with grant funding should be managed and conducted consistent with the Homeland Security Exercise and Evaluation Program (HSEEP)
- HSEEP guidance for exercise, design, development, conduct, evaluation, and improvement planning is located at: <https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep>

FUNDING RESTRICTIONS AND ALLOWABLE COSTS

- Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services
 - Subrecipients and their contractors must comply with the prohibitions set forth in Section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232 (2018) (FY 2019 NDAA) and 2 C.F.R. section 200.216, 200.327, 200.471, and Appendix II to 2 C.F.R. Part 200. The FY 2019 NDAA and these regulations as they apply to subrecipients and their contractors, provide for two distinct prohibitions: (1) prevent the use of federal award funds to procure or obtain covered telecommunications equipment or services; and (2) prevent the use of federal award funds to contract with any entity that uses such covered telecommunications equipment or services
 - Guidance is available at [Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services \(Interim\) #405-143-1](#)
 - Additional guidance is available at [Contract Provisions Guide: Navigating Appendix II to Part 200 – Contract Provisions for Non-Federal Entity Contracts Under Federal Awards \(fema.gov\)](#)

FUNDING RESTRICTIONS AND ALLOWABLE COSTS

- FEMA subrecipients may not use any FEMA funds under open or new awards to:
 - Procure or obtain any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology of any system;
 - Enter into, extend, or renew a contract to procure or obtain any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology of any system; or
 - Enter into, extend, or renew contracts with entities that use covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system

FUNDING RESTRICTIONS AND ALLOWABLE COSTS

■ Replacement Equipment and Services

- FEMA grant funding may be permitted to procure replacement equipment and services impacted by this prohibition, provided the costs are otherwise consistent with the requirements of the NOFO Definitions
- Per section 889(f)(2)-(3) of the FY 2019 NDAA and 2 C.F.R. § 200.216, covered telecommunications equipment or services means:
 - Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation, (or any subsidiary or affiliate of such entities);
 - For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);
 - Telecommunications or video surveillance services provided by such entities or using such equipment; or
 - Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the People's Republic of China.
- Examples of the types of products covered by this prohibition include phones, internet, video surveillance, and cloud servers when produced, provided, or used by the entities listed in the definition of "covered telecommunications equipment or services." See 2 C.F.R. § 200.471b

UNALLOWABLE COSTS

SLCGP funding 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 (This prohibition does not include minor building modifications necessary to install and connect grant-purchased equipment that do not substantially affect a building's structure, layout, systems, or critical aspects of a building's safety, or otherwise materially increase the value or useful life of a building);
- 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 purposes; and
- For any subrecipient cost-sharing contribution

REQUIRED SERVICES & MEMBERSHIPS

All SLCGP subrecipients are required to participate in a limited number of free services by CISA/DPS/OHS

■ Cyber Hygiene Services

- **Vulnerability Scanning – evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities**
 - Provides weekly vulnerability reports and ad-hoc alerts
 - To register for these services, email vulnerability@cisa.dhs.gov with the subject line “Requesting Cyber Hygiene Services – SLCGP” to get started. Indicate in the body of your email that you are requesting this service as part of the SLCGP. For more information, visit CISA’s [Cyber Hygiene Information Page](#).

***Note: Participation is not required for submission and approval of a grant but IS a post-award requirement**

CYBERSECURITY POSTURE

- If the applicant's cybersecurity posture does not contain the below listed benchmarks, the applicant **MUST** achieve these benchmarks during the grant period of performance, if selected for an award under SLCGP
 - Cybersecurity and/or data security policies
 - Cybersecurity training awareness program
 - Cybersecurity incident response plan
 - Receive cybersecurity threat intelligence
- OHS has resources available to assist with these benchmarks. Contact DPS/OHS Cybersecurity Team for assistance by phone at 573-526-0153 or by email at securityintel@mshp.dps.mo.gov

UNIQUE ENTITY IDENTIFIER

- Effective April 4, 2022, the Federal Government transitioned from using the Data Universal Numbering System (DUNS) Number to the Unique Entity Identifier (UEI)
- If your organization is already registered in the WebGrants System, you will need to email your UEI to Kelsey.Saunders@dps.mo.gov if you have not already done so
- If your organization is not yet registered in WebGrants, you will provide the UEI at the time of registration

****Agencies must have a UEI to be awarded funding****

UNIQUE ENTITY IDENTIFIER

Entities that had an active registration in the System for Award Management prior to this date have automatically been assigned a UEI

You can view the UEI in SAM.gov, located below the DUNS Number on your entity registration record

- In your workspace, select the numbered bubble above Active in Entity Management
- Your records should then appear and the UEI number will be on the left side

1 of 1 | Results per page: 25 | Sort by: Expiration Date Ascending

VILLAGE

DUNS Unique Entity ID: [REDACTED]

SAM Unique Entity ID: [REDACTED]

CAGE/NCAGE: [REDACTED]

Purpose of Registration: Federal Assistance Awards

Registration Status	Expiration Date
Active	Jun 10, 2022

Entity Management
What do I need for registration? [Register Entity](#)

Entity Registration

1	1	0	0	0
ACTIVE	DRAFT	WORK IN PROGRESS	SUBMITTED	PHRR

Next Update Due: **Jun 10, 2022** | Due in Next 30 days: **0 Entity Registrations**

Unique Entity ID

0	0	0	0
ACTIVE	DRAFT	WORK IN PROGRESS	SUBMITTED

UNIQUE ENTITY IDENTIFIER

If your agency did not have a DUNS number, you will follow the steps below to obtain a UEI

- Sign in to your SAM.gov account and the system will navigate you to your Workspace
- Under Entity Management, select Get Started

The screenshot displays the SAM.gov Workspace interface. On the left, the 'Workspace' section is visible, containing the 'Entity Management' area. This area is highlighted with a red dashed border and includes a 'Get Started' button. Below the button, there are statistics for 'Entity Registration' (Active: 0, Draft: 0, Work in Progress: 0, Submitted: 0) and 'Unique Entity ID' (Active: 0, Draft: 0). A red arrow points to the 'Get Started' button. On the right, the 'Profile' section shows a user profile, 'Downloads', 'Saved Searches', and 'Following' buttons. Below that, 'Pending Requests' and 'Notifications' sections are shown, both indicating 'No pending requests' and 'No available notifications' respectively, with 'See All' links.

WEBGRANTS APPLICATION

- Log in or register as a new agency at <https://dpsgrants.dps.mo.gov/index.do>
 - If your agency is already registered in the system, someone with access will need to add new users

Key Login

Enter your user id and password

User ID

Password

SIGN IN

Forgot User ID? Reset Password?

Click here to Register

- Two-factor authentication: Enter the one-time passcode sent by WebGrants

Key 2-Factor Authentication

Verify Email Address

Please check the email account for the email address provided in your registration.

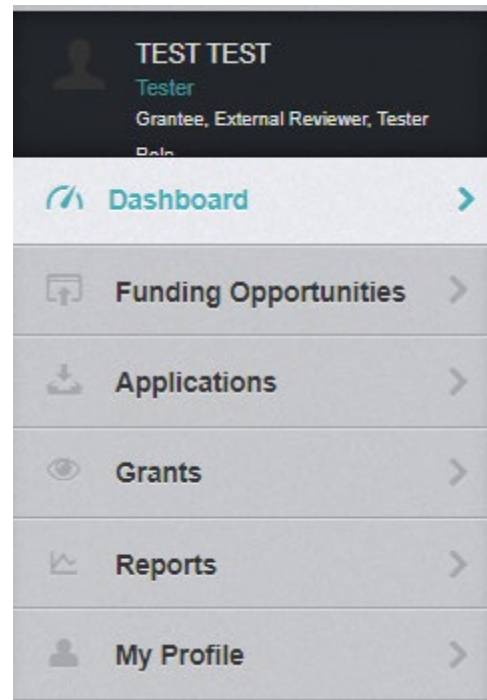
You should receive an email with a temporary passcode. Please enter that passcode below

Enter your Passcode

Submit

APPLICATION INSTRUCTIONS

- Select “Funding Opportunities” and select the FY 2024 State and Local Cybersecurity Grant Program (SLCGP) funding opportunity



APPLICATION INSTRUCTIONS

- Select “Start New Application”
 - Utilizing “Copy Existing Application” is not recommended as application forms change from year to year



APPLICATION INSTRUCTIONS

- After selecting “Start a New Application”, complete the “General Information” section
- “Project Title” should be short and specific to the project, see example below
- After completing the “General Information” select “Save Form Information”



Application - General Information Save Form Information

The Primary Contact is the individual in your organization who will be designated as the primary person responsible for this application from your organization. This individual will receive automated email notifications when your attention is needed on this application.
Select the organization, if you belong to more than one, for which you will be submitting this application.

