STATE AND LOCAL CYBERSECURITY GRANT PROGRAM (SLCGP)

FY 2023 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 2023 State and Local Cybersecurity Grant Program (SLCGP) is open October 5, 2023 – November 17, 2023 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: FY 2023State and Local Cybersecurity Grant Program (SLCGP) Notice of Funding Opportunity (NOFO)**
  - **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)

- 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

October 5, 2023:	SLCGP funding opportunity opens in WebGrants https://dpsgrants.dps.mo.gov/
November 17, 2023:	SLCGP applications due in WebGrants **5:00 pm CST** ***WebGrants will not accept any applications after this time***
December/January 2023:	Cybersecurity Planning Committee application review/scoring
February 1, 2024:	Projected Project Start Date
January 31, 2027:	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 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 2023 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 2023 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 2023 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 2023 SLCGP NOFO

STATE PRIORITIES

- Missouri has established eight priority areas for FY 2023
  - 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) 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 extra points during the application scoring process**

FY 2023 ANTICIPATED FUNDING

- The Federal Notice of Funding Opportunity has estimated funding levels for the FY 2023 SLCGP for Missouri at $7,748,105
- Three funding sources available for FY 2023 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

- 20% 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

  Subrecipient's Share Percentage x Project Costs = Required Match

- **Example 1:** $$\frac{\$100{,}000}{80\%} = \$125{,}000 \text{ Total Project Costs}$$

  20% x $125,000 = $25,000 Subrecipient Cost Share

- **Example 2:** $$\frac{\$200{,}000}{80\%} = \$250{,}000 \text{ Total Project Costs}$$

  20% x $250,000 = $50,000 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 agencies must have completed the 2023 Nationwide Cybersecurity Review (NCSR). **The NCSR must be completed and results received at the time of application submission**.
- 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: It may take approximately 4-6 hours to complete the NCSR and the agency should allow up to two weeks to receive the results.**
  - 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 2023 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 be 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**

  Use of force incidents reporting standards and procedures, publication of report data, analysis report. Each law enforcement agency shall certify compliance with section 590.1265 RSMo when applying for any grants administered by 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 prior twelve month period.*

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 is required to submit crime incident reports to the department of public safety on forms or in the format prescribed by the department and 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 prior twelve month period.*

  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 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) which can be located in the WebGrants application
  - **MUST** align with at least one of the FY 2023 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 2023 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 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:

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

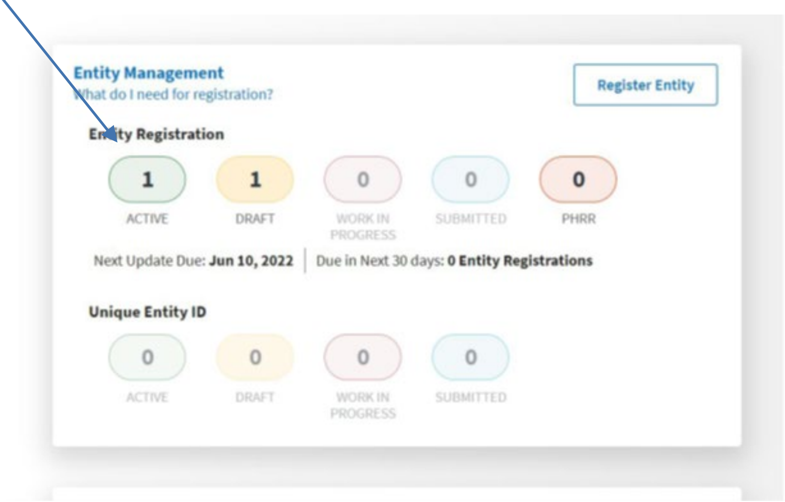
UNIQUE ENTITY IDENTIFIER

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



Entity Management

What do I need for registration?

Register Entity

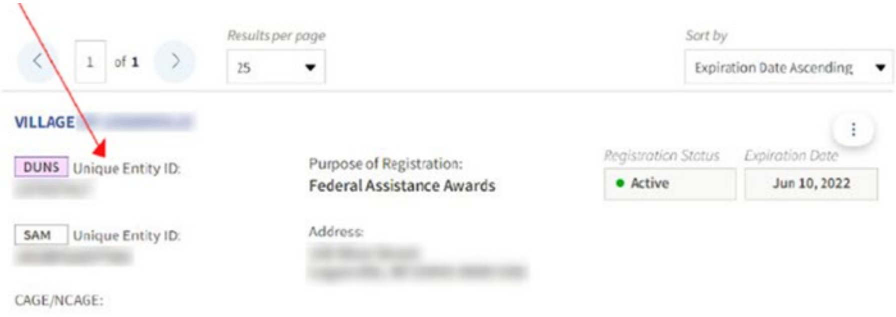
Entity Registration

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



< 1 of 1 >

Results per page: 25

Sort by: Expiration Date Ascending

VILLAGE [redacted]

DUNS Unique Entity ID: [redacted]

Purpose of Registration: Federal Assistance Awards

Registration Status: ● Active

Expiration Date: Jun 10, 2022

SAM Unique Entity ID: [redacted]

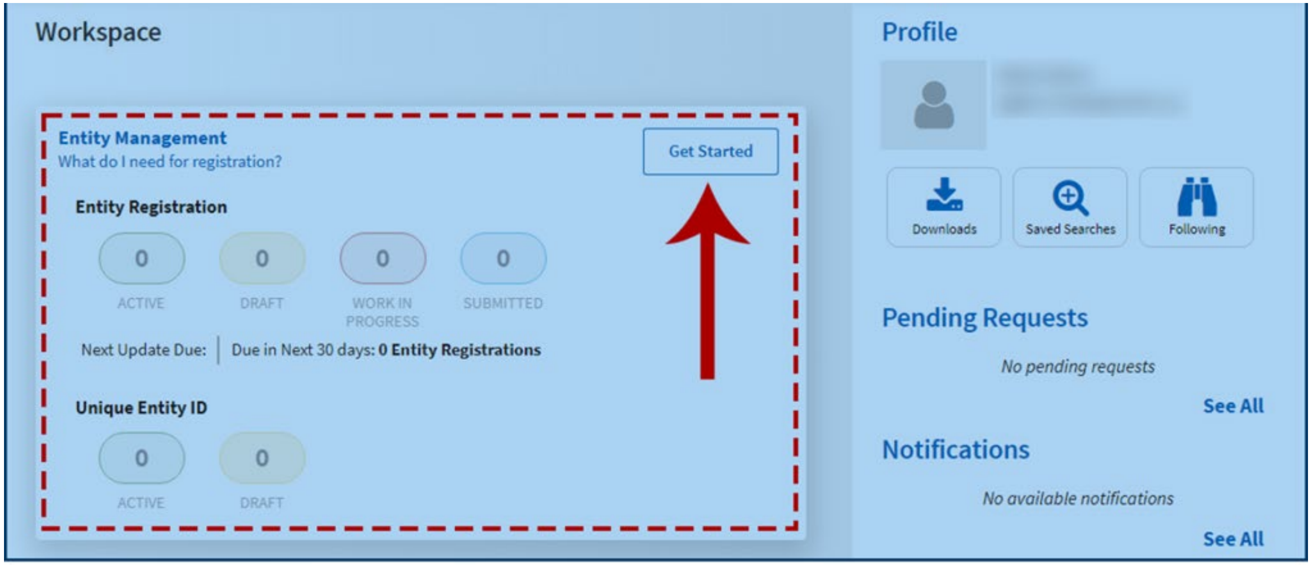
Address: [redacted]

CAGE/NCAGE:

UNIQUE ENTITY IDENTIFIER

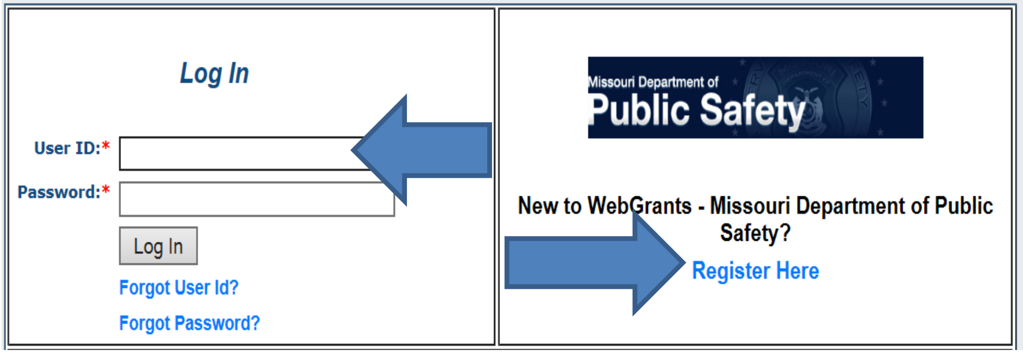
If your agency did not have a DUNS number, you will follow the steps below to obtain a UEI

- 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



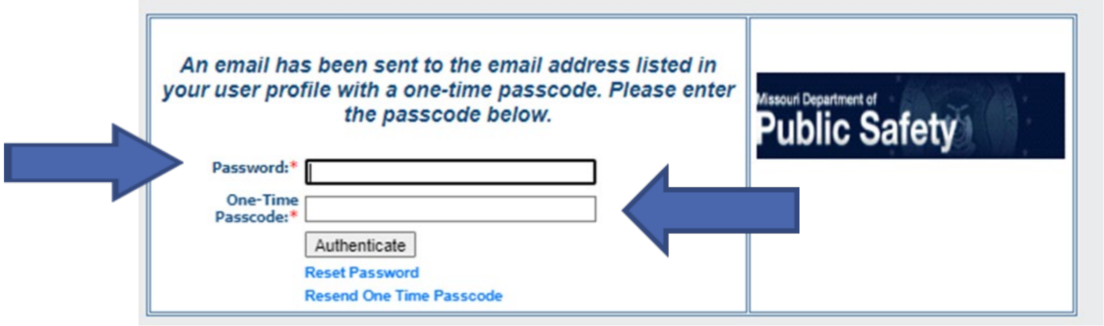
Log In

User ID:*

Password:*

New to WebGrants - Missouri Department of Public Safety?

