

# STATE AND LOCAL CYBERSECURITY GRANT PROGRAM (SLCGP)

FY 2022 APPLICATION WORKSHOP



# MISSOURI OFFICE OF HOMELAND SECURITY NOTICE OF FUNDING OPPORTUNITY

**We are pleased to announce the funding opportunity for the FY 2022 State and Local Cybersecurity Grant Program (SLCGP) is open  
November 16, 2022 – December 16, 2022 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>**

# STATE AND LOCAL CYBERSECURITY GRANT PROGRAM (SLCGP)

- The 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)

- The potential consequences of cyber incidents threaten national security. Strengthening cybersecurity practices and resilience of state and local governments is an important homeland security mission and the primary focus of the State and Local Cybersecurity Grant Program (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

<b>November 16, 2022:</b>	SLCGP funding opportunity opens in WebGrants <a href="https://dpsgrants.dps.mo.gov/">https://dpsgrants.dps.mo.gov/</a>
<b>December 16, 2022:</b>	SLCGP applications due in WebGrants <b>5:00 pm CST</b> <b><i>WebGrants will not accept any applications after this time</i></b>
<b>December/January 2022:</b>	Cybersecurity Planning Committee application review/scoring
<b>September 1, 2022:</b>	Projected Project Start Date
<b>August 31, 2025:</b>	Projected Project End Date

# OBJECTIVES

- The goal of 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 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.
  - 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 2022 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 2022 SLCGP NOFO\*

# OBJECTIVES

## ■ **Objective 3: Implement security protections commensurate with risk**

- Sub-objective 3.1 SLT 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 2022 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 2022 SLCGP NOFO\*

# STATE PRIORITIES

- Missouri has established seven priority areas for FY 2022
  - The seven 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) Migration to the .gov internet domain
- **Projects that align to State Priorities will receive extra points during the application scoring process**

# FY 2022 ANTICIPATED FUNDING

- The Federal Notice of Funding Opportunity has estimated funding levels for the FY 2022 SLCGP for Missouri at **\$3,839,975**
- Three funding sources available for FY 2022 SLCGP:
  1. Rural – funds 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
  2. Non-Rural – funds dedicated for entities encompassing a population of greater than 50,000 people that has 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
  3. State – funds dedicated for state agency applicants



# MAXIMUM AWARD

- The maximum award available is \$200,000 Federal share per applicant agency

# MATCH REQUIREMENTS

- 10% 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
- Example:
  - If the total cost of the project is \$100,000, the subrecipient share of 10% would be \$10,000 and the federal share of 90% would be \$90,000

# 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



# CYBERSECURITY ASSESSMENT

- To be eligible to receive SLCGP funding, the applicant agency must have a completed cybersecurity risk assessment
  - Requested project must align to closing gaps and/or strengthening capabilities identified in the agency's cybersecurity risk assessment

# FUNDING RESTRICTIONS AND ALLOWABLE COSTS

- All costs must comply with the 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)
- **MUST** align with at least one of the FY 2022 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 2022 SLCGP objectives, Missouri Comprehensive Cybersecurity Plan (CCP), and closing gaps and strengthening capabilities in the applicant's cybersecurity risk assessment

# 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

# 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/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 [SAFECON 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

# 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 assessments 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
  - 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, 200.326, 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 [Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services \(Interim\) #405-143-1](#), or superseding document.
  - 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

- Effective August 13, 2020, FEMA recipients and 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 and the Preparedness Grants Manual.

## ■ 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. § 200.471

# UNALLOWABLE COSTS

- SLCGP funding may not be used for the following:
  - To supplant state or local funds; however this shall not be construed to prohibit the use of funds from a grant under this NOFO for otherwise permissible uses on the basis that the SLT has previously used SLT funds to support the same or similar uses;
  - For any recipient cost-sharing contribution;
  - 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; or
  - For any purpose that does not address cybersecurity risks or cybersecurity threats on information systems owned or operated by, on or behalf of, the eligible entity that receives the grant or a local government within the jurisdiction of the eligible entity.

# REQUIRED SERVICES & MEMBERSHIPS

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

## ■ OHS Cybersecurity Program

- Must subscribe to the Missouri Office of Homeland Security (OHS) Cybersecurity Program
  - Subscribe by emailing [securityintel@mshp.dps.mo.gov](mailto: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 Office of Homeland Security (OHS), Missouri Information Analysis Center (MIAC), St. Louis Fusion Center, Kansas City Regional Fusion Center)

## ■ Cyber Hygiene Services

- Web Application Scanning – “internet scanning-as-a-service” to assess the “health” of your publicly accessible web applications by checking for known vulnerabilities and weak configurations
  - CISA can recommend ways to enhance security in accordance with industry and government best practices and standards
- 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

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

# REQUIRED SERVICES & MEMBERSHIPS

## ■ NCSR

- Free, anonymous, annual self-assessment designed to measure gaps and capabilities of a SLT's cybersecurity programs. It is based on the National Institute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and MS-ISAC.
- If awarded funding, subrecipients must complete the NCSR, administered by the MS-ISAC, during the first year of the award/subaward period of performance and annually, throughout the grant period of performance

# 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 OHS Cybersecurity Team for assistance by phone at 573-526-0153 or by email at [securityintel@mshp.dps.mo.gov](mailto: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](mailto: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

# 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

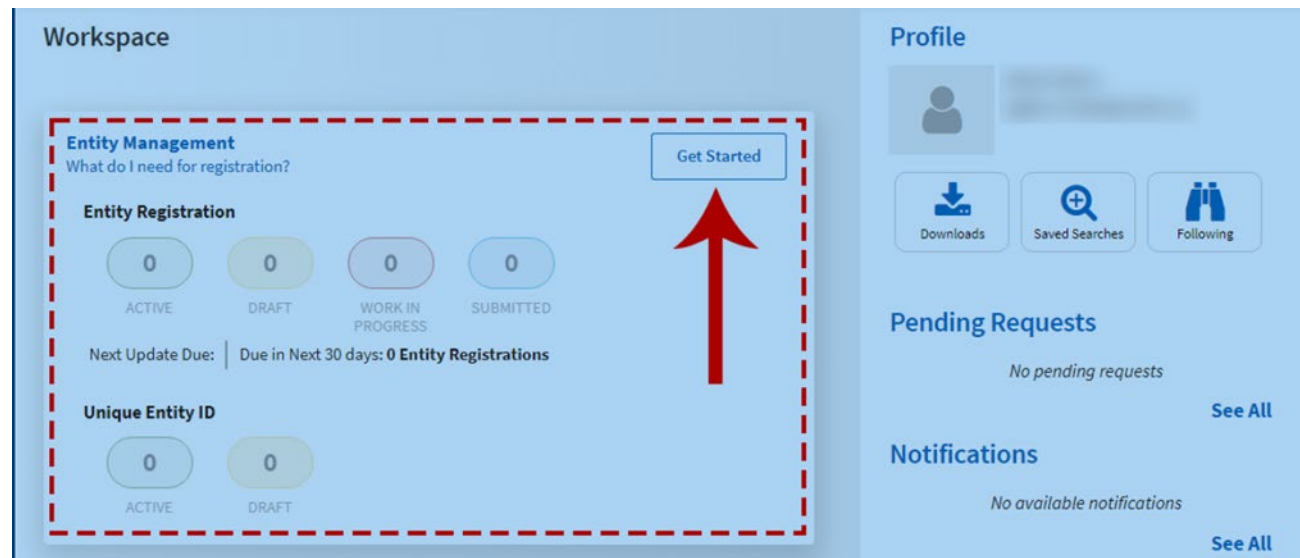
Entity Management workspace view. The 'DUNS' Unique Entity ID field is highlighted with a red arrow. The 'SAM' Unique Entity ID field is also visible. The 'Purpose of Registration' is 'Federal Assistance Awards'. The 'Registration Status' is 'Active' and the 'Expiration Date' is 'Jun 10, 2022'. The 'CAGE/NCAGE' field is at the bottom left.