Application Title*:

Primary Contact*:

Organization*:

Additional Contacts*:

APPLICATION INSTRUCTIONS

- Select the applicant organization then select “Save Form Information”

Application - General Information [Save Form Information](#)

The Primary Contact is the individual in your organization who will be designated as the primary person responsible for this application from your organization. This individual will receive automated email notifications when your attention is needed on this application.
Select the organization, if you belong to more than one, for which you will be submitting this application.

Application ID: 35461

Program Area*: State and Local Cybersecurity Grant Program

Funding Opportunity*: 35206-FY 2024 State and Local Cybersecurity Grant Program (SLCGP) TEST

Application Stage*: Final Application

Application Status*: Editing

Application Title*:

Primary Contact*: TEST TEST

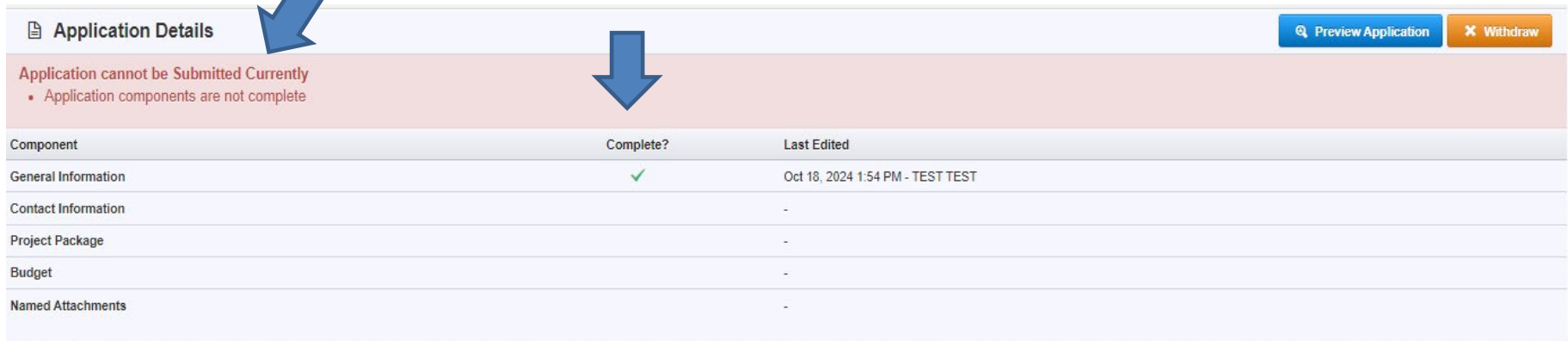
Organization*:

Additional Contacts*:



APPLICATION INSTRUCTIONS

- Complete each of the five “Application Details” with all required information then “Save” and “Mark Complete”
- **All forms must be marked complete in order to “Submit”**



The screenshot shows a web interface for an application. At the top left, there is a tab labeled 'Application Details' with a document icon. To the right of the tab are two buttons: 'Preview Application' (blue) and 'Withdraw' (orange). Below the tab, a red banner displays the message: 'Application cannot be Submitted Currently' followed by a bullet point: 'Application components are not complete'. Below this banner is a table with three columns: 'Component', 'Complete?', and 'Last Edited'. The table lists five components: 'General Information' (marked complete with a green checkmark), 'Contact Information', 'Project Package', 'Budget', and 'Named Attachments' (all marked as incomplete with dashes). Two blue arrows are overlaid on the image: one points to the 'Application Details' tab, and the other points to the 'Complete?' column header.

Component	Complete?	Last Edited
General Information	✓	Oct 18, 2024 1:54 PM - TEST TEST
Contact Information	-	-
Project Package	-	-
Budget	-	-
Named Attachments	-	-

CONTACT INFORMATION

■ Authorized Official

The Authorized Official is the individual who has the authority to legally bind the applicant into a contract and is generally the applicant's elected or appointed chief executive. For example:

- If the applicant agency is a city, the Mayor or City Administrator shall be the Authorized Official
- If the applicant agency is a county, the Presiding County Commissioner or County Executive shall be the Authorized Official (e.g.; the Sheriff is not the Authorized Official)
- If the applicant agency is a State Department, the Director shall be the Authorized Official
- If the applicant agency is a college/university, the President shall be the Authorized Official
- If the applicant agency is a nonprofit, the Board Chair shall be the Authorized Official (This includes Fire Protection District's)
- If the applicant agency is a Regional Planning Commission (RPC) or Council of Government (COG), the Executive Director shall be the Authorized Official.
- If the applicant agency is a special district, such as a Fire Protection District or Ambulance District, the Board Chair/President shall be the Authorized Official
- If the applicant agency is a school district, the Superintendent or School Board President shall be the Authorized Official

****If the Authorized Official has a different title, than those listed above, official documentation naming that position as the Authorized Official for your agency must be included in the application attachments or your application will not be considered for funding****

In order for an application to be considered eligible for funding, the agency's correct Authorized Official MUST be designated in the "Contact Information" form and the "Certified Assurances" form

CONTACT INFORMATION

- Please complete all contact information for
 - Authorized Official
 - Project Director
 - Fiscal Officer
 - Project Contact Person
- Required fields are designated with a red asterisk *
- Select “Save Form” at the top of the screen after entering all of the information



☰ Contact Information Save Form

A screenshot of the top of a web form. On the left, there is a hamburger menu icon followed by the text 'Contact Information'. On the right, there is a green button with a white document icon and the text 'Save Form'. A large blue arrow points from the right side of the image towards the 'Save Form' button.

- Then “Mark as Complete”



☰ Contact Information ✓ Mark as Complete Edit Form

A screenshot of the top of a web form. On the left, there is a hamburger menu icon followed by the text 'Contact Information'. On the right, there are two buttons: an orange button with a white checkmark icon and the text 'Mark as Complete', and a green button with a white document icon and the text 'Edit Form'. A large blue arrow points from the right side of the image towards the 'Mark as Complete' button.

SLCGP PROJECT PACKAGE

- All of the “SLCGP Project Package” information has been combined into one form with nine sections
 - Applicant Funding Stream Information (A)
 - Current Cybersecurity Posture (B)
 - Nationwide Cybersecurity Review (NCSR) (C)
 - Project Details (D)
 - DHS Performance Metrics (E)
 - Cost Share/Match Requirement (F)
 - Audit (G)
 - Risk Assessment (H)
 - Certified Assurances (I)

A. APPLICANT FUNDING STREAM INFORMATION

SLCGP Project Package

A. Applicant Funding Stream Information

A1. Please select the funding source from the dropdown that best represents the applicant agency. *:

Rural

Rural

Non-Rural

State

indicated for entities encompassing a population of less than 50,000
T been designated in the most recent decennial census as an "urbanized" area
Commerce.

Non-Rural funds are dedicated for entities encompassing a population
of greater than 50,000 people and/or have been designated in the most recent decennial census as an
"urbanized area" by the Secretary of Commerce.

State funds are dedicated for state agency applicants.

- AI. – Select from the dropdown, Rural, Non-Rural, or State based on your agency's jurisdiction
 - **Rural** funds are dedicated for entities encompassing a population of less than 50,000 people that has NOT been designated in the most recent decennial census as an "urbanized" area by the Secretary of Commerce.
 - **Non-Rural** funds are dedicated for entities encompassing a population of greater than 50,000 people and/or have been designated in the most recent decennial census as an "urbanized area" by the Secretary of Commerce.
 - **State** funds are dedicated for state agency applicants.

B. CURRENT CYBERSECURITY POSTURE

B1. Does your agency have cybersecurity and/or data security policies? *:

Yes

No

B1.a Please describe your agency's policies. :

Describe your agency's policies|

- B1. – Does your agency have cybersecurity and/or data security policies?
- If yes, B1.a Please describe your agency's policies.