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



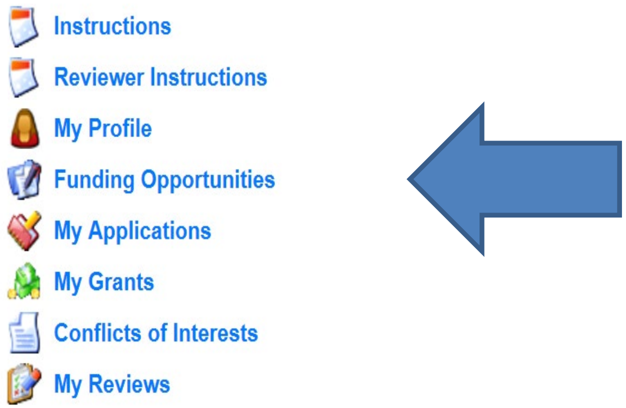
An email has been sent to the email address listed in your user profile with a one-time passcode. Please enter the passcode below.

Password:*

One-Time Passcode:*

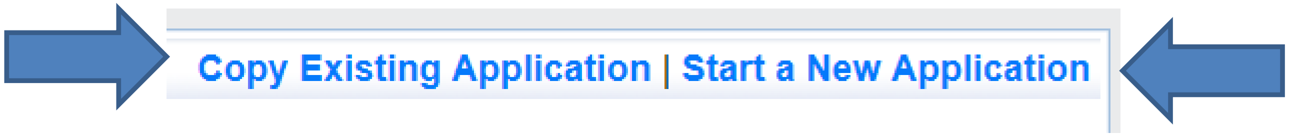
APPLICATION INSTRUCTIONS

- Select "Funding Opportunities" and select the FY 2023 State and Local Cybersecurity Grant Program (SLCGP) funding opportunity



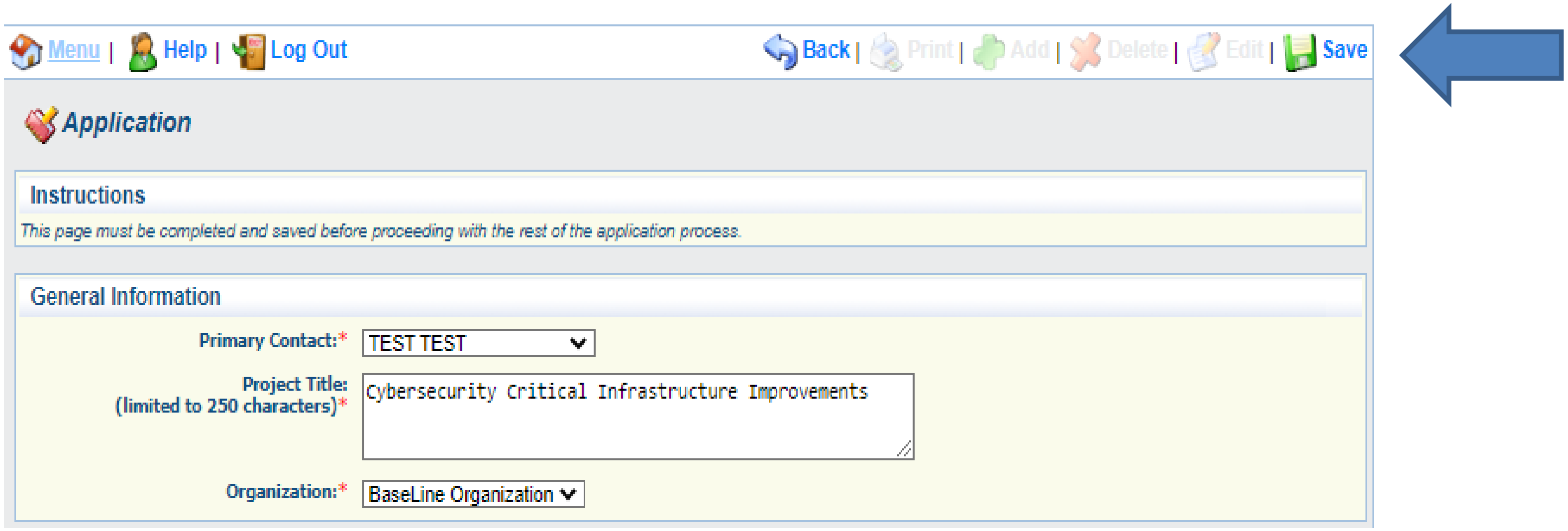
APPLICATION INSTRUCTIONS

- 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"



Application

Instructions

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

General Information

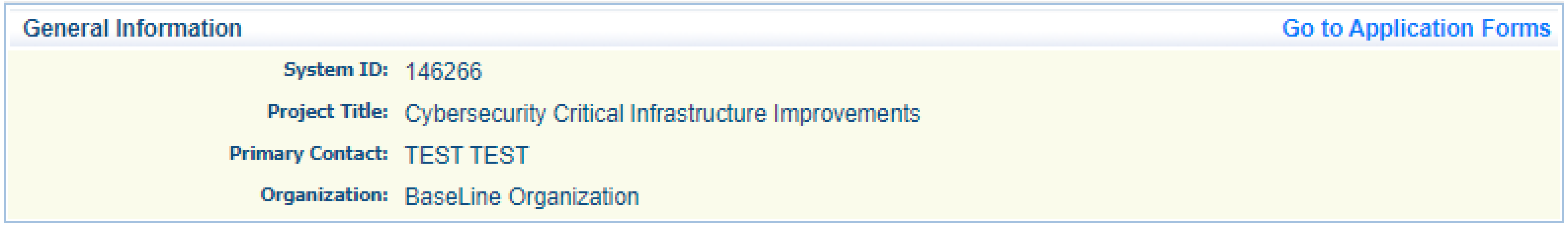
Primary Contact:* TEST TEST

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

Organization:* BaseLine Organization

APPLICATION INSTRUCTIONS

- Select "Go to Application Forms"



General Information

Go to Application Forms

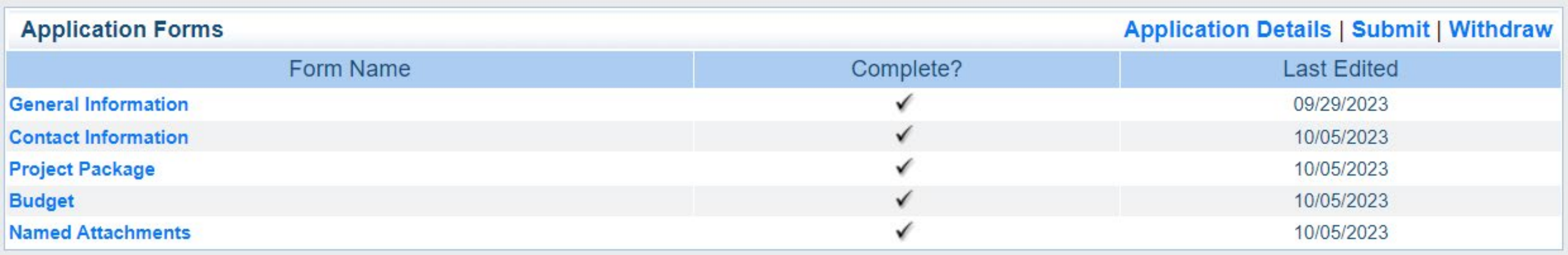
System ID: 146266

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 | Submit | Withdraw

Form Name	Complete?	Last Edited
General Information	✓	09/29/2023
Contact Information	✓	10/05/2023
Project Package	✓	10/05/2023
Budget	✓	10/05/2023
Named Attachments	✓	10/05/2023

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:

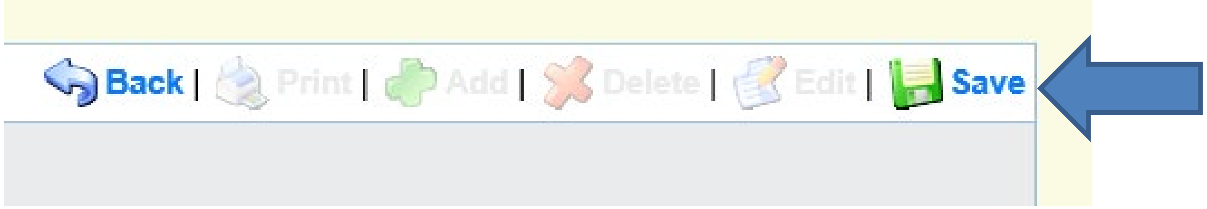
  - If the applicant agency is a city, the Mayor or City Administrator shall be the Authorized Official
  - If the applicant agency is a county, the Presiding County Commissioner or County Executive shall be the Authorized Official (e.g.; the Sheriff is not the Authorized Official)
  - If the applicant 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****