Entity Management dashboard. The 'Entity Registration' section shows five status bubbles: ACTIVE (1), DRAFT (1), WORK IN PROGRESS (0), SUBMITTED (0), and PHRR (0). The 'Unique Entity ID' section shows four bubbles: ACTIVE (0), DRAFT (0), WORK IN PROGRESS (0), and SUBMITTED (0). The 'Next Update Due' is 'Jun 10, 2022' and 'Due in Next 30 days: 0 Entity Registrations'. A 'Register Entity' button is in the top right.

# UNIQUE ENTITY IDENTIFIER

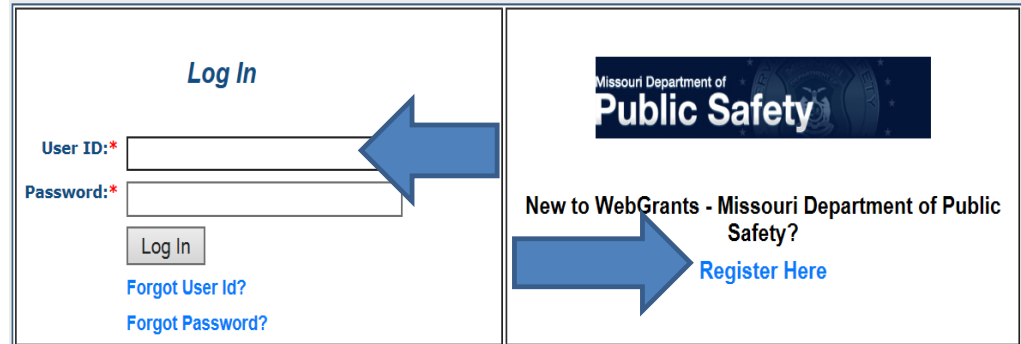
If your agency did not have a DUNS number, you will follow the steps below to obtain a UEI

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



# 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



**Log In**

User ID:\*

Password:\*

[Forgot User Id?](#)

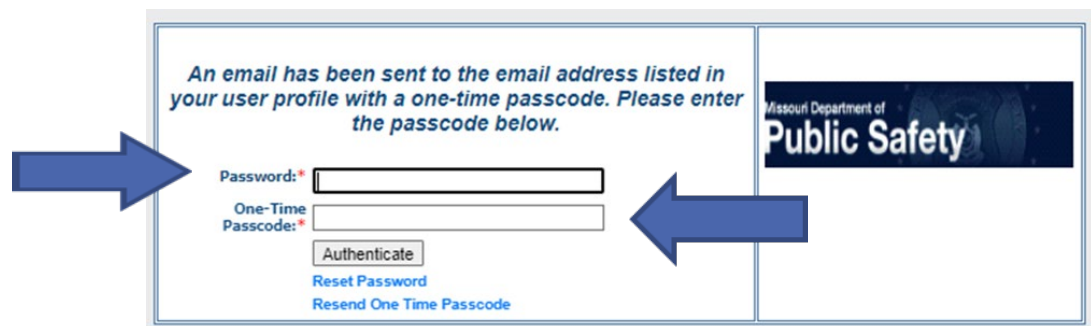
[Forgot Password?](#)

**Missouri Department of Public Safety**

New to WebGrants - Missouri Department of Public Safety?

[Register Here](#)

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



An email has been sent to the email address listed in your user profile with a one-time passcode. Please enter the passcode below.

Password:\*

One-Time Passcode:\*

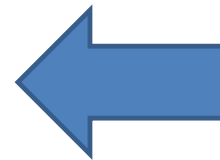
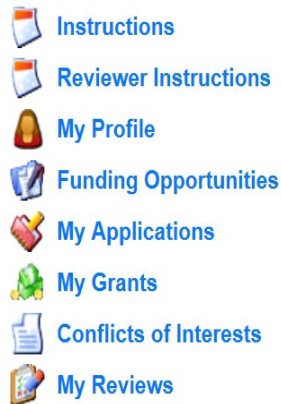
[Reset Password](#)

[Resend One Time Passcode](#)

**Missouri Department of Public Safety**

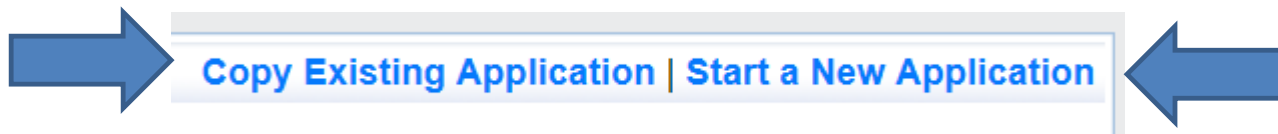
# APPLICATION INSTRUCTIONS

- Select “Funding Opportunities” and select the FY 2022 State and Local Cybersecurity Grant Program (SLCGP) funding opportunity