B. CURRENT CYBERSECURITY POSTURE

B2.a Please describe your agency's training awareness program. :

Describe your agency's training awareness program.

B2.b Does your agency perform phishing training? :

Yes

No

B2.b.1 Please explain the phishing training your agency performs. :

Explain the phishing training your agency performs.

B2.c Does the agency provide role-based cybersecurity training to employees? :

Yes

No

B2.c.1. Please explain the role-based cybersecurity training provided to employees. :

Explain the role-based cybersecurity training provided to employees.

- B2. Does your agency have a cybersecurity training awareness program?
 - If yes, B2.a Please describe your agency's training awareness program.
- B2.b Does your agency perform phishing training?
 - If yes, B2.b.1 Please explain the phishing training your agency performs
- B2.c Does the agency provide role-based cybersecurity training to employees?
 - If yes, B2.c.1 Please explain the role-based cybersecurity training provided to employees.

B. CURRENT CYBERSECURITY POSTURE

B3. Does your agency conduct cybersecurity awareness campaigns? *

Yes No

B3.a Please explain the cybersecurity awareness campaigns your agency conducts. :

Explain the cybersecurity awareness campaigns your agency conducts.

B4. Does your agency have in place the NICE Framework for workforce development and training plans? *

Yes No

B4.a Please explain how your agency implements your current NICE Framework components into your work flows. :

Explain how your agency implements your current NICE Framework components into your work flows.

- B3. Does your agency conduct cybersecurity awareness campaigns?
 - If yes, B3.a Please explain the cybersecurity awareness campaigns your agency.
- B4. Does your agency have in place the NICE Framework for workforce development and training plans?
 - If yes B4.a Please explain how your agency implements your current NICE Framework components into your work flows.

B. CURRENT CYBERSECURITY POSTURE

B5. Does your agency have a cybersecurity incident response plan? *

Yes No

B5.a Please describe your agency's cybersecurity incident response plan. :

Describe your agency's cybersecurity incident response plan.

B5.b Is your agency's cybersecurity incident plan CISA approved? :

Yes No

B5.c Does your agency train/exercise your cybersecurity incident response plan? :

Yes No

B5.c.1 Describe how your agency trains/exercises your incident response plan:

Explain how your agency trains/exercises your incident response plan.

- B5. Does your agency have a cybersecurity incident response plan?
 - If yes B5.a Please describe your agency's cybersecurity incident response plan.
 - If yes B5.b Is your agency's cybersecurity incident plan CISA approved?
 - If yes B5.c Does your agency train/exercise your cybersecurity incident response plan?
 - If yes B5.c.1 Describe how your agency trains/exercises your incident response plan.
 - If no B5.c.1 Please explain why your agency does not train/exercise your cybersecurity incident response plan

B. CURRENT CYBERSECURITY POSTURE

B6. Does your agency have the capabilities to analyze network traffic and activities related to potential threats? *:

Yes

No

B6.a Please explain how your agency currently analyzes network traffic and activities related to potential threats. :

Explain how your agency currently analyzes network traffic and activities related to potential threats.

B7. Does your agency implement multi-factor authentication (MFA)?*:

Yes

No

B7.a Please explain how your project implements multi-factor authentication. :

Explain how your project implements multi-factor authentication.

B7.b Does your agency implement multi-factor authentication for all remote access and privileged accounts? :

Yes

No

- **B6. Does your agency have the capabilities to analyze network traffic and activities related to potential threats?**
 - If yes, B6.a Please explain how your agency currently analyzes network traffic and activities related to potential threats.
- **B7. Does your agency implement multi-factor authentication (MFA)?**
 - If yes, B7.a Please explain how your project implements multi-factor authentication.
 - If yes, B7.b Does your agency implement multi-factor authentication for all remote access and privileged accounts.

B. CURRENT CYBERSECURITY POSTURE

B8. Does your agency have a program to identify and eliminate the use of end of life software and hardware? *

Yes No

B8.a Please explain the process your agency uses to identify and eliminate the use of end of life software and hardware. :

Explain the process your agency uses to identify and eliminate the use of end of life software and hardware.

B9. Does your agency prohibit known/fixed/default passwords and credentials? *

Yes No

B10. Does your agency operate under a .gov internet domain? *

Yes No

- B8. Does your agency have a program to identify and eliminate the use of end of life software and hardware?
 - If yes B8.a Please explain the process your agency uses to identify and eliminate the use of end of life software and hardware.
- B9. Does your agency prohibit known/fixed/default passwords and credentials?
- B10. Does your agency operate under a .gov internet domain?

B. CURRENT CYBERSECURITY POSTURE

B11. Does your agency receive cybersecurity threat intelligence?*

Yes

No

B11.a Please describe the sources of threat intelligence (i.e., federal, state, local, private sector/vendor) :

Describe the sources of threat intelligence your agency receives.

B12. Does your agency participate in information sharing with federal, state, and local agencies? (i.e., Missouri Department of Public Safety (DPS)/Office of Homeland Security (OHS), Missouri Information Analysis Center (MIAC), St. Louis Fusion Center, Kansas City Regional Fusion Center) *:

Yes

No

B12.a Please explain why your agency does not participate in information sharing with federal, state, and local agencies. :

Explain why your agency does not participate in information sharing with federal, state, and local agencies. |

- **B11. Does your agency receive cybersecurity threat intelligence?**
 - If yes B11.a Please describe the sources of threat intelligence (i.e., federal, state, local, private sector/vendor).
- **B12. Does your agency participate in information sharing with federal, state, and local agencies? (i.e., Missouri Department of Public Safety (DPS)/Office of Homeland Security (OHS), Missouri Information Analysis Center (MIAC), St. Louis Fusion Center, Kansas City Regional Fusion Center)**
 - If no B12.a Please explain why your agency does not participate in information sharing with federal, state, and local agencies.

B. CURRENT CYBERSECURITY POSTURE

B13. Does your agency subscribe to the Missouri Department of Public Safety (DPS)/Office of Homeland Security (OHS) Cybersecurity Program?*

 Yes No

Applicants MUST subscribe to the Missouri Department of Public Safety (DPS)/Office of Homeland Security (OHS) Cybersecurity Program and participate in information sharing with federal, state, and local agencies at the time of application submission to be eligible for funding. Entities can subscribe by emailing securityintel@mshp.dps.mo.gov with your name, agency/entity, title, desk phone, work phone, and email address.

B13.a Please check the box to certify understanding that the applicant agency must subscribe to the Missouri Office of Homeland Security (OHS) Cybersecurity Program at the time of application. To subscribe to the Missouri Department of Public Safety (DPS)/Office of Homeland Security (OHS) Cybersecurity Program, email securityintel@mshp.dps.mo.gov with your name, agency/entity, title, desk phone, work phone, and email address.:

■ B13. Does your agency subscribe to the Missouri Department of Public Safety (DPS)/Office of Homeland Security (OHS) Cybersecurity Program?

■ If no, B13.a Please check the box to certify understanding that the applicant agency must subscribe to the Missouri Department of Public Safety/Office of Homeland Security (OHS) Cybersecurity Program at the **time of application**.

■ To subscribe to the Missouri DPS Office of Homeland Security (OHS) Cybersecurity Program, email SecurityIntel@mshp.dps.mo.gov with your name, agency/entity, title, desk phone, work phone, and email address.

C. NATIONWIDE CYBERSECURITY REVIEW (NCSR)

■ The following documents are available to assist in completion of the NCSR:

- [NCSR FAQs](#)
- [NCSR One Page Overview](#)
- [NCSR General User Guide](#)
- [NCSR Assessment Demo](#)
- [NCSR Completion Certificate Instructions](#)

C. NATIONWIDE CYBERSECURITY REVIEW (NCSR)

C. Nationwide Cybersecurity Review (NCSR)

Completion of the 2024 NCSR and receipt of results is required to be eligible for FY 2024 SLCGP funding.

The NCSR is a no-cost, anonymous, annual self-assessment that is designed to measure gaps and capabilities of U.S. State, Local, Tribal, and Territorial (SLTT) governments' cybersecurity programs.

The NCSR can be completed at the following link: <https://www.cisecurity.org/ms-isac/services/ncsr>.

The 2024 NCSR Completion Certificate must be uploaded in the Named Attachments Form.