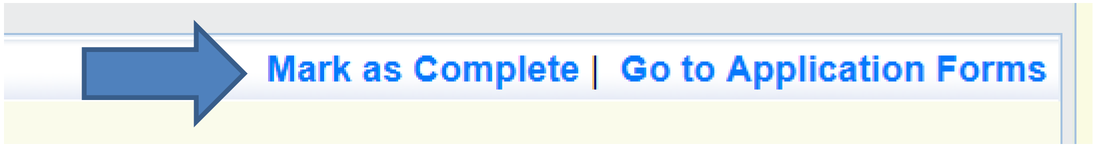
In order for an application to be considered eligible for funding, the agency's correct Authorized Official <u>MUST</u> be designated in the "Contact Information" form and the "Certified Assurances" form

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



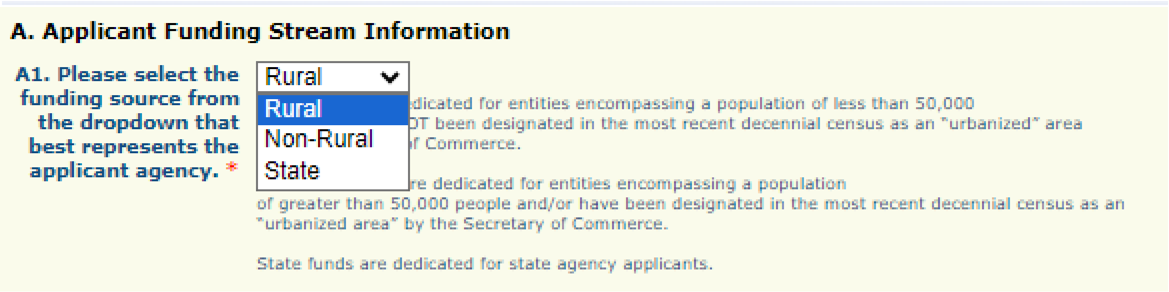
- Then "Mark as Complete"



SLCGP PROJECT PACKAGE

- All of the "SLCGP Project Package" information has been combined into one form with 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



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

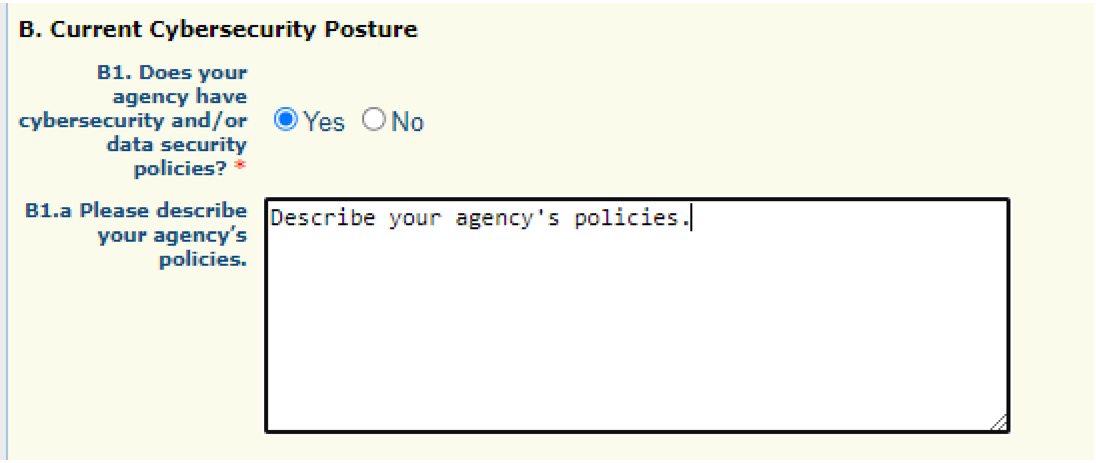
dicated for entities encompassing a population of less than 50,000
OT been designated in the most recent decennial census as an "urbanized" area
f Commerce.

re 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.

- A1. – Select from the dropdown, Rural, Non-Rural, 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



B. Current Cybersecurity Posture

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

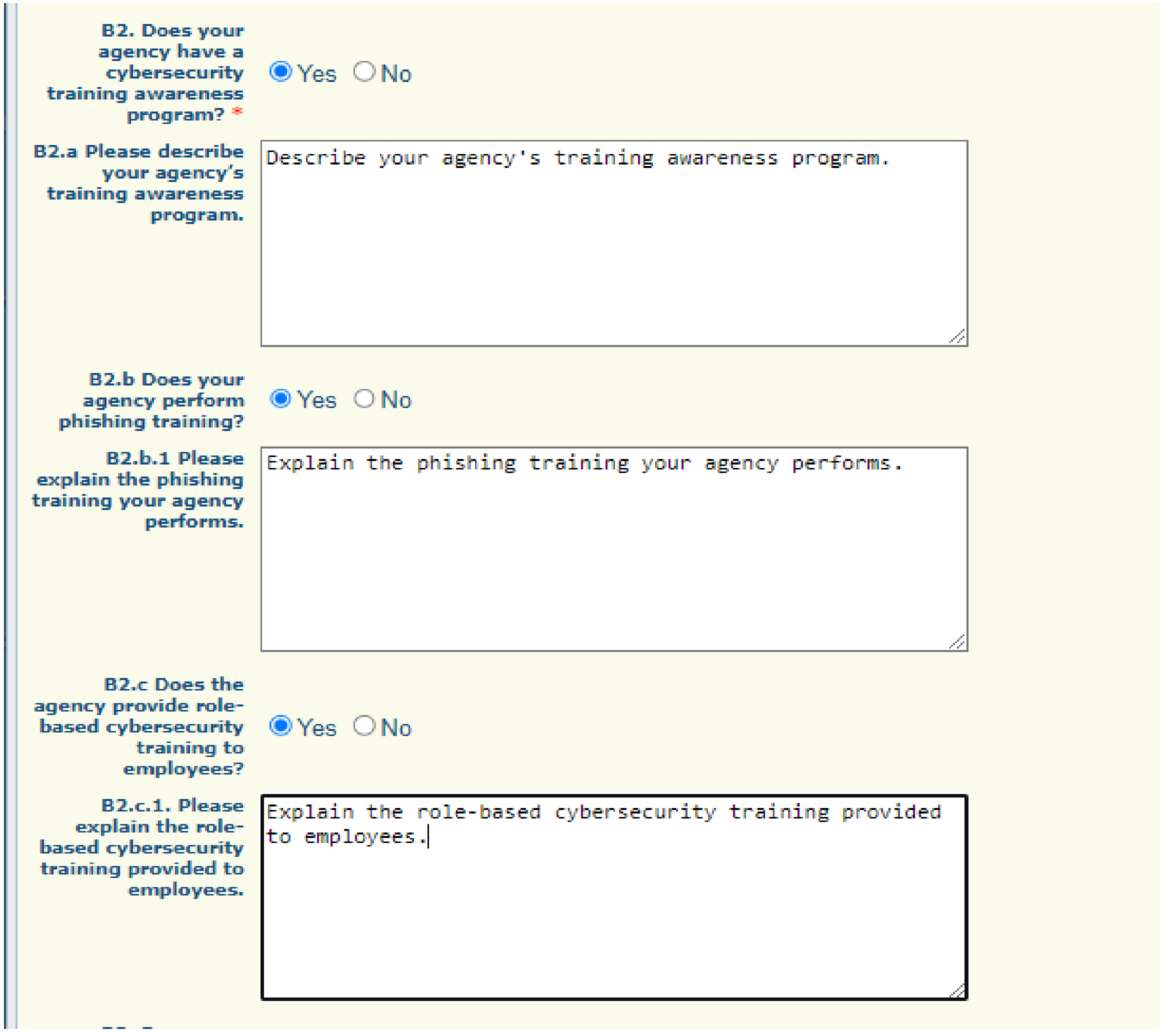
● Yes ○ No

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. Does your agency have a cybersecurity training awareness program? *

● Yes ○ No

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?

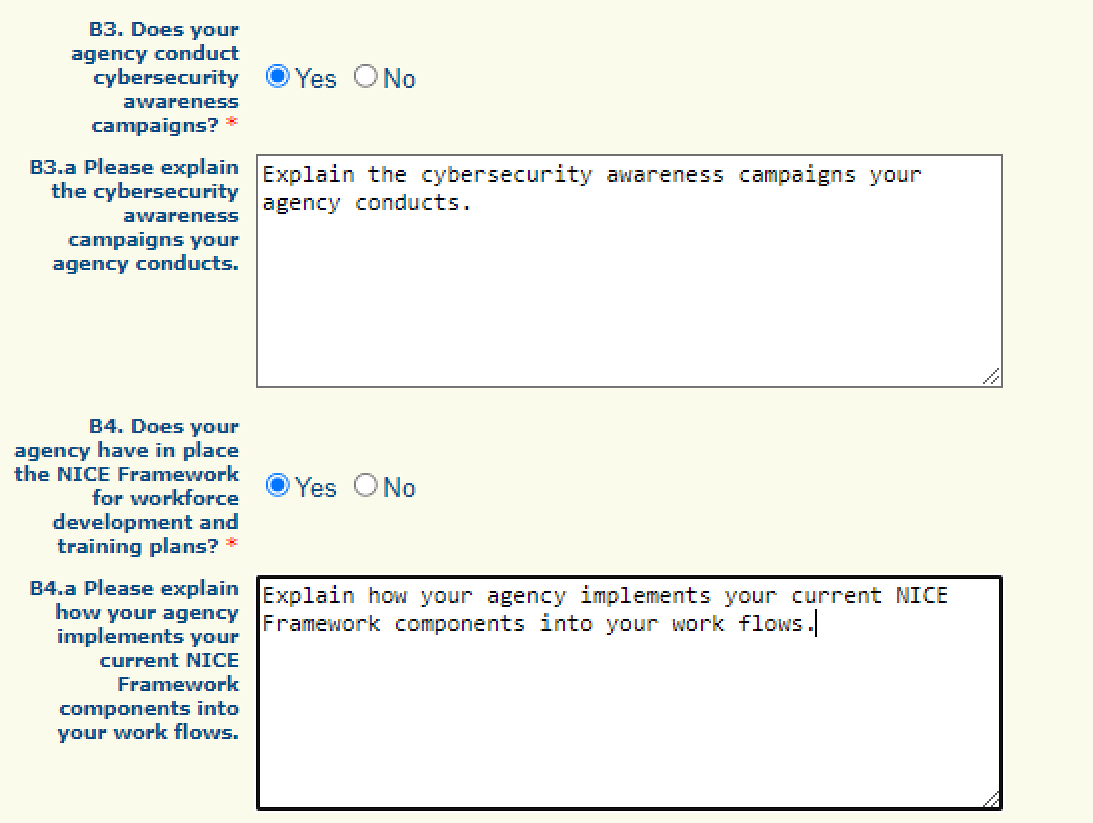
● Yes ○ No

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.