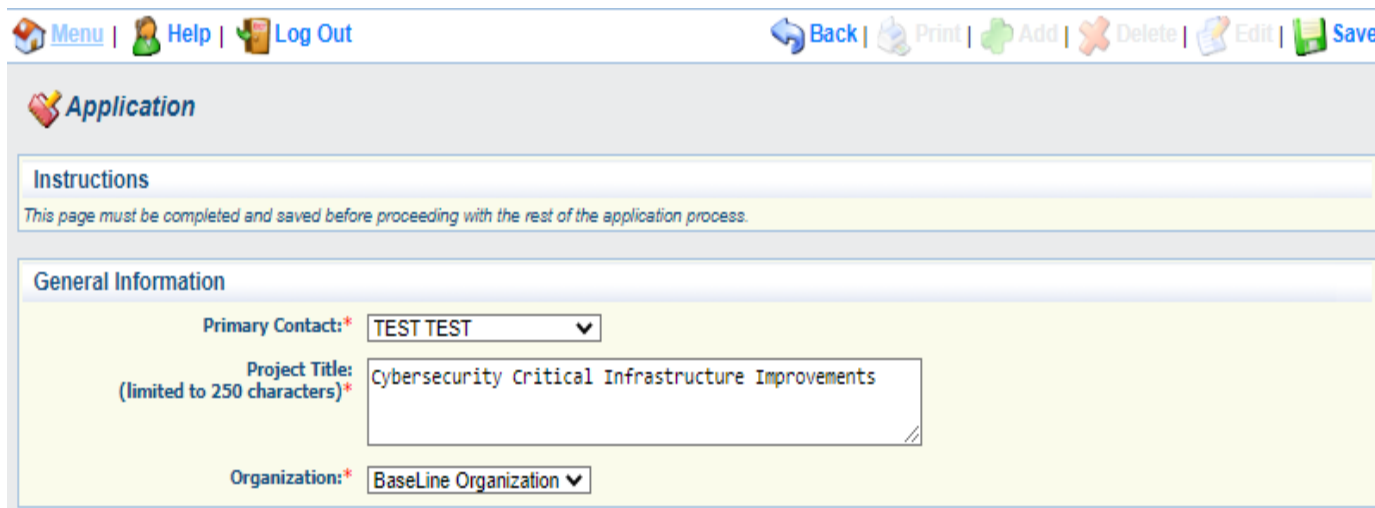
# APPLICATION INSTRUCTIONS

- Select “Start New Application”



# 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”



The screenshot shows a web application interface. At the top, there is a navigation bar with links: Menu, Help, Log Out, Back, Print, Add, Delete, Edit, and Save. Below this is a section titled "Application" with a sub-section "Instructions" containing the text: "This page must be completed and saved before proceeding with the rest of the application process." The main section is "General Information" and contains three fields: "Primary Contact:" with a dropdown menu showing "TEST TEST", "Project Title:" with a text box containing "Cybersecurity Critical Infrastructure Improvements" (noted as limited to 250 characters), and "Organization:" with a dropdown menu showing "BaseLine Organization". A large blue arrow points to the "Save" button in the top navigation bar.

Menu | Help | Log Out | Back | Print | Add | Delete | Edit | Save

**Application**

**Instructions**

*This page must be completed and saved before proceeding with the rest of the application process.*

**General Information**

Primary Contact:\* TEST TEST ▼

Project Title:  
(limited to 250 characters)\* Cybersecurity Critical Infrastructure Improvements

Organization:\* BaseLine Organization ▼

# APPLICATION INSTRUCTIONS

- Select “Go to Application Forms”



General Information	<a href="#">Go to Application Forms</a>
System ID: 146266	
Project Title: Cybersecurity Critical Infrastructure Improvements	
Primary Contact: TEST TEST	
Organization: BaseLine Organization	

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



Application Forms		Application Details   <a href="#">Submit</a>   <a href="#">Withdraw</a>	
	Form Name	Complete?	Last Edited
<a href="#">General Information</a>		✓	10/20/2022
<a href="#">Project Package</a>		✓	10/31/2022
<a href="#">Budget</a>		✓	10/24/2022
<a href="#">Contact Information</a>		✓	10/24/2022
<a href="#">Named Attachments</a>		✓	10/24/2022



# CONTACT INFORMATION

## ■ Authorized Official

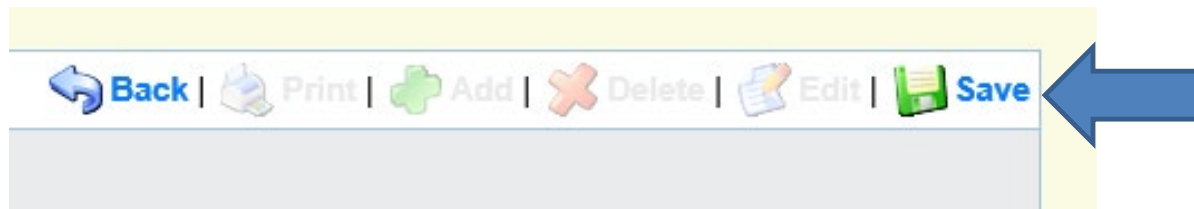
The Authorized Official is the individual who has the authority to legally bind the applicant into a contract and is generally the applicant's elected or appointed chief executive. For example:

- 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

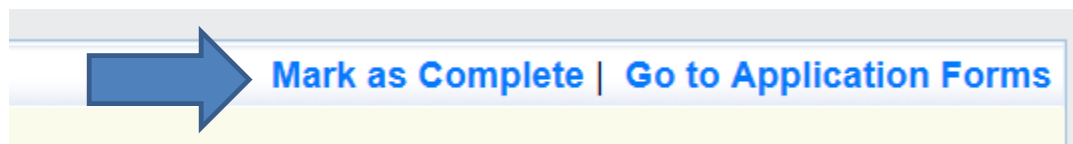
**In order for an application to be considered eligible for funding, the agency's correct Authorized Official MUST be designated in the "Contact Information" form and the "Certified Assurances" form**

# 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 \*
- Click “Save” at the top of the screen after entering all of the information



- Then “Mark as Complete”



# SLCGP PROJECT PACKAGE

- All of the “SLCGP Project Package” information has been combined into one form with four sections
  - Project Worksheet
  - Audit
  - Risk Assessment
  - Certified Assurances

# PROJECT WORKSHEET

## SLCGP Project Package

### Project Worksheet

1. Project Title:\*

2. Please select from the dropdown menu if the applicant agency's jurisdiction is located within a rural area, non-rural area, or is a state agency. A rural area is defined in 49 U.S.C. section 5302 as an area 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. \*

3. Please list the population for the applicant agency's jurisdiction. For example, if the applicant agency is a city, the city's population should be provided. If the applicant agency is a county, the county's population should be provided. If your agency is a state agency, enter N/A. \*

- 1. – Please provide an appropriate title to describe your agency's requested project.
- 2. - Select from the dropdown, Rural, Non-Rural, State based on your agency's jurisdiction.
  - Rural area is defined as an area 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.
- 3. – Please provide the population for your agency's jurisdiction.

# PROJECT WORKSHEET

4. Please give a brief overall description of your requested project. \*

Please give a brief description of the overall project.