C1. Has your agency completed the 2024 NCSR and received the results?*

Yes

No

C2. Please indicate the NCSR maturity scale for each section of the applicant agency's 2024 NCSR.

Identify*:

Protect*:

Detect*:

Respond*:

Recover*:

■ C1. Has your agency completed the 2024 NCSR and received the results?

** Completion of the 2024 NCSR and receipt of results is required to be eligible for FY 2024 SLCGP funding. **

**The 2024 NCSR Completion Certificate must be uploaded in the Named Attachments Form. **

■ C2. Please indicate the NCSR maturity scale for each section of the applicant agency's 2024 NCSR.

- Identity
- Protect
- Detect
- Respond
- Recover

D. PROJECT DETAILS

D. Project Details

D1. Please give a brief overall description of your requested project.*:

Give a brief overall description of your project.

D2. Provide a summary of specific project actions/items that will be purchased with grant funds.*:

Provide a summary of actions/items that will be completed with the grant funds.

- D1. Please give a brief overall description of your requested project.
- D2. Provide a summary of specific project actions/items that will be purchased with grant funds.

D. PROJECT DETAILS

Please Note: Acquiring land or constructing, remodeling, or performing alterations of buildings or other physical facilities is not allowable. This prohibition does not include minor building modifications necessary to install and connect grant-purchased equipment that do not substantially affect a building's structure, layout, systems, or critical aspects of a building's safety, or otherwise materially increase the value or useful life of a building.

D.3 Will the proposed project involve any changes to the natural or built environment to involve any building modification or ground disturbance. For Example: drilling a hole in a wall of a building to mount equipment or run wire for new equipment.*:

 Yes No

D3.a Please explain how the requested project will involve changes to the built or natural environment.:

Explain how the requested project will involve changes to the built or natural environment. i.e., drilling a hole in the wall to mount a piece of equipment.

- **D3. Will the proposed project involve any changes to the natural or built environment to involve any building modification or ground disturbance.**
- **If yes D3.a Please explain how the requested project will involve changes to the built or natural environment.**

D. PROJECT DETAILS

D4. Provide an estimated duration of the project (how long will it take to complete this project). *:

Provide the estimated duration of the project.

Remember project activities MUST fall within the grant period of performance.

Project activities must be completed during the grant period of performance.

The grant period of performance for the FY 2024 SLCGP is February 1, 2025 – January 31, 2028.

- D4. Provide an estimated duration of the project (how long will it take to complete this project).

**** Project activities must be completed during the grant period of performance. The grant period of performance for the FY 2024 SLCGP is February 1, 2025 – January 31, 2028 ****

D. PROJECT DETAILS

D5. Please explain why this project is necessary and how it will improve the cybersecurity posture of your agency and the state of Missouri. *:

Explain why the project is necessary and how it will improve the cybersecurity posture of your agency and the state of Missouri.

D6. Please explain how this project will close gaps and strengthen capabilities identified in your agency's 2024 Nationwide Cybersecurity Review (NCSR). *:

Explain how the project will close gaps and strengthen capabilities identified in your agency's 2024 NCSR.

- D5. Please explain why this project is necessary and how it will improve the cybersecurity posture of your agency and the state of Missouri.
- D6. Please explain how this project will close gaps and strengthen capabilities identified in your agency's 2024 Nationwide Cybersecurity Review (NCSR).

D. PROJECT DETAILS

D7. By checking this box the applicant agency attests the requested project works to close gaps and strengthen capabilities identified in their agency's Nationwide Cybersecurity Review (NCSR). Note The NCSR is subject to review by the Missouri Department of Public Safety (DPS)/Office of Homeland Security (OHS). *



D8. Please select from the list which NIST functions your project will address. *

Identify
Protect
Detect
Respond
Recover

D8.a Please explain how your project will address the above selected NIST functions. *

Explain how your project will address NIST function(s) selected above|

- D7. By checking this box the applicant agency attests the requested project works to close gaps and strengthen capabilities identified in their agency's Nationwide Cybersecurity Review (NCSR). Note: The NCSR is subject to review by the Missouri Department of Public Safety (DPS)/Office of Homeland Security (OHS).
- D.8 Please select from the list which NIST functions your project will address.
 - To make multiple selections, you may click in the box after making your first selection to make additional selections.
- D.8.a Please explain how your project will address the above selected NIST functions

D. PROJECT DETAILS

D9. Does the requested project align to any of the state of Missouri established priorities for the FY 2024 SLCGP. The priorities are listed in the FY 2024 SLCGP Notice of Funding Opportunity. *:

Yes

No

D9.a Please select which priority(s) your project aligns with.:

D9.b Please explain how your project aligns to the priorities selected in question D8.a.:

D9.b Please explain how your project aligns to the priorities selected in question D9.a.:

Implement multi-factor authentication

Implement enhanced logging

Data encryption for data at rest and in transit

End use of unsupported/end of life software and hardware that are accessible from the Internet

Prohibit use of known/fixed/default passwords and credentials

Ensure the ability to reconstitute systems (backups)

Migration to the .gov internet domain

Explain how your project aligns to the priorities selected in D9.a

■ D9. Does the requested project align to any of the state of Missouri established priorities for the FY 2024 SLCGP. The priorities are listed in the FY 2024 Notice of Funding Opportunity (NOFO)

■ If yes, D9.a Please select which priority(s) your project aligns with.

■ Press Ctrl + Click to select multiple items.

■ If yes, D9.b Please explain how your project aligns to the priorities selected in question D9.a

D. PROJECT DETAILS

D10. Please select the SLCGP Objective, Sub-objective(s), and Outcome(s) that your project best aligns with.

The Objectives, Sub-Objectives, and Outcomes of the FY 2024 SLCGP are discussed in detail in Appendix A of the NOFO

Only one project and objective can be submitted per application.

A maximum of four applications, not to exceed \$200,000 cumulatively, will be allowed per applicant agency.

Objective*:

Objective 1 - Develop and establish appropriate governance structures, as well as develop, implement, or revise cybersecurity plans, to improve cap

Please select the Sub-Objective(s) your project aligns with. The sub-objective MUST correlate with the Objective #1-4 that was selected above.

For example:

Only Sub-Objective 1.1, 1.2, and 1.3 correlate with Objective 1

Only Sub-Objective 2.1, 2.2, 2.3, 2.4, and 2.5 correlate with Objective 2.

Sub-Objective*:

* Sub-Objective 1.1 - Establish cybersecurity governance structures and implement a program to evaluate maturity of the cybersecurity program aligned to Cybersecurity Per

Please select the Outcome(s) your project aligns with. The outcome(s) MUST correlate with the Objective #1-4 and Sub-Objective that was selected at

For example:

Only Outcome 1.1.1 and 1.1.2 correlates with Objective 1 and Sub-Objective 1.1.

Only Outcome 2.2.1 correlates with Objective 2 and Sub-Objective 2.2.

Outcomes*:

* Outcome 1.1.1 - Participants have established and documented a uniform cybersecurity governance structure that is accountable to organizational leadership and works to

■ D10. Please select the SLCGP Objective, Sub-Objective, and Outcome that your project best aligns with. The Objectives, Sub-Objectives, and Outcomes of the FY 2024 SLCGP are discussed in detail in Appendix A of the FY 2024 SLCGP NOFO.

■ The sub-objective **MUST** correlate with the Objective #1-4 that was selected above.

To make multiple selections, you may click in the box after making your first selection to make additional selections.

■ The outcome(s) **MUST** correlate with the Objective #1-4 and Sub-Objective that was selected above.

To make multiple selections, you may click in the box after making your first selection to make additional selections.

**** Only one project and objective can be submitted per application. A maximum of four applications, not to exceed \$200,000, cumulatively will be allowed per applicant agency ****

D. PROJECT DETAILS

D11. Please explain how the requested project aligns with the [Missouri Comprehensive Cybersecurity Plan](#).

✖

Explain how the project aligns with the Missouri Comprehensive Cybersecurity Plan. |

- D11. Please explain how the requested project aligns with the Missouri Comprehensive Cybersecurity Plan (CCP). The Missouri CCP is linked within question D11 and can also be accessed as an attachment to the application.