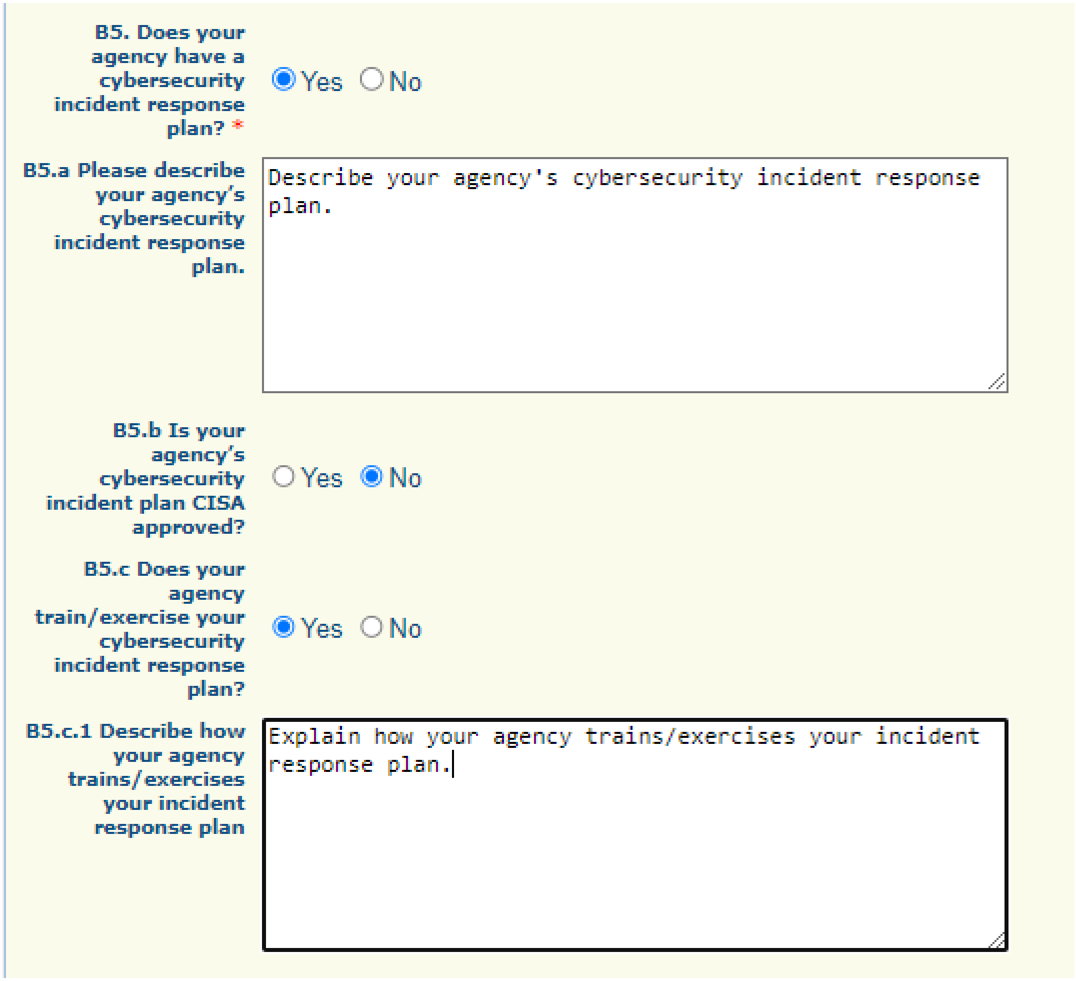
B. CURRENT CYBERSECURITY POSTURE



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

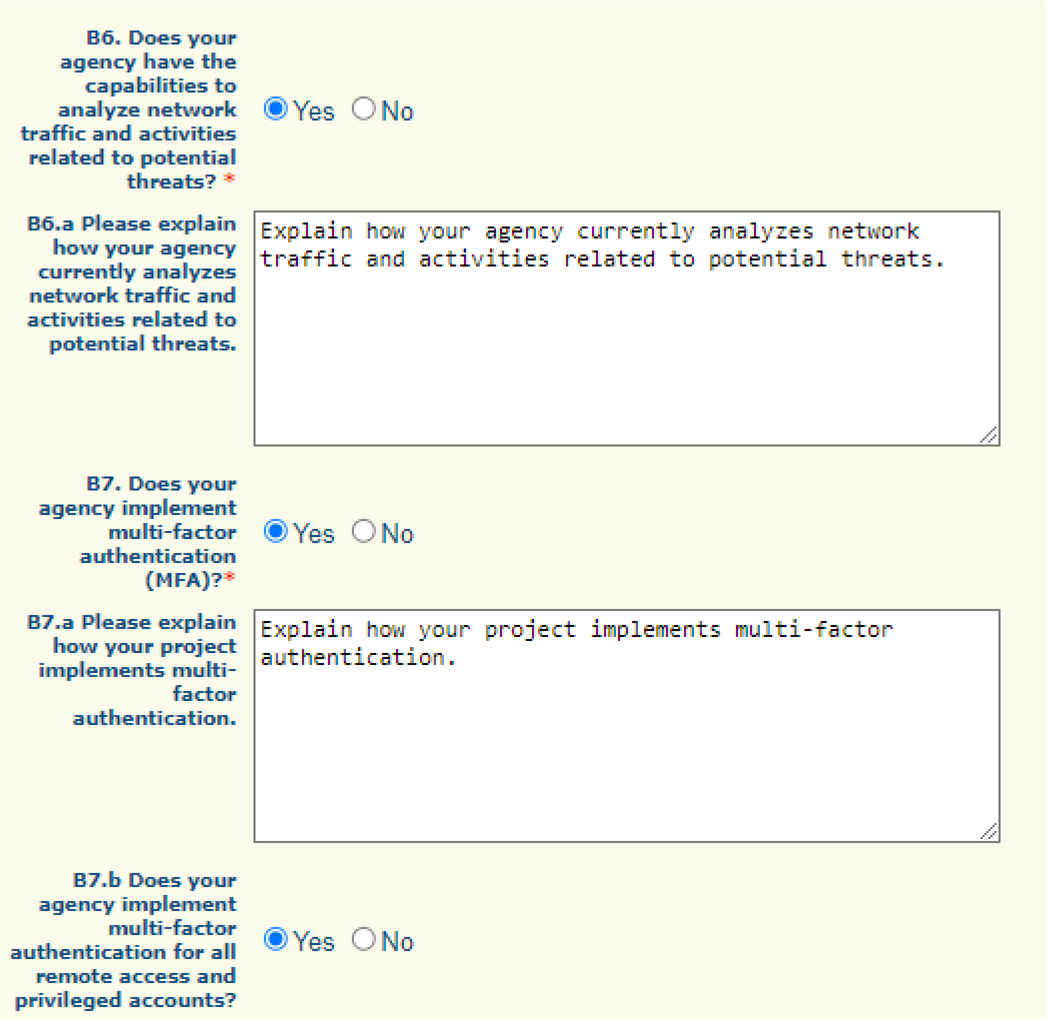
B5.c Does your agency train/exercise your cybersecurity incident response plan? ● Yes ○ No