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

Please include each item that will be purchased with a description of how the item will be used to support your project objectives.

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

Please provide details on the duration of the requested project.

7. Why is this project necessary for your agency/region/state? \*

Please explain why this project is necessary for your agency/region/state.

- 4. – Please provide a description of the overall requested project.
- 5. – Please list all items requested in this project and how they will support the project.
- 6. – Please provide details of the duration of the requested project.
- 7. – Please provide detail on why this requested project will benefit your agency.

# PROJECT WORKSHEET

8. To be eligible to receive SLCGP funding, the applicant agency must have a completed cybersecurity risk assessment. Is the completed assessment the Nationwide Cybersecurity Review (NCSR)?\*

☒ Yes ☐ No

8.1. Please indicate the NCSR maturity scale rating for each section of the applicant agency's most recent NCSR.


Identify:

Protect:

Detect:

Respond:

Recover:

8.1.a. Date of most current NCSR Assessment:  

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

Please explain how this requested project will help your agency close gaps and strengthen capabilities identified in your agency's NCSR.

- 8. – To be **ELIGIBLE** to receive SLCGP Funding you must have a Cybersecurity risk assessment completed. Is the completed assessment the NCSR?
- 8.1 – When **YES** is selected on question 8, please list your maturity scale ratings for each section: Identify, Protect, Detect, Respond, and Recover from your most recent NCSR.
- 8.1.a. – Please list the completion date of your agency's most recent NCSR.
- 8.2 – Please explain how this requested project will help close gaps and strengthen capabilities identified in your agency's NCSR assessment.

# PROJECT WORKSHEET

8. To be eligible to receive SLCGP funding, the applicant agency must have a completed cybersecurity risk assessment. Is the completed assessment the Nationwide Cybersecurity Review (NCSR)?\*

☐ Yes ☒ No

8.1. Please indicate what cybersecurity risk assessment your agency completed.

Name of risk assessment

8.1.a. Date of most current Cybersecurity Assessment:

12/31/2021



8.2. Please explain how this project will help close gaps and strengthen capabilities identified in your agency's cybersecurity risk assessment.

Please explain how the requested project will help your agency close gaps and strengthen capabilities identified in your agency's cybersecurity assessment.

- 8. – To be **ELIGIBLE** to receive SLCGP Funding you must have a Cybersecurity risk assessment completed. Is the completed assessment the NCSR?
- 8.1 – When **NO** is selected on question 8, please indicate which cybersecurity assessment was completed.
- 8.1.a. – Please list the completion date of your agency's cybersecurity risk assessment.
- 8.2 – Please explain how this requested project will help close gaps and strengthen capabilities identified in your cybersecurity risk assessment.

# PROJECT WORKSHEET

9. Which of the NIST Functions will your project fulfill?\*

Identify  
Protect  
Detect  
Respond  
Recover

Please press Ctrl + Click to select multiple items

10. 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) or other cybersecurity risk assessment. Note: The NCSR or other cybersecurity risk assessment is subject to review by the Missouri Office of Homeland Security (OHS).\*

☒

- 9. – Please select which of the NIST functions your requested project will address. (Press Ctrl + Click to select multiple items)
- 10. – Checking this box indicates your agency attests the requested project works to close gaps and strengthen capabilities in the NCSR or other cybersecurity risk assessment.



# PROJECT WORKSHEET

11. Does your agency have cybersecurity and/or data security policies?\*

☒ Yes ☐ No

11.1. Please describe your agency's policies.

Describe your agency's policies.

11. Does your agency have cybersecurity and/or data security policies?\*

☐ Yes ☒ No

11.1. Will this project assist your agency in developing cybersecurity and/or data security policies?

☒ Yes ☐ No

11.1.a. Please explain how this project will assist in developing cybersecurity and/or data security policies.

Explain how this project will assist in developing cybersecurity and/or data security policies.

■ 11. Does your agency have cybersecurity and/or data security policies?

■ 11.1 If **YES**, describe your agency's policies.

■ 11.1 If **NO**, will this project assist your agency in developing cybersecurity and/or data security policies?

■ 11.1.a If **YES**, explain how this project will assist in developing cybersecurity and/or data security policies.

# PROJECT WORKSHEET

12. Does your agency have a cybersecurity training awareness program? ☒ Yes ☐ No

12.1. Please describe your agency's training awareness program.

Describe your agency's training awareness program.

12. Does your agency have a cybersecurity training awareness program? ☐ Yes ☒ No

12.1. Will this project assist your agency in developing a cybersecurity training awareness program? ☒ Yes ☐ No

12.1.a. Please explain how this project will assist your agency in developing a cybersecurity training awareness program.

Explain how this project will assist in developing a cybersecurity training awareness program.

■ 12. Does your agency have a cybersecurity training awareness program?

■ 12.1 If **YES**, describe your agency's training awareness program.

■ 12.1 If **NO**, will this project assist your agency in developing a cybersecurity training awareness program?

■ 12.1.a If **YES**, explain how this project will assist in developing a cybersecurity training awareness program.

# PROJECT WORKSHEET

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

☒ Yes ☐ No

13.1. Please describe your agency's cybersecurity incident response plan.

Describe your agency's cybersecurity incident response plan.

13.1.a. Is your agency's cybersecurity incident response plan CISA approved?

☐ Yes ☒ No

13.1.b. Does your agency train/exercise your cybersecurity incident response plan?

☒ Yes ☐ No

13.1.c. Please describe the training/exercising of your incident response plan.

Describe the training/exercising of your incident response plan.

13.1.b. Does your agency train/exercise your cybersecurity incident response plan?

☐ Yes ☒ No

13.1.c. Why does your agency not train/exercise your plan?

Explain why your agency does not train/exercise your plan.

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

☐ Yes ☒ No

13.1. Will the requested project assist in the development of a cybersecurity incident response plan?

☒ Yes ☐ No

- 13. Does your agency have a cybersecurity incident response plan?
- 13.1 If **YES**, describe your agency's cybersecurity incident response plan.
  - 13.1.a Is your agency's cybersecurity incident response plan CISA approved?
  - 13.1.b Does your agency train/exercise your cybersecurity incident response plan?
  - 13.1.c If **YES**, describe the training/exercising of your incident response plan.
  - 13.1.c If **NO**, why does your agency not train/exercise your plan?
- 13.1 If **NO**, will this project assist in the development of a cybersecurity incident response plan?

# PROJECT WORKSHEET

14. Does your agency receive cybersecurity threat intelligence?\*

☒ Yes ☐ No

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

Describe the sources of threat intelligence.