D. PROJECT DETAILS

D12. By checking this box, the applicant agency attests they do not have funds that are budgeted for the requested project as supplanting is not allowed for the FY 2024 SLCGP. *:



D13. By checking this box, the applicant agency certifies understanding that project activities must be completed within the period of performance (February 1, 2025 – January 31, 2028) and work on the project cannot begin until a grant award (Subaward Agreement) has been received and fully executed. If project activities are started prior to the completion of the above listed activities, costs will be deemed ineligible. *:



D14. How does your agency plan to financially sustain the requested items in the future without grant funding? *:

Explain how the agency plans to financially sustain the requested item(s) in the future without grant funding.

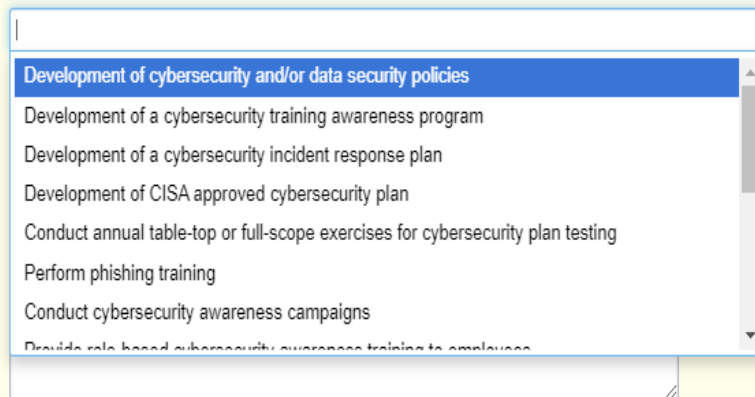
- D12. By checking this box, the applicant agency attests they do not have funds that are budgeted for the requested project as supplanting is not allowed for the FY 2024 SLCGP.
- D13 By checking this box, the applicant agency certifies understanding that project activities must be completed within the period of performance (**February 1, 2025 – January 31, 2028**) and work on the project **CANNOT** begin until a grant award (Subaward Agreement) has been received and fully executed. If project activities are started prior to the completion of the above listed activities, costs will be deemed **INELIGIBLE**.
- D14. How does your agency plan to financially sustain the requested items in the future without grant funding?

E. DHS PERFORMANCE METRICS

E. DHS Performance Metrics

E1. Please select from the “dropdown” if the requested project will result in the fulfillment of any of the activities. If the requested project will not fulfill any of the activities, select N/A. *:

E1.a If your project will achieve one or more of the activities selected in E1, please describe how your project will accomplish these activities. :



The image shows a screenshot of a web form's dropdown menu. The menu is open, displaying a list of activities. The first option, "Development of cybersecurity and/or data security policies", is highlighted in blue. Below it are several other options, including "Development of a cybersecurity training awareness program", "Development of a cybersecurity incident response plan", "Development of CISA approved cybersecurity plan", "Conduct annual table-top or full-scope exercises for cybersecurity plan testing", "Perform phishing training", "Conduct cybersecurity awareness campaigns", and "Provide role-based cybersecurity awareness training to employees".

- E1. Please select from the “dropdown” below if the requested project will result in the fulfillment of any of the following activities. If the requested project will not fulfill any of the following activities, select N/A.

To make multiple selections, you may click in the box after making your first selection to make additional selections.

- E1.a If your project will achieve one of the above activities, please describe how your project will accomplish these activities.

F. COST SHARE/MATCH REQUIREMENT

F. Cost Share/Match Requirement

F1. Will your agency be utilizing cash (hard) match to meet the 30% match requirement? *: Yes No

F1.a Please describe the source of the cash :

Describe the source of the cash|

Funds from other Federal grants cannot be utilized to fulfill the match requirement on the FY 2024 SLCGP, unless specifically authorized.

- F.I Will your agency be utilizing cash (hard) match to meet the 30% match requirement?
- If yes, F.I.a Please describe the source of the cash
 - ** Funds from other Federal grants cannot be utilized to fulfill the match requirement on the FY 2024 SLCGP, unless specifically authorized. **
- Please reference slide 16 of this PowerPoint for examples on how to calculate match for your requested project.

F. COST SHARE/MATCH REQUIREMENT

F2. Will your agency be utilizing in-kind (soft) match to meet the 30% match requirement?*

Yes

No

Only property or services that comply with program guidance and/or program regulations, are allowable. A subrecipient cannot use a source for the soft match that is completely unrelated to the SLCGP program's goals, objectives, NOFO, etc. The same contribution cannot be used if it is already used as match for another Federal grant program or paid from other grant funds, unless specifically authorized.

F2.a Please describe the in-kind match that will be utilized.:

Describe the in-kind match that will be utilized.

The same contribution cannot be used if it is already used as match for another Federal grant program or paid from other grant funds, unless specifically authorized.

- F2. Will your agency be utilizing in-kind (soft) match to meet the 30% match requirement?
 - Only property or services that comply with program guidance and/or program regulations, are allowable. A subrecipient cannot use a source for the soft match that is completely unrelated to the SLCGP program's goals, objectives, NOFO, etc.
- If yes, F2.a Please describe the in-kind match that will be utilized
 - The same contribution cannot be used if it is already used as match for another Federal grant program or paid from other grant funds, unless specifically authorized.

F. COST SHARE/MATCH REQUIREMENT

F2.b Please describe how the in-kind match relates to the project :

Describe how the in-kind match relates to the project.

F2.c Will the agency be able to provide supporting documentation for the in-kind match? :

Yes

No

F2.d By checking this box the applicant agency attests the in-kind match has not and/or will not be utilized to fulfill a match requirement on any other Federal grant. :



- If yes, F2.b Please describe how the in-kind match relates to the project.
- If yes, F2.c Will the agency be able to provide supporting documentation for the in-kind match?
- If yes, F2.d By checking this box the applicant agency attests the in-kind match has not and/or will not be utilized to fulfill a match requirement on any other Federal grant.

G. AUDIT

- Utilizing your agency's most recent audit, please complete all required fields in the "Audit" section
 - If your agency does not have an audit, complete this section utilizing your most recent annual financial statement and attach the statement in lieu of the audit
 - *Note – If your audit covered a period that ended more than three years ago, please provide the most recent financial statement for your agency's last fiscal year, as well as a copy of the audit
- All attachments will be uploaded in the "Named Attachments" form of the application

G. AUDIT

- Using your most recent audit, annual financial statement, and/or SEFA, complete the “Audit” section indicating whether the \$750,000 threshold for federal audits was met per Part 2 CFR 200.501
 - The \$750,000 federal expenditure threshold is met when an agency has **expended** \$750,000 or more in federal funds during their last fiscal year. This information can be found on the agency’s most recent audit, annual financial statements, and/or SEFA. (The total amount of federal funds expended is derived from all federal sources, not just Department of Homeland Security funds)

G. AUDIT

G. Audit

G1. Has the Applicant Agency exceeded the federal expenditure threshold of \$750,000 in federal funds during agency's last fiscal year? *:

Yes

No

If the applicant agency exceeded the federal expenditure threshold in their last fiscal year, they must have their Single Audit or Program Specific Audit completed and submitted to the DPS/OHS within nine (9) months after the end of the audited fiscal year.

G2. Date last audit completed *:

12/31/2023

If an agency has never had an audit, please enter the date of the last annual financial statement.

G3. By checking this box the applicant agency understands they are required to upload a copy of the agency's most recent completed audit (or annual financial statement) in the Named Attachments section of this application. *:



H. RISK ASSESSMENT

- The “Risk Assessment” section is to gather information the awarding agency will use to conduct a risk assessment of your agency, as required by 2 CFR 200.332
- Depending on the responses to these questions, the awarding agency may contact you for additional information

H. Risk Assessment

H1. Does the applicant agency have new personnel that will be working on this award? *:

 Yes No

New personnel is defined as working with this award type less than 12 months.

H1.a. Please list the name(s) of new personnel and their title(s) :

List names of new personnel and their titles.

H2. Does the applicant agency have a new fiscal or time accounting system that will be used on this award? *:

 Yes No

New fiscal or time accounting system is defined as a system being utilized less than 12 months within the applicant agency.

H3. Does the applicant agency receive any direct Federal awards? *:

 Yes No

Direct grants are grants that you apply directly to the federal government for and there is no intermediary agency such as OHS.

H3.a. Please list the direct Federal awards the agency receives.:

List direct Federal awards the agency receives.