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

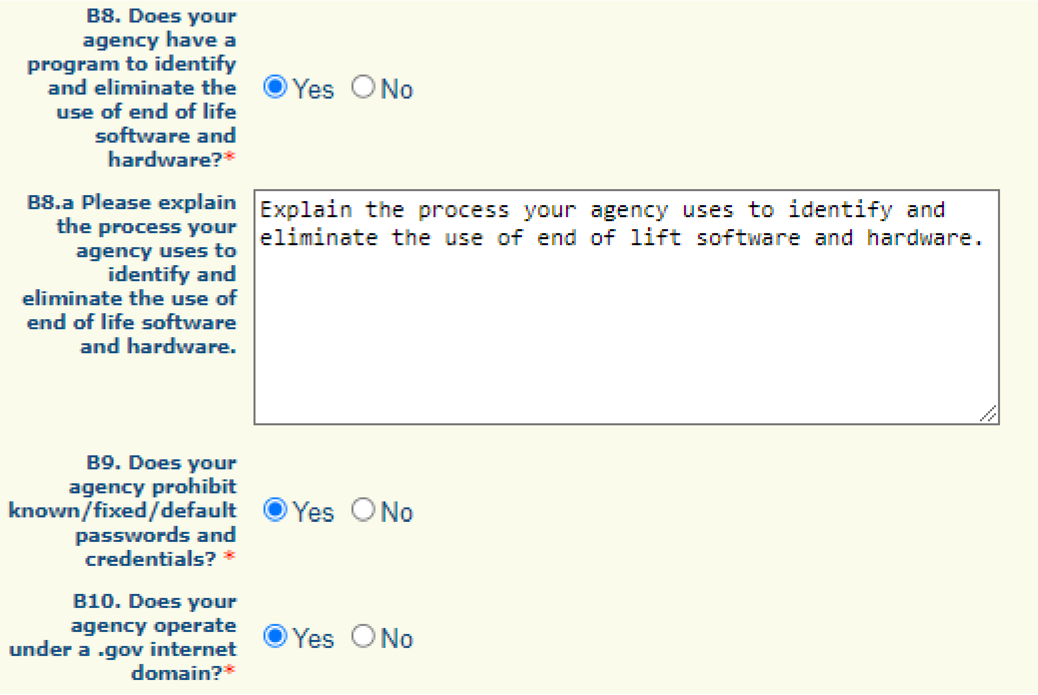
B7.a Please explain how your project implements multi-factor authentication.

```
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.

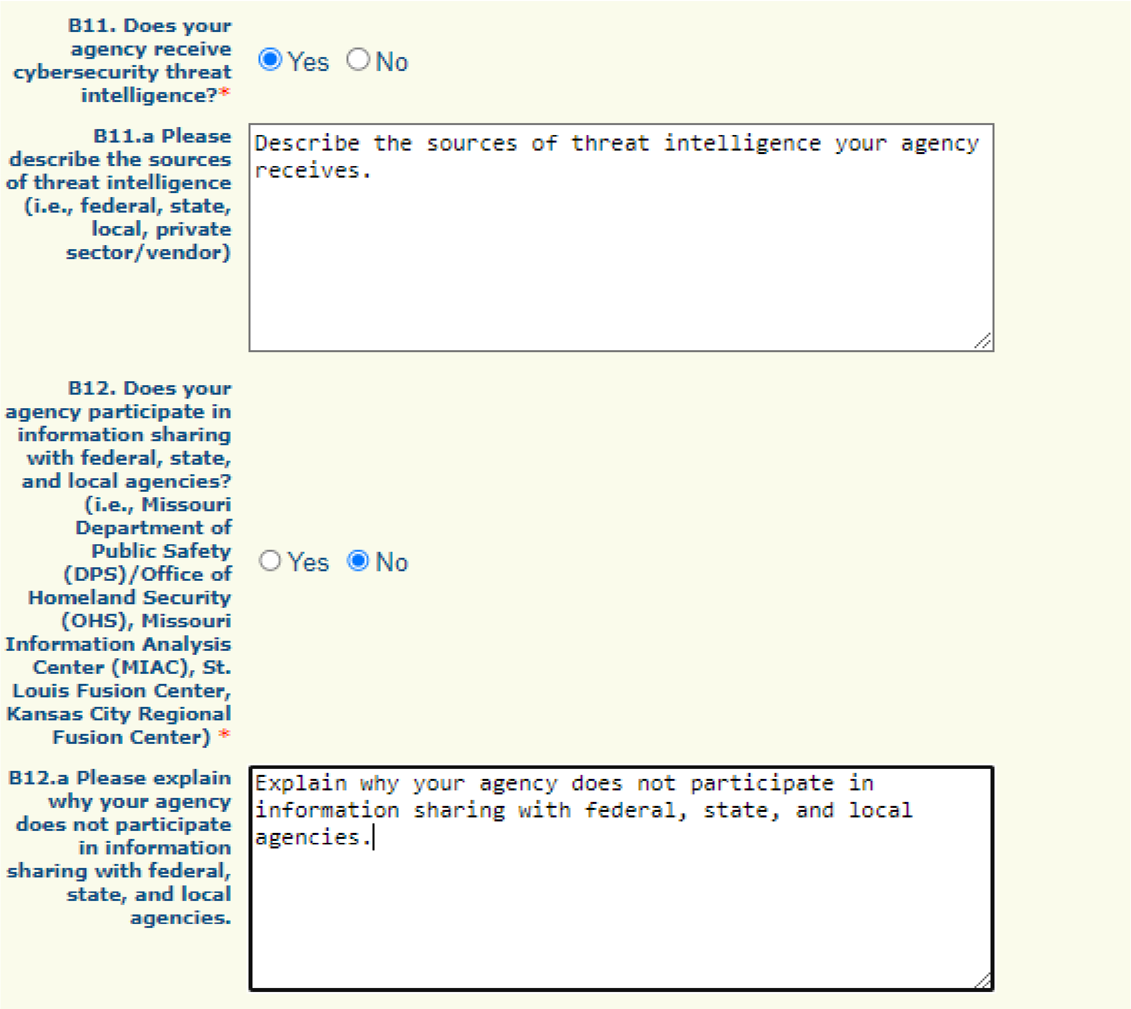
```
Explain the process your agency uses to identify and
eliminate the use of end of lift software and hardware.
```

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) *

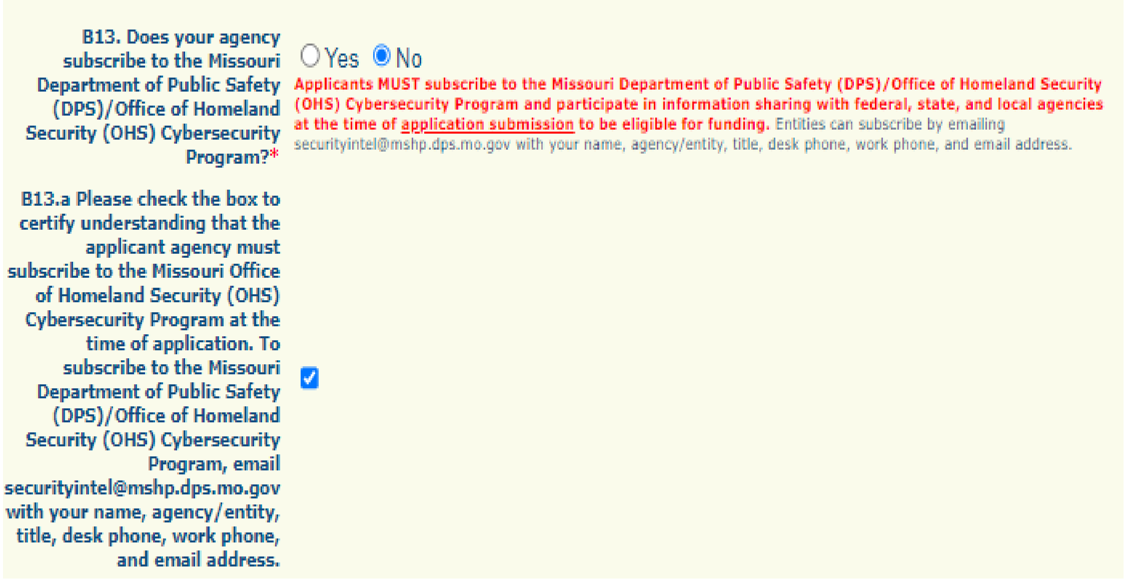
○ Yes ● No

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?*

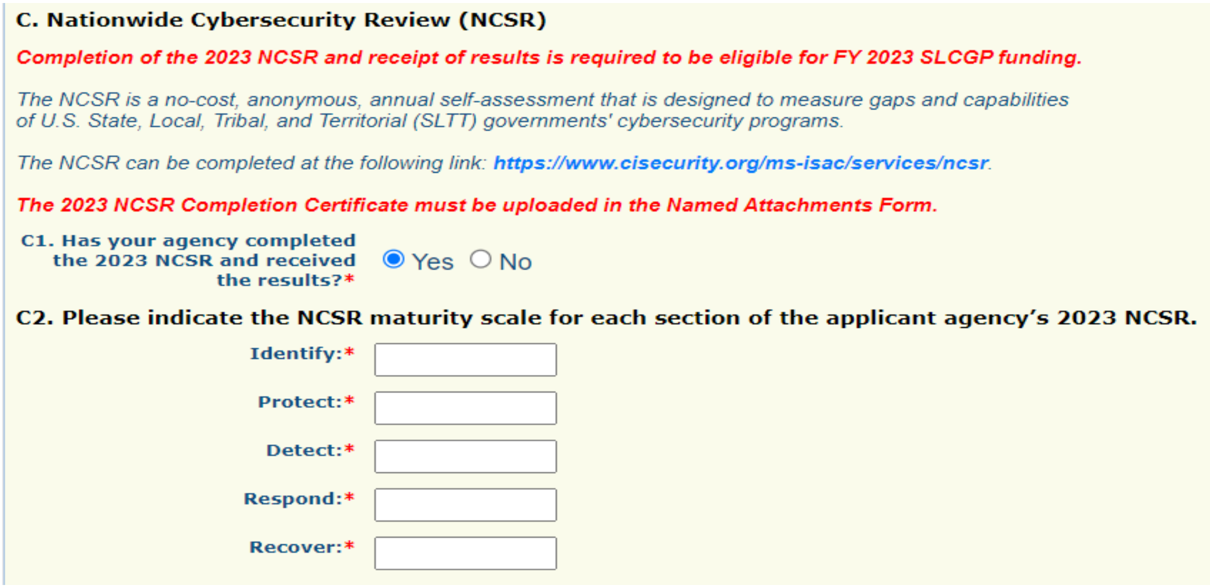
○ Yes ● No

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)



C. Nationwide Cybersecurity Review (NCSR)

Completion of the 2023 NCSR and receipt of results is required to be eligible for FY 2023 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 2023 NCSR Completion Certificate must be uploaded in the Named Attachments Form.

C1. Has your agency completed the 2023 NCSR and received the results?* ● Yes ○ No

C2. Please indicate the NCSR maturity scale for each section of the applicant agency's 2023 NCSR.

Identify:*

Protect:*

Detect:*

Respond:*

Recover:*

- 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

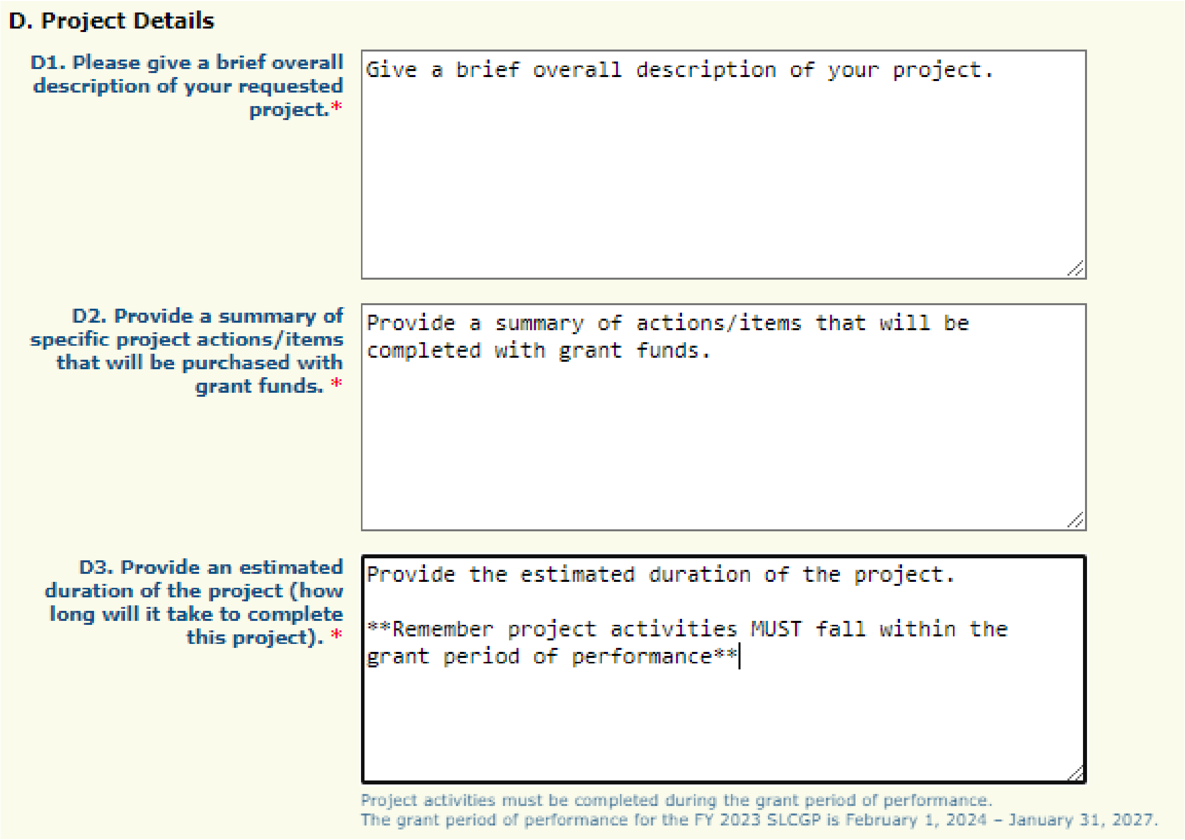
- C1. Has your agency completed the 2023 NCSR and received the results?

  ** Completion of the 2023 NCSR and receipt of results is required to be eligible for FY 2023 SLCGP funding. **

  ****The 2023 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 2023 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 grant funds.

D3. Provide an estimated duration of the project (how long will it take to complete this project). *

Provide the estimated duration of the project.

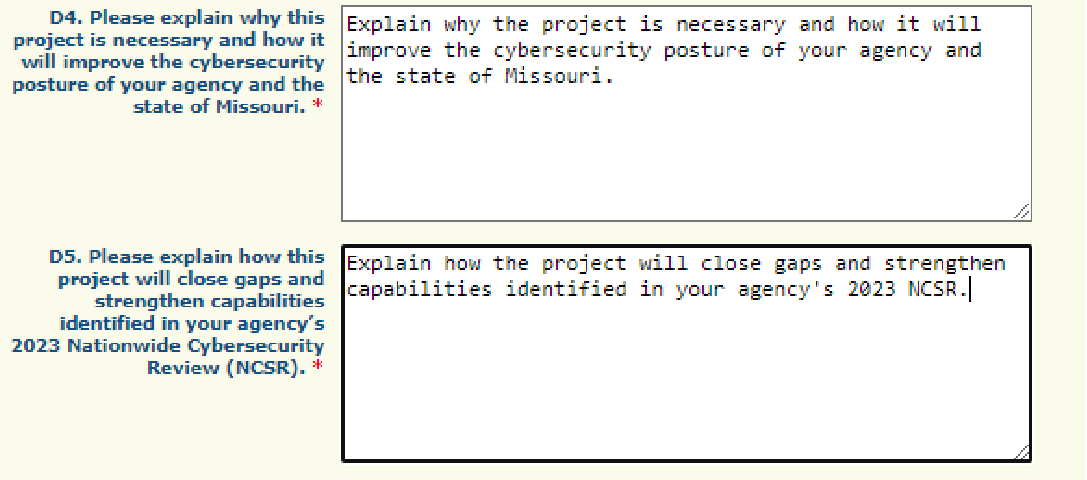
Remember project activities MUST fall within the grant period of performance

Project activities must be completed during the grant period of performance.
The grant period of performance for the FY 2023 SLCGP is February 1, 2024 – January 31, 2027.

- 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.
- D3. 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 2023 SLCGP is **February 1, 2024 – January 31, 2027** **

D. PROJECT DETAILS



D4. Please explain why this project is necessary and how it will improve the cybersecurity posture of your agency and the state of Missouri. *

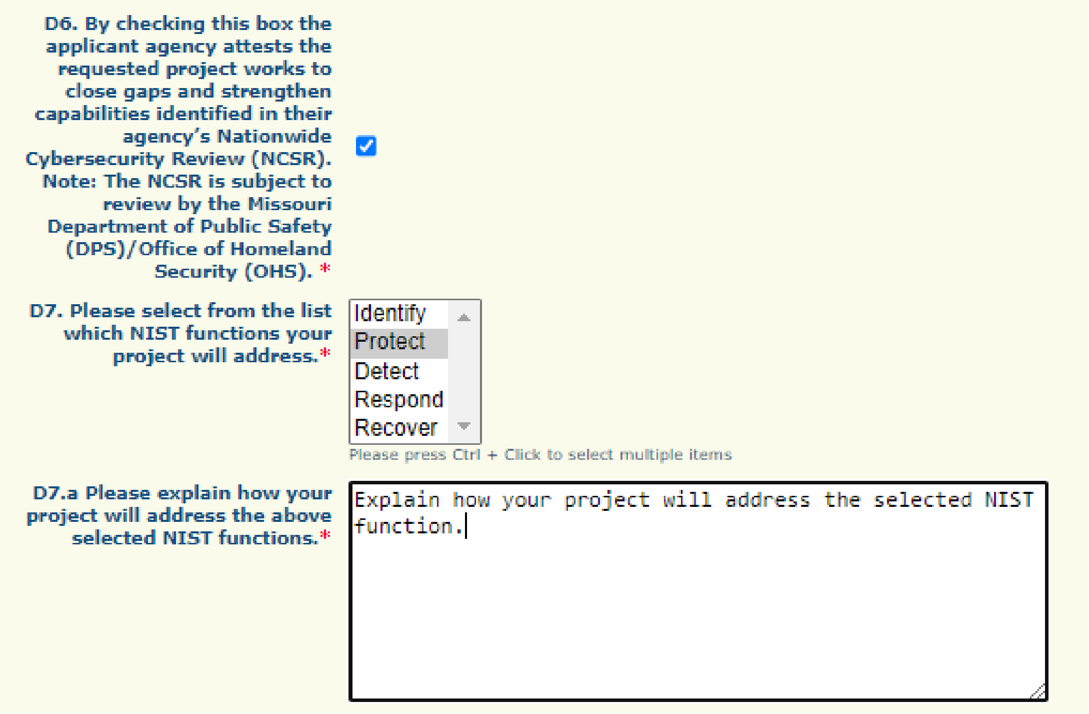
Explain why the project is necessary and how it will improve the cybersecurity posture of your agency and the state of Missouri.

D5. Please explain how this project will close gaps and strengthen capabilities identified in your agency's 2023 Nationwide Cybersecurity Review (NCSR). *