- 14. Does your agency receive cybersecurity threat intelligence?
- 14.1 If **YES**, describe the sources of threat intelligence. (i.e., federal, state, local, private sector/vendor)

# PROJECT WORKSHEET

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

☒ Yes ☐ No

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

☐ Yes ☒ No

15.1. 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.

- 15. Does your agency participate in information sharing with federal, state, and local agencies? (i.e., Missouri Office of Homeland Security (OHS), Missouri Information Analysis Center (MIAC), St. Louis Fusion Center, Kansas City Regional Fusion Center)
- 15.1 If **NO**, explain why your agency does not participate in information sharing with federal, state, and local agencies.

# PROJECT WORKSHEET

16. Does your agency subscribe to the Missouri Office of Homeland Security (OHS) Cybersecurity Program? ☒ Yes ☐ No

16.1. Would your agency like to subscribe to the Missouri Office of Homeland Security (OHS) Cybersecurity Program? ☒ Yes ☐ No  
If yes, please email [SecurityIntel@mshp.dps.mo.gov](mailto:SecurityIntel@mshp.dps.mo.gov) with your name, agency/entity, title, desk phone, work phone, and email address.

- 16. Does your agency subscribe to the Missouri Office of Homeland Security (OHS) Cybersecurity Program?
- 16.1 If **NO**, would your agency like to subscribe to the Missouri Office of Homeland Security (OHS) Cybersecurity Program?
- If yes, please email [securityintel@mshp.dps.mo.gov](mailto:securityintel@mshp.dps.mo.gov) with your name, agency/entity, title, desk phone, work phone, and email address.

# PROJECT WORKSHEET

17. Does the requested project align to any of the state of Missouri established priorities for the FY 2022 SLCGP? The priorities are listed in the FY 2022 SLCGP Notice of Funding Opportunity.

☒ Yes ☐ No

17.1. Please select which priority(s) your project aligns with.

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

Please press Ctrl + Click to select multiple items

17.1.a. Please explain how your project aligns to the priorities selected in question 17.1.

Explain how your project aligns to the priorities selected in question 17.1

■ 17. Does your project align to any of the state of Missouri established priorities for the FY 2022 SLCGP? Priorities are listed in the FY 2022 SLCGP Notice of Funding Opportunity.

■ 17.1 If **YES**, select which priority(s) your project aligns with. (Press Ctrl + Click to select multiple items)

■ 17.1.a Explain how your project aligns to the priorities selected in 17.1.

# PROJECT WORKSHEET

- 18. – Please select the objective, sub-objective, and outcome your requested project aligns with. The objectives, sub-objectives, and outcomes of the FY2022 SLCGP are discussed in detail in Appendix A of the FY 2022 SLCGP NOFO. Your agency's requested project may align to more than one objective, sub-objective, and outcome.
- 18.a. – Select yes or no depending on whether your agency's requested project aligns with another objective, sub-objective, and outcome.
- \*You may select up to 20 objectives, sub-objectives, and outcomes\*



# PROJECT WORKSHEET

18. Please select the SLCGP objective, sub-objective, and outcome your project aligns with. The objectives, sub-objectives, and outcomes of the FY 2022 SLCGP are discussed in detail in Appendix A of the FY 2022 SLCGP NOFO. The requested project may align to more than one objective, sub-objective, and outcome.

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

Sub-Objective:\* Sub-Objective 1.2 - Develop, implement, or revise, and test cybersecurity plans, including cyber incident response plans, with clearly defined roles and respon

Outcome:\* Outcome 1.2.1 - Develop, implement, or revise, and exercise cyber incident response plans. ▼

18.a. Does your project aligns with an additional objective, sub-objective, and outcome?\*

Yes ▼

18.1. Please select the SLCGP objective, sub-objective, and outcome your project aligns with. The requested project may align to more than one objective, sub-

Objective:

Sub-Objective: ▼

Outcome: ▼

# PROJECT WORKSHEET

19. Please explain how the requested project aligns with the Missouri Cybersecurity Plan.\*

Explain how the requested project aligns with the Missouri Cybersecurity Plan.

- 19. Please explain how the requested project aligns with the Missouri Cybersecurity Plan.

# PROJECT WORKSHEET

20. Will this project assist in developing a CISA approved cybersecurity plan?\*

☒ Yes ☐ No

20.1. Explain how your project will assist in developing a CISA approved cybersecurity plan.

Explain how your project will assist in developing a CISA approved cybersecurity plan.

21. Will this project conduct annual table-top or full-scope exercises to test the agency's cybersecurity plan?\*

☐ Yes ☒ No

22. Does your agency perform phishing training?\*

☒ Yes ☐ No

22.1 Please explain the phishing training your agency performs.

Explain the phishing training your agency performs.

22. Does your agency perform phishing training?\*

☐ Yes ☒ No

22.1 Will this project assist your agency in performing phishing training?

☒ Yes ☐ No

22.1.a Please explain how this project will assist your agency in performing phishing training.

Explain how this project will assist your agency in performing phishing training.

■ 20. Will this project assist in developing a CISA approved cybersecurity plan?

■ 20.1 If **YES**, explain how your project will assist in developing a CISA approved plan.

■ 21. Will this project conduct annual table-top or full-scope exercises to test the agency's cybersecurity plan?

■ 22. Does your agency perform phishing training?

■ 22.1 If **YES**, explain the phishing training performed.

■ 22.1 If **NO**, will this project assist your agency in performing phishing training?

■ 22.1.a If **YES**, explain how this project will assist your agency in performing phishing training.

# PROJECT WORKSHEET

23. Does your agency conduct cybersecurity awareness campaigns?\*

☒ Yes ☐ No

23.1. Please explain the cybersecurity awareness campaigns your agency conducts.

Explain the cybersecurity awareness campaigns your agency conducts.

23. Does your agency conduct cybersecurity awareness campaigns?\*

☐ Yes ☒ No

23.1. Will this project assist your agency in conducting awareness campaigns?

☒ Yes ☐ No

23.1.a. Please explain how this project will assist your agency in conducting awareness campaigns.

Explain how this project will assist your agency in conducting awareness campaigns.

- 23. Does your agency conduct cybersecurity awareness campaigns?
  - 23.1 If **YES**, explain the cybersecurity awareness campaigns your agency conducts.
  - 23.1 If **NO**, will this project assist your agency in conducting awareness campaigns?
    - 23.1.a If **YES**, explain how this project will assist your agency in conducting awareness campaigns.

# PROJECT WORKSHEET

24. Does your agency provide role-based cybersecurity awareness training to employees?\*

☒ Yes ☐ No

24.1. Please explain the role-based cybersecurity awareness training that is provided to employees.

Explain the role-based cybersecurity training that is provided.