H3.b. Did the applicant agency receive any Federal monitoring on a direct federal award in their last fiscal year? :

 Yes No

H3.b.1. Please list the direct awards that were monitored and indicate if there were any findings or recommendations. :

List the direct Federal awards that were monitored and indicate if there were any findings or recommendations.

I. CERTIFIED ASSURANCES

The “Certified Assurances” section MUST be completed with the agency’s correct Authorized Official to be considered eligible for funding

****If the Authorized Official has a different title, than those listed, official documentation naming that position as the Authorized Official for your agency must be included in the application attachments or your application will not be considered for funding****

Applications can be saved without the Authorized Official’s information while they review, but MUST be completed before the form can be marked complete and submitted

I. CERTIFIED ASSURANCES

I. Certified Assurances

To the best of my knowledge and belief, all data in this application is true and correct, the document has been duly authorized by the governing body of the applicant, and the applicant attests to and/or will comply with the following Certified Assurances if the assistance is awarded:

SLOGP Certified Assurances

11. By checking this box, I have read and agree to the terms and conditions of this grant.*

In order to be considered eligible for funding, the correct Authorized Official must be designated and have knowledge of the certified assurances associated with this funding opportunity.

If the incorrect Authorized Official is listed in #12 of the application, the application will be deemed ineligible for funding.

The Authorized Official is the individual who has the authority to legally bind the applicant into a contract and is generally the applicant's elected or appointed chief executive. For example:

- If the applicant agency is a city, the Mayor or City Administrator shall be the Authorized Official
- If the applicant agency is a county, the Presiding County Commissioner or County Executive shall be the Authorized Official
- If the applicant agency is a State Department, the Director shall be the Authorized Official
- If the applicant agency is a college/university, the President shall be the Authorized Official
- If the applicant agency is a nonprofit, the Board Chair/President shall be the Authorized Official, this includes Fire Protection Districts.
- If the applicant agency is a Regional Planning Commission (RPC) or Council of Government (COG), the Executive Director shall be the Authorized Official
- If the applicant agency is a special district, such as Fire Protection District or Ambulance District, the Board Chair/President shall be the Authorized Official
- If the applicant agency is a school district, the Superintendent or School Board President shall be the Authorized Official

If a designee is being utilized to authorize the application, the Missouri Department of Public Safety (DPS) reserves the right to request documentation that indicates the designee has the authority to legally bind the applicant into a contract in lieu of the Authorized Official at the time of application submission.

****If the Authorized Official has a different title, than those listed above, official documentation naming that position as the Authorized Official for your agency must be included in the application attachments or your application will not be considered for funding****

The above list is not an all-inclusive list. If your agency does not fall into the above listed categories, or if you are unsure of who the Authorized Official is for your agency, please contact the Missouri Department of Public Safety (DPS)/Office of Homeland Security (OHS) at (573) 522-8125.

12. Authorized Official Name and Title *:

13. Name and Title of person completing this application *:

14. By checking this box, I certify I have read and understand that the correct Authorized Official MUST be designated on this form in order to be eligible for funding.*

15. Date*:

BUDGET

****Quotes/Cost Basis are required for all items requested. You will be required to upload these documents in the named attachments form of your application.****

Select "Save Form" to begin entering requested items in the budget

Save Form

Enter each budget line by selecting "Add Row" in the corresponding budget category and completing all required information, then "Save Form" and "Add Row" if additional budget lines are needed

Budget Sections:

- Personnel
- Benefits
- Travel
- Equipment
- Supplies/Operations
- Contractual

☰ **Equipment** - Multi-List ✓ Mark as Complete + Add Row

All equipment items are defined as tangible property having an acquisition cost of \$5,000 or more, and a useful life of more than one year.

All Equipment purchased has to be an allowable item on the Authorized Equipment List (AEL).

Equipment quotes may be uploaded in Named Attachment component of the application .

To include an equipment item in the budget, select "Add Row". To include more than one equipment expense, repeat this step for each budget item.

Item Name	AEL #	Quantity	Unit Cost	Total Cost	Match Amount	Type of Match	Function	Federal Amount
No Data for Table								

Last Edited By: Sue Ann Surface - Oct 17, 2024 11:43 AM + Add Row

BUDGET – CASH MATCH

Equipment

Save Row

All equipment items are defined as tangible property having an acquisition cost of \$5,000 or more, and a useful life of more than one year.

All Equipment purchased has to be an allowable item on the Authorized Equipment List (AEL).

Equipment quotes may be uploaded in Named Attachment component of the application. ,

To include an equipment item in the budget, select "Add Row". To include more than one equipment expense, repeat this step for each budget item.

Item Name*:

AEL #:

Quantity*:

Unit Cost*:

Total Cost*:

Match Amount*:

Type of Match*:

Function*:

Federal Amount:



- The Federal amount of funds requested will automatically calculate based on the amount entered for match
- Total Cost = Local Match Amount + Federal Amount Requested.
- 30% match requirement for FY24 SLCGP.
- The screenshot on this slide shows a cash match example.
- **NOTE** - You will only include the match amount if utilizing Hard (Cash) match (in-kind match example on next page)

BUDGET – IN-KIND MATCH

- In-kind Match: If you are utilizing in-kind match you will complete two steps to enter the costs in the budget form:
 - Step 1: Enter the budget line item information for your in-kind match.
 - Total Cost should = Local Match Amount.
 - No Federal amount will be accounted for on this line.
 - Step 2: Enter the budget line item information for the items requested in the project (items grant funds will be utilized for)
 - Total Cost = Full cost of item that you are requested grant funds for
 - Match Amount should be entered as \$0.00
 - Your match amount is accounted for in Step 1

The steps described above are shown on the next two slides

BUDGET – IN-KIND MATCH

Supplies/Operations

Save Row

Supplies and Operations items are defined as property with acquisition cost less than \$5,000, or a useful life of less than one year.

To include a supply or operational expense in the budget, select "Add Row". To include more than one supply or operational expense, repeat this step for each budget item.

Supply/Operation Type*: Other (computer, projector, chair, etc.)

List each supply/operational item by type.

Item Name*: Laptop

Quantity*: 1

Enter the requested number of months, people, units, etc. If the expense is a one-time cost, enter 1.

Unit Cost*: 2678.57

Total Cost*: 2678.57

Match Amount*: 2678.57

Type of Match*: In-Kind

Function*: Equipment

Federal Amount:

- Step 1
 - Add a budget line to account for the in-kind match.
- Total Cost should = Local Match Amount.
- No Federal amount (grant funds) will be accounted for on this line.

BUDGET – IN-KIND MATCH

Supplies/Operations

Delete Row Save Row

Supplies and Operations items are defined as property with acquisition cost less than \$5,000, or a useful life of less than one year.

To include a supply or operational expense in the budget, select "Add Row". To include more than one supply or operational expense, repeat this step for each budget item.

Supply/Operation Type*: Other (computer, projector, chair, etc.)

List each supply/operational item by type.

Item Name*: Laptops

Quantity*: 2.00

Enter the requested number of months, people, units, etc. If the expense is a one-time cost, enter 1.

Unit Cost*: \$3,125.00

Total Cost*: \$6,250.00

Match Amount*: \$0.00

Type of Match*: In-Kind

Function*: Equipment

Federal Amount: \$6,250.00

- Step 2
 - Add a budget line item for the item(s) requested in the project (items grant funds will be utilized for)
 - Match Amount should be entered as \$0.00
 - Your match amount was accounted for in Step 1

BUDGET – IN-KIND MATCH

☰ Supplies/Operations - Multi-List

✓ Mark as Complete

+ Add Row

Supplies and Operations items are defined as property with acquisition cost less than \$5,000, or a useful life of less than one year.

To include a supply or operational expense in the budget, select "Add Row". To include more than one supply or operational expense, repeat this step for each budget item.

Supply/Operation Type	Item Name	Quantity	Unit Cost	Total Cost	Match Amount	Type of Match	Function	Federal Amount
Other (computer, projector, chair, etc.)	Laptop	1.00	\$2,678.57	\$2,678.57	\$2,678.57	In-Kind	Equipment	\$0.00
Other (computer, projector, chair, etc.)	Laptops	2.00	\$3,125.00	\$6,250.00	\$0.00	In-Kind	Equipment	\$6,250.00
				\$8,928.57	\$2,678.57			\$6,250.00

- The screen above shows an example of what the in-kind match (server) and the requested items to purchase with grant funds (laptops) would look like when utilizing in-kind match.