Explain how the project will close gaps and strengthen capabilities identified in your agency's 2023 NCSR.

- D4. Please explain why this project is necessary and how it will improve the cybersecurity posture of your agency and the state of Missouri.
- D5. Please explain how this project will close gaps and strengthen capabilities identified in your agency's 2023 Nationwide Cybersecurity Review (NCSR).

D. PROJECT DETAILS



D6. 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). * ☑

D7. Please select from the list which NIST functions your project will address.*

- Identify
- Protect
- Detect
- Respond
- Recover

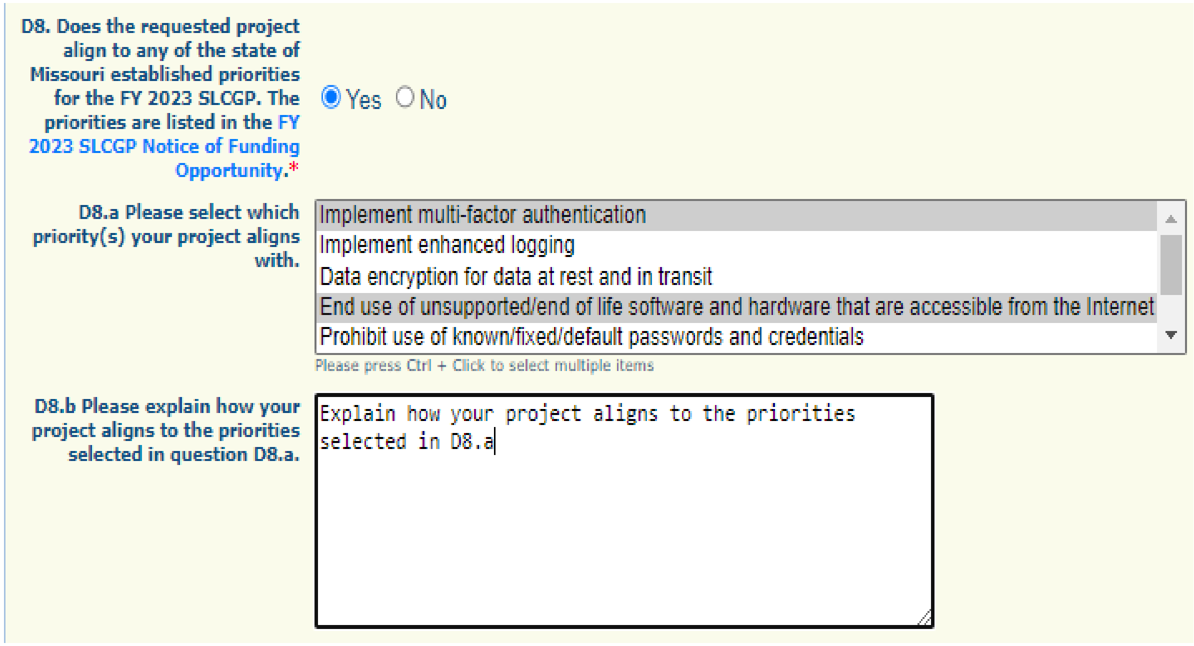
Please press Ctrl + Click to select multiple items

D7.a Please explain how your project will address the above selected NIST functions.*

Explain how your project will address the selected NIST function.

- D6. 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.7 Please select from the list which NIST functions your project will address.
  - Press Ctrl + Click to select multiple items.
- D.7.a Please explain how your project will address the above selected NIST functions

D. PROJECT DETAILS



D8. Does the requested project align to any of the state of Missouri established priorities for the FY 2023 SLCGP. The priorities are listed in the FY 2023 SLCGP Notice of Funding Opportunity.* ● Yes ○ No

D8.a 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

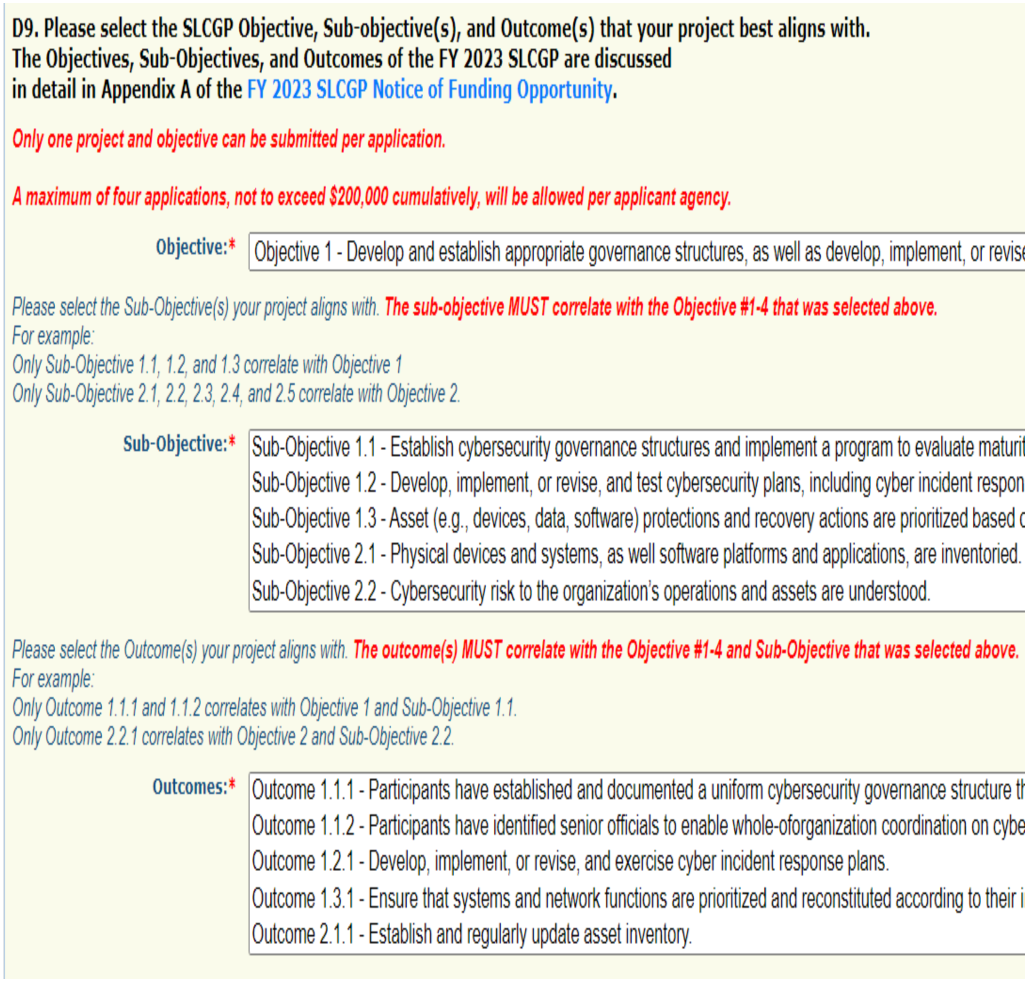
Please press Ctrl + Click to select multiple items

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

Explain how your project aligns to the priorities selected in D8.a

- D8. Does the requested project align to any of the state of Missouri established priorities for the FY 2023 SLCGP. The priorities are listed in the [FY 2023 Notice of Funding Opportunity]().
  - If yes, D8.a Please select which priority(s) your project aligns with. Dropdown multi-select list from NOFO.
    - Press Ctrl + Click to select multiple items.
  - If yes, D8.b Please explain how your project aligns to the priorities selected in question D8.a

D. PROJECT DETAILS



D9. 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 2023 SLCGP are discussed in detail in Appendix A of the FY 2023 SLCGP Notice of Funding Opportunity.

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

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 maturi
Sub-Objective 1.2 - Develop, implement, or revise, and test cybersecurity plans, including cyber incident respon