24. Does your agency provide role-based cybersecurity awareness training to employees?\*

☐ Yes ☒ No

24.1. Will this project assist your agency in providing role-based cybersecurity awareness training to employees?

☒ Yes ☐ No

24.1.a. Please explain how this project will assist your agency in providing role-based cybersecurity training to employees?

Explain how this project will assist your agency in providing role-based cybersecurity training.

■ 24. Does your agency provide role-based cybersecurity awareness training to employees?

■ 24.1 If **YES**, explain the role-based cybersecurity awareness training that is provided to employees.

■ 24.1 If **NO**, will this project assist your agency in providing role-based cybersecurity awareness training to employees?

■ 24.1.a If **YES**, explain how this project will assist your agency in providing role-based cybersecurity training to employees.

# PROJECT WORKSHEET

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

☒ Yes ☐ No

25.1. 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.

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

☐ Yes ☒ No

25.1. Will this project help your agency in developing a NICE Framework?

☒ Yes ☐ No

25.1.a. Please explain how this project will assist in developing a NICE Framework and how your agency plans to implement the Framework?

Explain how this project will assist in developing a NICE framework and how your agency plans to implement the framework.

■ 25. Does your agency have in place the NICE framework for workforce development and training plans?

■ 25.1 If **YES**, explain how your agency implements your current NICE framework components into your work flows.

■ 25.1 If **NO**, will this project help your agency in developing a NICE framework?

■ 25.1.a If **YES**, explain how this project will assist in developing a NICE framework and how your agency plans to implement the framework.

# PROJECT WORKSHEET

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

☒ Yes ☐ No

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

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

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

☐ Yes ☒ No

26.1. Will this project assist your agency in developing capabilities to analyze network traffic and activities related to potential threats?

☒ Yes ☐ No

26.1.a. Please explain how this project will assist your agency in developing capabilities to analyze network traffic and activities related to potential threats?

Explain how this project will assist your agency in developing capabilities to analyze network traffic and activities related to potential threats.

■ 26. Does your agency have the capabilities to analyze network traffic and activities related to potential threats?

■ 26.1 If **YES**, explain how your agency currently analyzes network traffic and activities related to potential threats.

■ 26.1 If **NO**, will this project assist your agency in developing capabilities to analyze network traffic and activities related to potential threats?

■ 26.1.a If **YES**, explain how this project will assist your agency in developing capabilities to analyze network traffic and activities related to potential threats.

# PROJECT WORKSHEET

27. Does your agency implement multi-factor authentication (MFA) for all remote access and privileged accounts?\*

☒ Yes ☐ No

27.1. Please explain how your agency currently implements multi-factor authentication for all remote access and privileged accounts.

Explain how your agency currently implements multi-factor authentication for all remote access and privileged accounts.

27. Does your agency implement multi-factor authentication (MFA) for all remote access and privileged accounts?\*

☐ Yes ☒ No

27.1. Will this project assist your agency in implementing multi-factor authentication for all remote access and privileged accounts?

☒ Yes ☐ No

27.1.a. Please explain how this project will assist your agency in implementing multi-factor authentication for all remote access and privileged accounts?

Explain how this project will assist your agency in implementing multi-factor authentication for all remote access and privileged accounts.

■ 27. Does your agency implement multi-factor authentication (MFA) for all remote access and privileged accounts?

■ 27.1 If **YES**, explain how your agency currently implements multi-factor authentication for all remote access and privileged accounts.

■ 27.1 If **NO**, will this project assist your agency in implementing multi-factor authentication for all remote access and privileged accounts?

■ 27.1.a If **YES**, explain how this project will assist your agency in implementing multi-factor authentication for all remote access and privileged accounts.



# PROJECT WORKSHEET

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

☒ Yes ☐ No

28.1. 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.

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

☐ Yes ☒ No

28.1. Will this project assist your agency in developing a program to identify and eliminate the use of end of life software and hardware?

☒ Yes ☐ No

28.1.a. Please explain how this project will assist your agency in developing a program to identify and eliminate the use of end of life software and hardware?

Explain how this project will assist your agency in developing a program to identify and eliminate the use of end of life software and hardware.

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

■ 28.1 If **YES**, explain the process your agency uses to identify and eliminate the use of end of life software and hardware.

■ 28.1 If **NO**, will this project assist your agency in developing a program to identify and eliminate the use of end of life software and hardware?

■ 28.1.a If **YES**, explain how this project will assist your agency in developing a program to identify and eliminate the use of end of life software and hardware.

# PROJECT WORKSHEET

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

☒ Yes ☐ No

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

☐ Yes ☒ No

29.1. Will this project assist your agency to implement prohibiting known/fixed/default passwords and credentials?

☒ Yes ☐ No

■ 29. Does your agency prohibit known/fixed/default passwords and credentials?

■ 29.1 If **NO**, will this project assist your agency to implement prohibiting known/fixed/default passwords and credentials?

# PROJECT WORKSHEET

30. Does your agency operate under a .gov internet domain?\* ☒ Yes ☐ No

30. Does your agency operate under a .gov internet domain?\* ☐ Yes ☒ No

30.1. Is your agency planning to transition to a .gov internet domain under this project? ☒ Yes ☐ No

■ 30. Does your agency operate under a .gov domain?

■ 30.1 If **NO**, is your agency planning to transition to a .gov internet domain under this project?

# PROJECT WORKSHEET

31. Will your agency be utilizing cash (hard) match to meet the 10% match requirement?\*

☒ Yes ☐ No

31.1. If cash match will be utilized, please describe the source of the cash.

Describe the source of the cash

- 31. Will your agency be utilizing cash (hard) match to meet the 10% match requirement?
- 31.1 If **YES**, describe the source of the cash.

# PROJECT WORKSHEET

32. Will your agency be utilizing in-kind (soft) match to meet the 10% match requirement?\*

☒ Yes ☐ No

32.1. If in-kind match will be utilized, please describe the in-kind match.

Describe the in-kind match.

32.2. Please describe how the in-kind match relates to the requested project.

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

32.3 Will the agency be able to provide supporting documentation for the in-kind match?

☒ Yes ☐ No

32.4 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.



- 32. Will your agency be utilizing in-kind (soft) match to meet the 10% match requirement?
  - 32.1 If **YES**, describe the in-kind match.
  - 32.2 If **YES**, describe how the in-kind match relates to the requested project.
  - 32.3 If **YES**, will the agency be able to provide supporting documentation for the in-kind match?
  - 32.4 If **YES**, check the box to attest the in-kind match has not and/or will not be utilized to fulfill a match requirement on any other Federal grant.

# PROJECT WORKSHEET

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

Explain how your agency plans to financially sustain the requested items in the future without grant funding.