BUDGET

- **Cost Share or Match:** 30% cost share requirement (cash [hard match] or in-kind [soft match])
- Reference slide 16 to find examples of how to calculate your match.
- Be sure the correct match amounts are included in the Budget Form of your application
 - **** If less than 30% match is included in your budget, your application will be deemed INELIGIBLE****

BUDGET

- Provide required justification for all budget lines by selecting “Edit Form”
Justification for all sections can be completed at one time



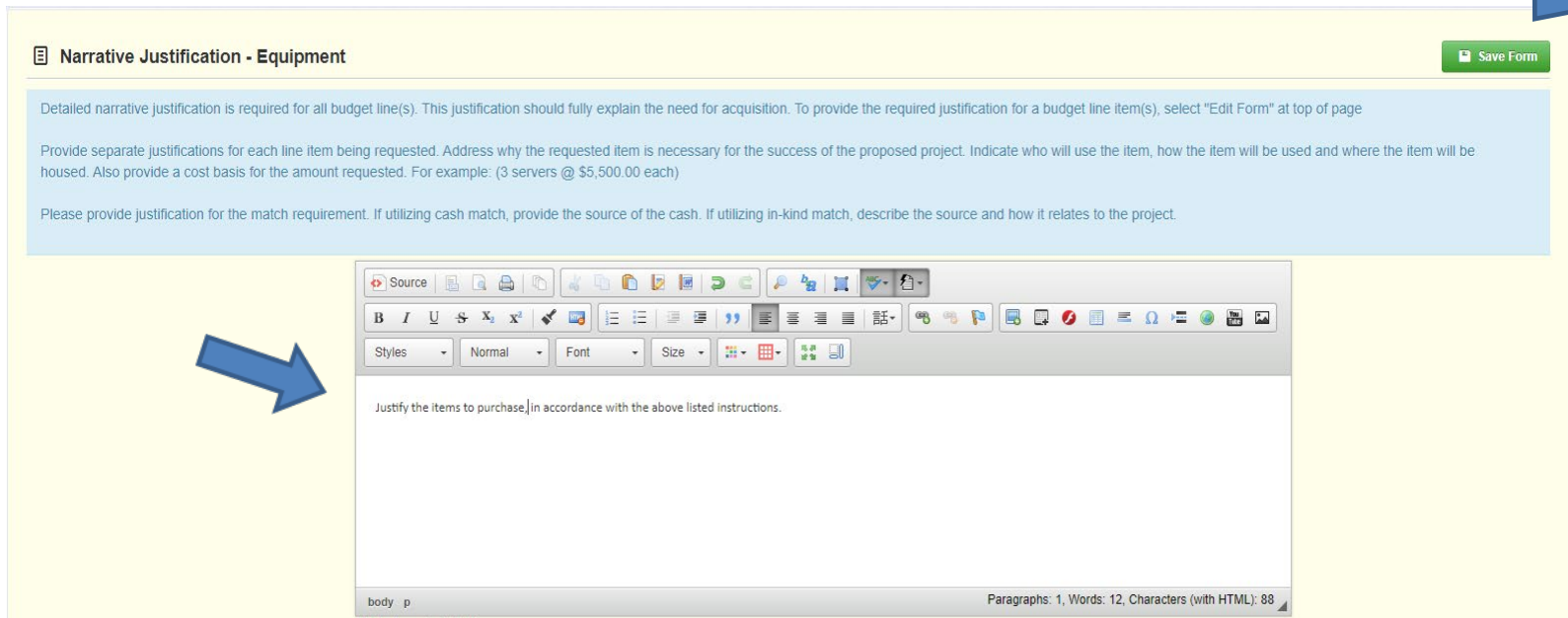
 Narrative Justification - Equipment

 Mark as Complete

 Edit Form

BUDGET

- The instructions for each budget section provides a description of what information should be included in the budget narrative justifications



Narrative Justification - Equipment Save Form

Detailed narrative justification is required for all budget line(s). This justification should fully explain the need for acquisition. To provide the required justification for a budget line item(s), select "Edit Form" at top of page

Provide separate justifications for each line item being requested. Address why the requested item is necessary for the success of the proposed project. Indicate who will use the item, how the item will be used and where the item will be housed. Also provide a cost basis for the amount requested. For example: (3 servers @ \$5,500.00 each)

Please provide justification for the match requirement. If utilizing cash match, provide the source of the cash. If utilizing in-kind match, describe the source and how it relates to the project.

Justify the items to purchase in accordance with the above listed instructions.

body p Paragraphs: 1, Words: 12, Characters (with HTML): 88

- **DO NOT** put “See attachment” in the narrative justifications! Each section must be completed. If you have information that will not fit in the justification, please enter a summary in the justification and then include the statement “Additional information can be located in the “Named Attachment” section.
- When justifications for all sections have been completed, mark “Save Form” and “Mark as Complete” at the top of page.

BUDGET

■ Personnel Narrative Justification

- Provide each employee, what duties they will be required to complete for the project, their salary, and their estimated hours spent on the project as a cost basis
- Provide justification to fulfill the 30% match requirement
 - Cash
 - Provide the source of the cash match
 - In-Kind
 - Describe the source of the in-kind match
 - Describe how the in-kind match relates to the project

BUDGET

■ Personnel Benefits Narrative Justification

- Provide each employee, what benefits they receive, the cost of each benefit, how it is determined (i.e., monthly or percentage based) and the rate
- Provide justification to fulfill the 30% match requirement
 - Cash
 - Provide the source of the cash match
 - In-Kind
 - Describe the source of the in-kind match
 - Describe how the in-kind match relates to the project

BUDGET

■ Travel Costs

- Meal per diem rates cannot exceed the rates approved by the Missouri Office of Administration
 - <https://oa.mo.gov/accounting/state-employees/travel-portal-information/meals-per-diem>
- Mileage rates cannot exceed the state rates approved by the Missouri Office of Administration
 - <https://oa.mo.gov/accounting/state-employees/travel-portal-information/mileage>
- Lodging rates cannot exceed the established CONUS rates
 - <https://www.gsa.gov/travel/plan-book/per-diem-rates?gsaredirect=portalcategory>
- Each agency must follow their own travel policy

BUDGET

■ Travel Narrative Justification

- Each travel event requested should be listed in the justification and include a full cost basis for the amount requested, including:
 - Justification for the travel
 - Number of staff traveling
 - Estimated dates and locations
 - What costs are being requested and the estimated rate (i.e., lodging, meal per diem, conference fees, etc.)
- Provide justification to fulfill the 30% match requirement
 - Cash
 - Provide the source of the cash match
 - In-Kind
 - Describe the source of the in-kind match
 - Describe how the in-kind match relates to the project

BUDGET

- Equipment is defined as tangible, personal property (including information technology systems) having a useful life of more than one year and a per-unit acquisition cost of \$5,000.00 or more
- Authorized Equipment List (AEL) Number is required on the budget, the link to the site is provided in the instructions

☰ Equipment - Multi-List

✓ Mark as Complete

+ Add Row

All equipment items are defined as tangible property having an acquisition cost of \$5,000 or more, and a useful life of more than one year.

All Equipment purchased has to be an allowable item on the Authorized Equipment List (AEL).



Equipment quotes may be uploaded in Named Attachment component of the application. ,

To include an equipment item in the budget, select "Add Row". To include more than one equipment expense, repeat this step for each budget item.

BUDGET

- Search the site for the correct AEL number

Authorized Equipment List

The Authorized Equipment List (AEL) is a tool for emergency managers, first responders and homeland security professionals. It contains approved equipment types allowed under FEMA's preparedness grant programs.

How to Use the List

You have two options to find the equipment you need:

Browse

Click to open accordions and drill down to the specific equipment.

[Browse the List](#)

Advanced Search

Enter keywords, filter by category, or sort.