Sub-Objective 1.3 - Asset (e.g., devices, data, software) protections and recovery actions are prioritized based c
Sub-Objective 2.1 - Physical devices and systems, as well software platforms and applications, are inventoried.
Sub-Objective 2.2 - Cybersecurity risk to the organization's operations and assets are understood.

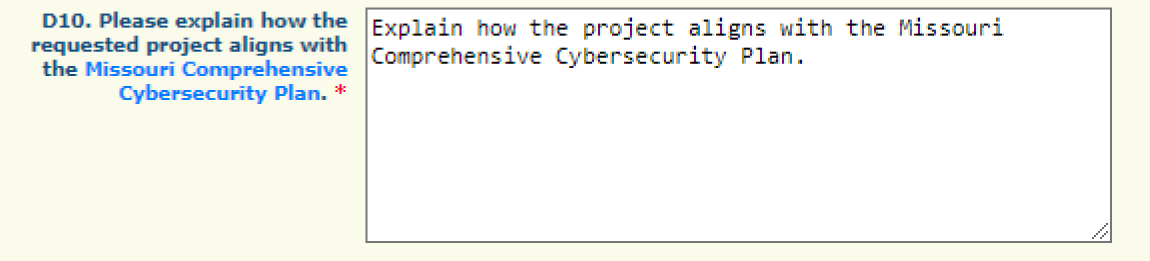
Please select the Outcome(s) your project aligns with. ***The outcome(s) MUST correlate with the Objective #1-4 and Sub-Objective that was selected above.***
For example:
Only Outcome 1.1.1 and 1.1.2 correlates with Objective 1 and Sub-Objective 1.1.
Only Outcome 2.2.1 correlates with Objective 2 and Sub-Objective 2.2.

Outcomes:*
Outcome 1.1.1 - Participants have established and documented a uniform cybersecurity governance structure tl
Outcome 1.1.2 - Participants have identified senior officials to enable whole-oforganization coordination on cybe
Outcome 1.2.1 - Develop, implement, or revise, and exercise cyber incident response plans.
Outcome 1.3.1 - Ensure that systems and network functions are prioritized and reconstituted according to their i
Outcome 2.1.1 - Establish and regularly update asset inventory.

- D9. Please select the SLCGP Objective, Sub-Objective, and Outcome that your project best aligns with. The Objectives, Sub-Objectives, and Outcomes of the FY 2023 SLCGP are discussed in detail in Appendix A of the FY 2023 SLCGP NOFO.
- ***The sub-objective MUST correlate with the Objective #1-4 that was selected above.***
- ***The outcome(s) MUST correlate with the Objective #1-4 and Sub-Objective that was selected above.***

**** 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

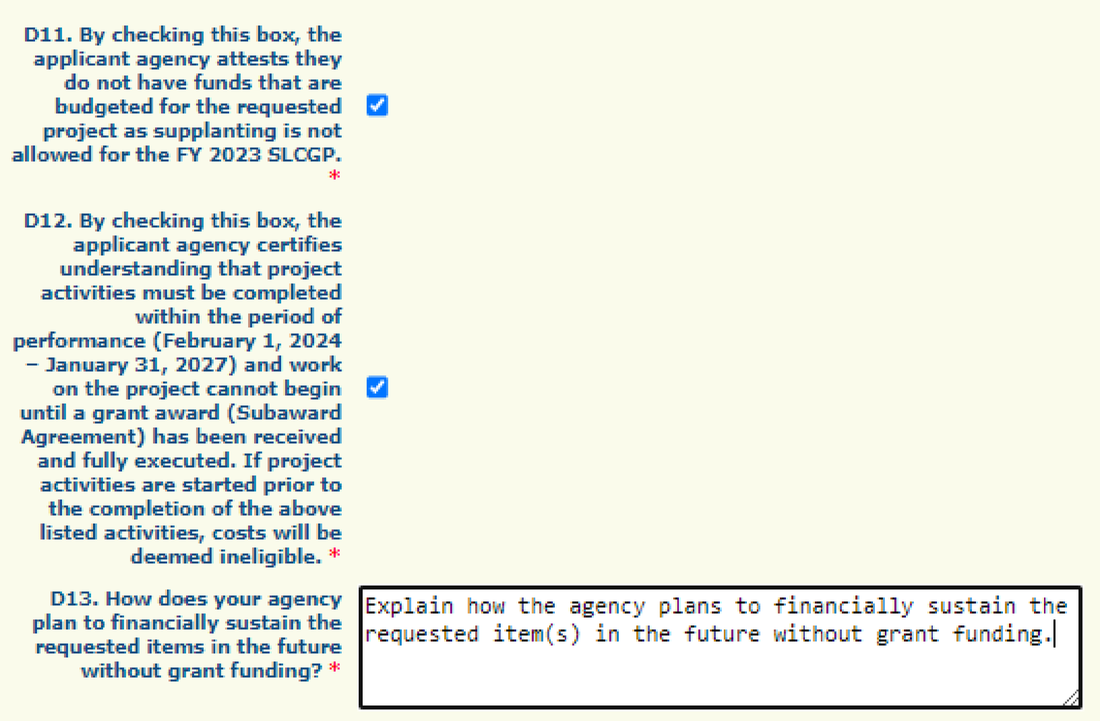


D10. Please explain how the requested project aligns with the Missouri Comprehensive Cybersecurity Plan. *

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

- D10. Please explain how the requested project aligns with the Missouri Comprehensive Cybersecurity Plan (CCP). The Missouri CCP can be located within the WebGrants application.

D. PROJECT DETAILS



D11. 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 2023 SLCGP. * ☑

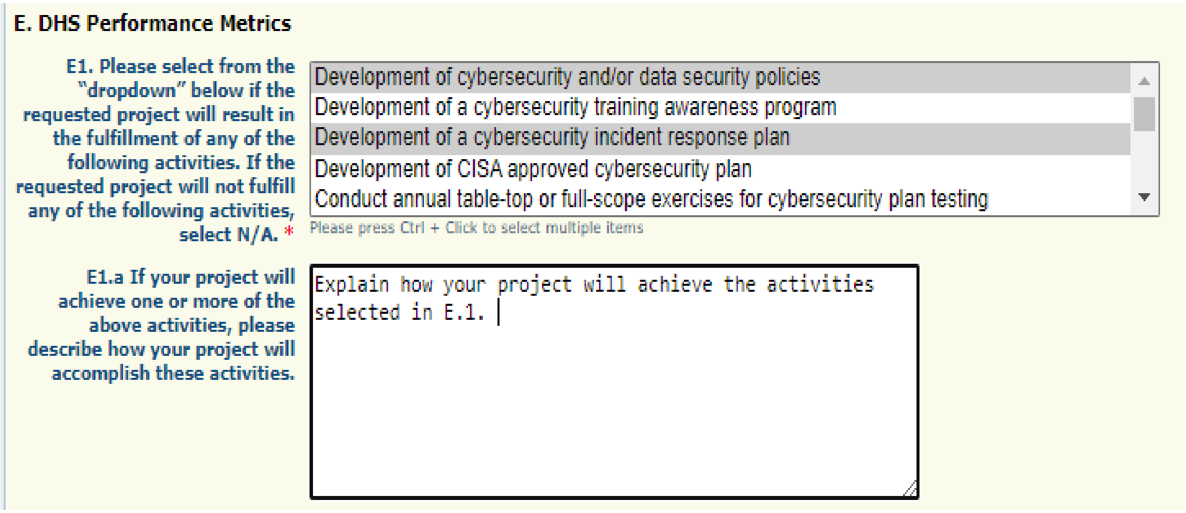
D12. By checking this box, the applicant agency certifies understanding that project activities must be completed within the period of performance (February 1, 2024 – January 31, 2027) and work on the project cannot begin until a grant award (Subaward Agreement) has been received and fully executed. If project activities are started prior to the completion of the above listed activities, costs will be deemed ineligible. * ☑

D13. 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.
```