- 33. How does your agency plan to financially sustain the requested items in the future WITHOUT grant funding?

# 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
- Please upload your Schedule of Expenditures of Federal Awards (SEFA) for the period covering your agency's last fiscal year if this is not already included in your audit
- All attachments will be uploaded in the "Named Attachment" form on the application

# AUDIT

- Using your most recent audit, annual financial statement, and/or SEFA, complete the “Audit Certification” 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)



# AUDIT

## Audit

34. 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

35. Date last audit completed: MM/DD/YYYY \*

12/31/2021

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

36. 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. \*



# 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

## Risk Assessment

37. 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.

37.1. Please list the name(s) of new personnel and their title(s)

List names of new personnel and their titles.

38. 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.

39. 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.

39.1. Please list the direct Federal awards the agency receives.

List direct Federal awards the agency receives.

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

☒ Yes ☐ No

39.2.a. 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.

# CERTIFIED ASSURANCES

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

## 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 agency.  
SLCGP Certified Assurances

40. 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 grant. **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 official.

- 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 a designee is being utilized to authorize the application, the Missouri Department of Public Safety (DPS) reserves the right to request documentation that it is a valid application submission.

\*\*The above list is not an all-inclusive list. If you do 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) for assistance.

41. Authorized Official Name and Title: \*

42. Name and Title of person completing this application: \*

43. Date: \*



**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**

# BUDGET

Enter each budget line by selecting “Add” and completing all required information, then “Save” and “Add” if additional budget lines are needed

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

# BUDGET

Equipment

Add

All equipment items are defined as tangible property having an acquisition cost of \$1,000 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.

Item Name:	AEL #:	Quantity:	Unit Cost:	Total Cost:	Local Match Amount:	Type of Match:	Function:	Federal Amount:
				\$0.00	\$0.00			\$0.00

Menu | Help | Log Out

Back | Print | Add | Delete | Edit | Save

Application

Application: 147151 - FY 2022 SLCGP Test

Program Area: State and Local Cybersecurity Grant Program (SLCGP)

Funding Opportunities: 147047 - FY 2022 State and Local Cybersecurity Grant Program (SLCGP) TEST

Application Deadline: Final Application Deadline not Applicable

Organization: BaseLine Organization

Equipment

All equipment items are defined as tangible property having an acquisition cost of \$1,000 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.

Item Name:\*

Firewall

AEL #:\*

05NP-00-FWAL

Quantity:\*

1.0

Unit Cost:\*

\$10,000.00

Total Cost:\*

\$10,000.00

Match Amount:\*

\$1,000.00

Type of Match:\*

Cash

In-Kind

Function:\*

Equipment




Please press Ctrl + Click to select multiple items







- The Federal amount of funds requested will automatically calculate based on the match requirement
- $\text{Total Cost} = \text{Local Match Amount} + \text{Federal Amount Requested}$


# BUDGET

- Provide required justification for all budget lines by clicking “Edit” at top of the page
- Justification for all sections can be completed at one time



 Menu |  Help |  Log Out

 Back |  Print |  Add |  Delete |  Edit |  Save

 **Application**

**Application: 146266 - Cybersecurity Critical Infrastructure Improvements**

**Program Area:** State and Local Cybersecurity Grant Program (SLCGP)

**Funding Opportunities:** 146160 - SLCGP - Test

**Application Deadline:** Final Application Deadline not Applicable

**Organization:** BaseLine Organization

# BUDGET

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

## Narrative Justification - Equipment

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

Provide separate justifications for each line item being requested. Address why the requested item is necessary for the success of the proposed project. Indicate amount requested. For example: (3 laptops @ \$1,500.00 each)

Please provide justification for the 10% match requirement. If utilizing cash match, provide the source of the cash. If utilizing in-kind match, describe the source a

Rich text editor toolbar with icons for: Cut, Copy, Paste, Undo, Redo, Bold, Italic, Underline, Link, Unlink, Bulleted List, Numbered List, Indent, Outdent, and various alignment options.

Justify the items to purchased, in accordance with the above listed instructions.

- 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” 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 10% 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 10% 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 10% 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 \$1,000.00 or more
- Authorized Equipment List (AEL) Number is required on the budget, the link to the site provided is in the instructions

## Equipment

*All equipment items are defined as tangible property having an acquisition cost of \$1,000 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.*



# BUDGET

■ Search the site for the correct AEL number

## Authorized Equipment List

The Authorized Equipment List (AEL) is a list of approved equipment types allowed under FEMA's preparedness grant programs. The intended audience of this tool is emergency managers, first responders, and other homeland security professionals. The list consists of 21 equipment categories divided into categories, sub-categories and then individual equipment items. NOTE: There are no commercially available products listed; it only consists of equipment types.

Download CSV

### Search

Search by item number, item title, keyword, or grant program and then click Apply. Search results display below.

### Section

06 - Interoperable Communications Equipment



### Category

- Please select -



- Please select -

Select a primary section, category and sub-category and then click Apply.

Apply

# 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 10% 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 10% 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 10% 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
  - Federal Funds Schedule (if not included in the audit)
- Other Supporting Attachments (if applicable)
  - Quotes or other cost basis
  - Other supporting information (up to 5 attachments)