[Advanced Search](#)

BUDGET

- Equipment Narrative Justification
 - Include why the requested item is necessary for the project
 - Include who will use the item
 - Include how the item will be used
 - Include where the item will be housed
 - Provide a cost basis for the amount requested
 - Provide justification to fulfill the 30% match requirement
 - Cash
 - Provide the source of the cash match
 - In-Kind
 - Describe the source of the in-kind match
 - Describe how the in-kind match relates to the project

BUDGET

- Supplies Narrative Justification
 - Include how the requested item supports the project
 - Include why the amount requested is necessary
 - Include a cost basis
 - For a service that fits the criteria for supplies, the dates covered must be provided (i.e., annual software license, phone, or internet service)
 - Provide justification to fulfill the 30% match requirement
 - Cash
 - Provide the source of the cash match
 - In-Kind
 - Describe the source of the in-kind match
 - Describe how the in-kind match relates to the project

BUDGET

- Contractual Narrative Justification
 - Include what will be provided by the contract
 - Include estimated dates of service or delivery
 - Include why the contract is needed to support the project
 - Include a cost basis for the amount requested
 - Provide justification to fulfill the 30% match requirement
 - Cash
 - Provide the source of the cash match
 - In-Kind
 - Describe the source of the in-kind match
 - Describe how the in-kind match relates to the project


NAMED ATTACHMENTS

All attachments must be included in this section

- Required Attachments
 - Audit/Financial Statement
 - Quote/Cost Basis
 - 2024 NCSR Completion Certificate
 - [NCSR Completion Certificate Instructions](#)
- Other Supporting Attachments (if applicable)
 - Other supporting information (up to 5 attachments)

NAMED ATTACHMENTS

- To add each attachment select the name of the attachment

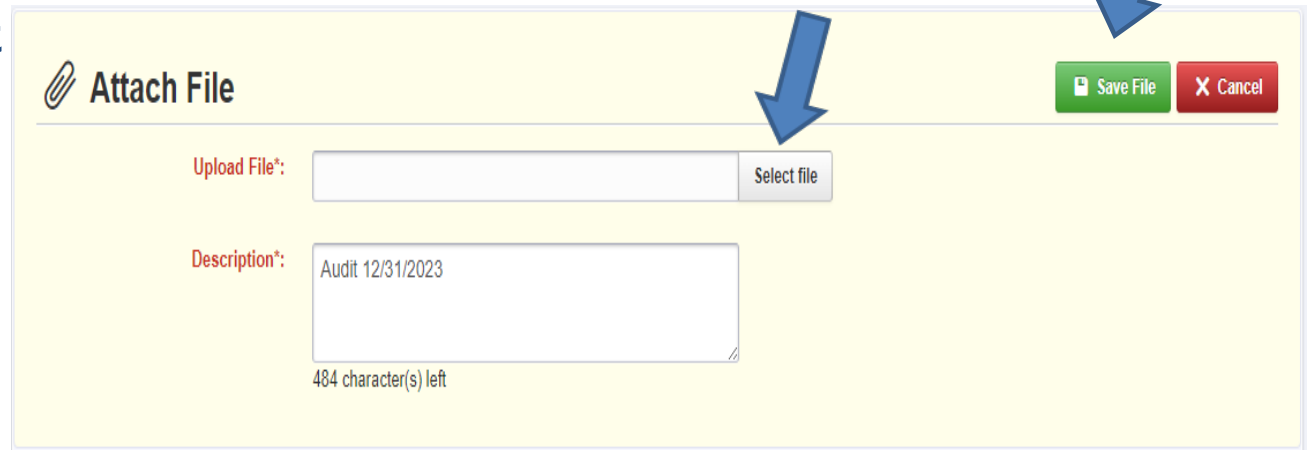
 - Named Attachments  Mark as Complete

Named Attachment	Required	Description	File Name 	Type	Size	Upload Date	Delete?
Audit/Financial Statement (REQUIRED)*	✓						
Quote/Cost Basis (REQUIRED)*	✓						
2024 NCSR Completion Certificate (REQUIRED)*	✓						
Other Supporting Information							
Other Supporting Information							
Other Supporting Information							
Other Supporting Information							
Other Supporting Information							

- The following documents are required documents and must be uploaded before the form can be marked complete
 - Audit/Financial Statement
 - Quote/Cost Basis
 - 2024 NCSR Completion Certificate

NAMED ATTACHMENTS

- Browse to select document
- Add a description to identify the document in the application, and select “Save File”

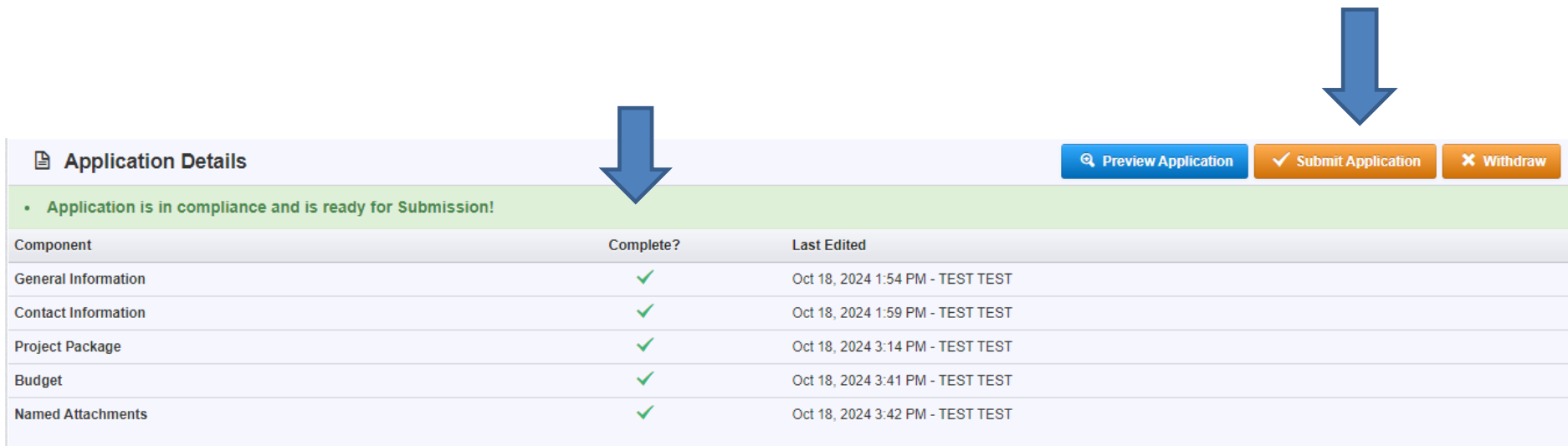


The screenshot shows a dialog box titled "Attach File" with a paperclip icon. It contains the following elements:

- Upload File*:** A text input field with a "Select file" button to its right. A blue arrow points to this button.
- Description*:** A text area containing the text "Audit 12/31/2023". Below the text area, it says "484 character(s) left".
- Buttons:** In the top right corner, there are two buttons: a green "Save File" button and a red "Cancel" button. A blue arrow points to the "Save File" button.

SUBMISSION

- All forms **must be** marked complete in order to submit the application
- When everything is complete, select “Submit”



Application Details

Application is in compliance and is ready for Submission!

Preview Application Submit Application Withdraw

Component	Complete?	Last Edited
General Information	✓	Oct 18, 2024 1:54 PM - TEST TEST
Contact Information	✓	Oct 18, 2024 1:59 PM - TEST TEST
Project Package	✓	Oct 18, 2024 3:14 PM - TEST TEST
Budget	✓	Oct 18, 2024 3:41 PM - TEST TEST
Named Attachments	✓	Oct 18, 2024 3:42 PM - TEST TEST

MISSOURI DEPARTMENT OF PUBLIC SAFETY(DPS)/OFFICE OF HOMELAND SECURITY(OHS) CYBERSECURITY PROGRAM

Contact the Missouri Department of Public Safety (DPS)/Office of Homeland Security (OHS) Cybersecurity Program for project specific questions:

Phone: 573-526-0153

Email: securityintel@mshp.dps.mo.gov

MISSOURI DPS GRANTS

Contact the Missouri DPS Grants for grant or WebGrants specific questions:

Chelse Dowell

Grants Specialist

(573) 751-3879

chelse.dowell@dps.mo.gov

Sue Ann Surface

Grants Specialist

(573) 751-5951

sueann.surface@dps.mo.gov

Chelsey Call

Grants Supervisor

(573) 526-9203

chelsey.call@dps.mo.gov

Kelsey Saunders

Grant Support Specialist

(573) 522-6125

kelsey.saunders@dps.mo.gov

Joni McCarter

Program Manager

(573) 526-9020

joni.mccarter@dps.mo.gov