# NAMED ATTACHMENTS

- To add each attachment select the name of the attachment

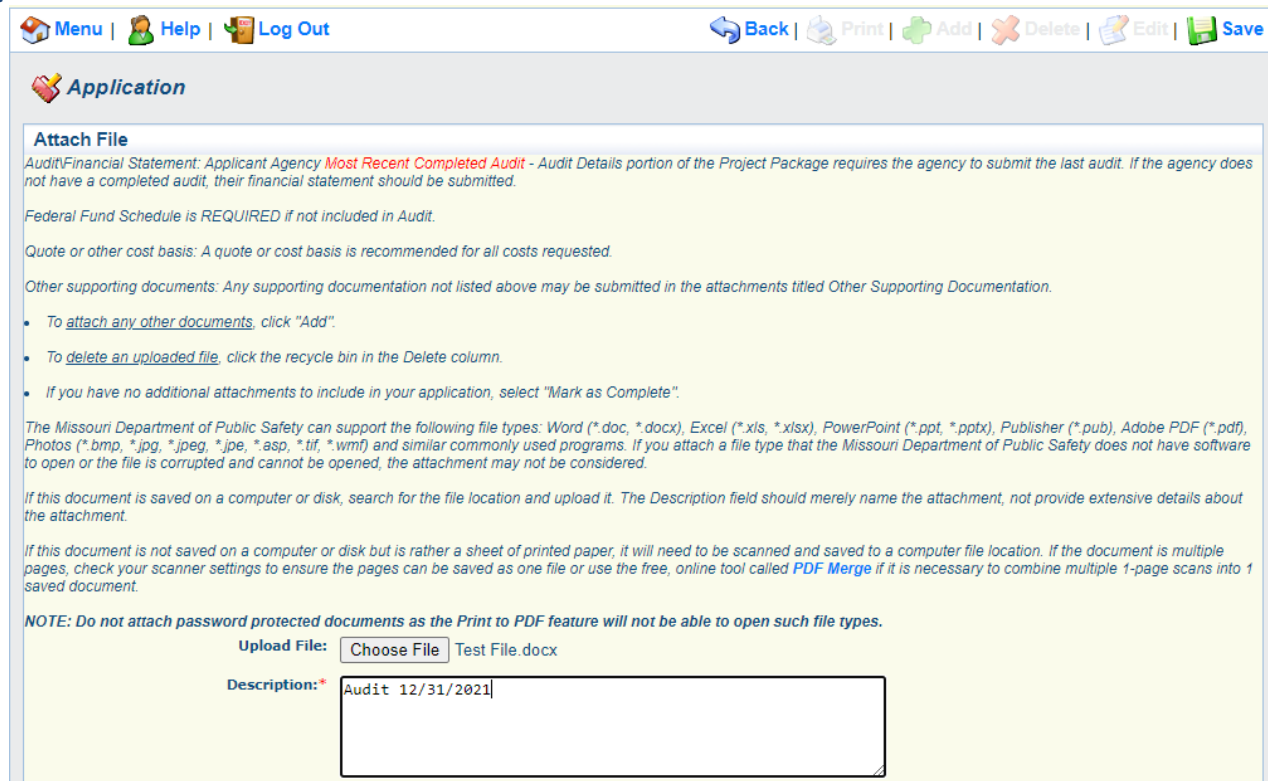


Named Attachments							<a href="#">Mark as Complete</a>   <a href="#">Go to Application Forms</a>
Attachment	Description	File Name	Type	File Size	Date Uploaded	Delete?	
<a href="#">Audit/Financial Statement (REQUIRED)*</a>							
<a href="#">Federal Fund Schedule (REQUIRED if not included in Audit)</a>							
<a href="#">Quote or other costs basis</a>							
<a href="#">Other Supporting Information</a>							
<a href="#">Other Supporting Information</a>							
<a href="#">Other Supporting Information</a>							
<a href="#">Other Supporting Information</a>							
<a href="#">Other Supporting Information</a>							

- The applicant agency's most recent audit/financial statement and federal funds schedule are required documents and must be uploaded before the form can be marked complete

# NAMED ATTACHMENTS

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



The screenshot shows a web application interface for attaching files. At the top, there is a navigation bar with links for Menu, Help, and Log Out. To the right of the navigation bar are action buttons: Back, Print, Add, Delete, Edit, and Save. A large blue arrow points to the 'Save' button. Below the navigation bar is a section titled 'Application'. Under this section is a form titled 'Attach File'. The form contains several paragraphs of instructions and a list of bullet points. At the bottom of the form, there is a section for 'Upload File' with a 'Choose File' button and a text input field for 'Description:'. The text input field contains the text 'Audit 12/31/2021'.

Menu | Help | Log Out

Back | Print | Add | Delete | Edit | Save

### Application

#### Attach File

AuditFinancial Statement: Applicant Agency **Most Recent Completed Audit** - Audit Details portion of the Project Package requires the agency to submit the last audit. If the agency does not have a completed audit, their financial statement should be submitted.

Federal Fund Schedule is **REQUIRED** if not included in Audit.

Quote or other cost basis: A quote or cost basis is recommended for all costs requested.

Other supporting documents: Any supporting documentation not listed above may be submitted in the attachments titled Other Supporting Documentation.

- To [attach any other documents](#), click "Add".
- To [delete an uploaded file](#), click the recycle bin in the Delete column.
- If you have no additional attachments to include in your application, select "Mark as Complete".

The Missouri Department of Public Safety can support the following file types: Word (\*.doc, \*.docx), Excel (\*.xls, \*.xlsx), PowerPoint (\*.ppt, \*.pptx), Publisher (\*.pub), Adobe PDF (\*.pdf), Photos (\*.bmp, \*.jpg, \*.jpeg, \*.jpe, \*.asp, \*.tif, \*.wmf) and similar commonly used programs. If you attach a file type that the Missouri Department of Public Safety does not have software to open or the file is corrupted and cannot be opened, the attachment may not be considered.

If this document is saved on a computer or disk, search for the file location and upload it. The Description field should merely name the attachment, not provide extensive details about the attachment.

If this document is not saved on a computer or disk but is rather a sheet of printed paper, it will need to be scanned and saved to a computer file location. If the document is multiple pages, check your scanner settings to ensure the pages can be saved as one file or use the free, online tool called [PDF Merge](#) if it is necessary to combine multiple 1-page scans into 1 saved document.

**NOTE: Do not attach password protected documents as the Print to PDF feature will not be able to open such file types.**

Upload File:  Test File.docx

Description:\*

# SUBMISSION

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



Application Forms		Application Details   <a href="#">Submit</a>   <a href="#">Withdraw</a>	
Form Name	Complete?	Last Edited	
<a href="#">General Information</a>	✓	10/20/2022	
<a href="#">Project Package</a>	✓	10/24/2022	
<a href="#">Budget</a>	✓	10/24/2022	
<a href="#">Contact Information</a>	✓	10/24/2022	
<a href="#">Named Attachments</a>	✓	10/24/2022	

# OFFICE OF HOMELAND SECURITY - CYBERSECURITY

Contact the Missouri Office of Homeland Security Cybersecurity for project specific questions:

Phone: 573-526-0153

Email: [securityintel@mshp.dps.mo.gov](mailto:securityintel@mshp.dps.mo.gov)

# OFFICE OF HOMELAND SECURITY - CYBERSECURITY

Contact the Missouri Office of Homeland Security Grants for grant or WebGrants specific questions:

**Chelse Dowell**

Grants Specialist

(573) 751-3879

[chelse.dowell@dps.mo.gov](mailto:chelse.dowell@dps.mo.gov)

**Kelsey Saunders**

Grant Support Specialist

(573) 522-6125

[kelsey.saunders@dps.mo.gov](mailto:kelsey.saunders@dps.mo.gov)

**Chelsey Call**

Grants Supervisor

(573) 526-9203

[chelsey.call@dps.mo.gov](mailto:chelsey.call@dps.mo.gov)

**Joni McCarter**

Program Manager

(573) 526-9020

[joni.mccarter@dps.mo.gov](mailto:joni.mccarter@dps.mo.gov)