- D11. 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 2023 SLCGP.
- D12. By checking this box, the applicant agency certifies understanding that project activities must be completed within the period of performance (**February 1, 2024 – January 31, 2027**) 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**.
- D13. 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" 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. *

- Development of cybersecurity and/or data security policies
- 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

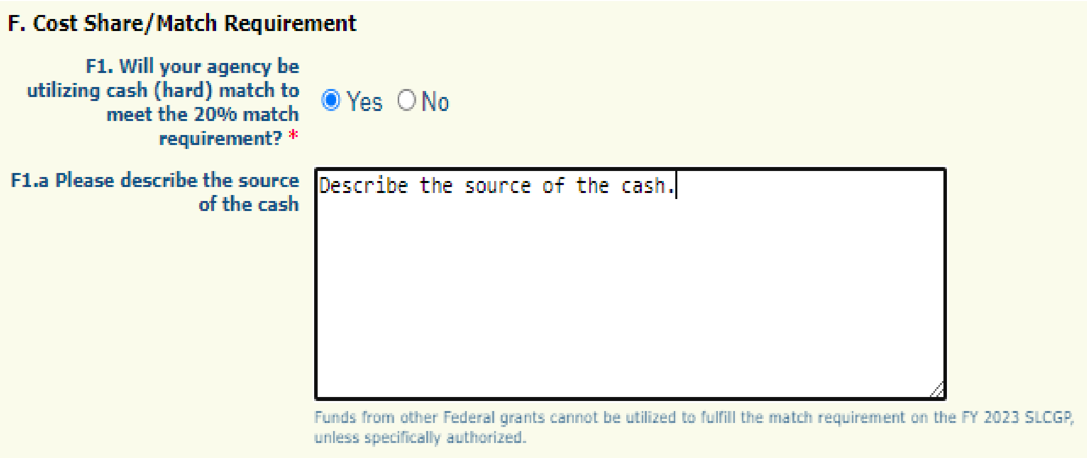
Please press Ctrl + Click to select multiple items

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

Explain how your project will achieve the activities selected in E.1.

- 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.
  - Press Ctrl + Click to select multiple items.
- 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 20% match requirement? * ● Yes ○ No

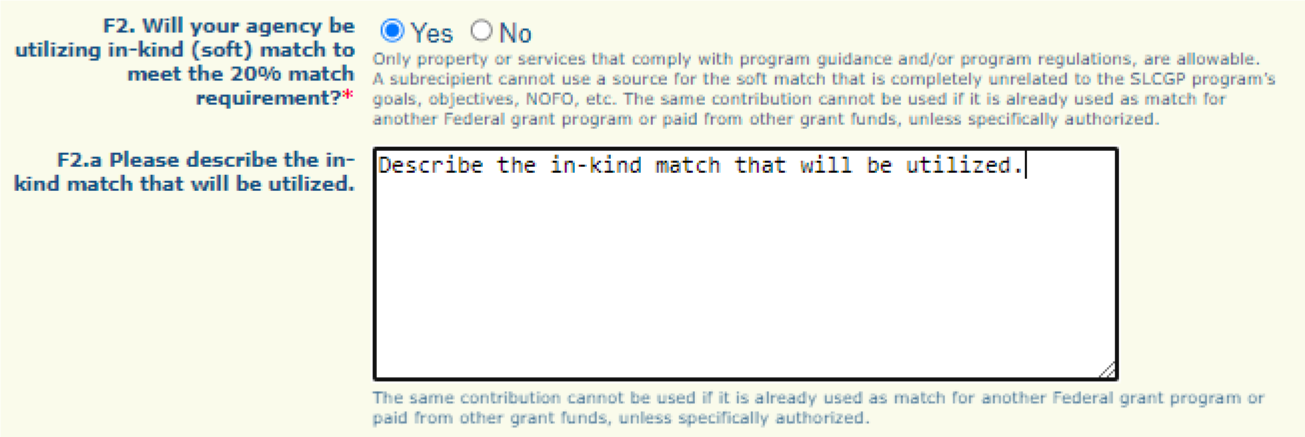
F1.a Please describe the source of the cash: Describe the source of the cash.

Funds from other Federal grants cannot be utilized to fulfill the match requirement on the FY 2023 SLCGP, unless specifically authorized.

- F.1 Will your agency be utilizing cash (hard) match to meet the 20% match requirement?
- If yes, F1.a Please describe the source of the cash

  ** Funds from other Federal grants cannot be utilized to fulfill the match requirement on the FY 2023 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 20% 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.

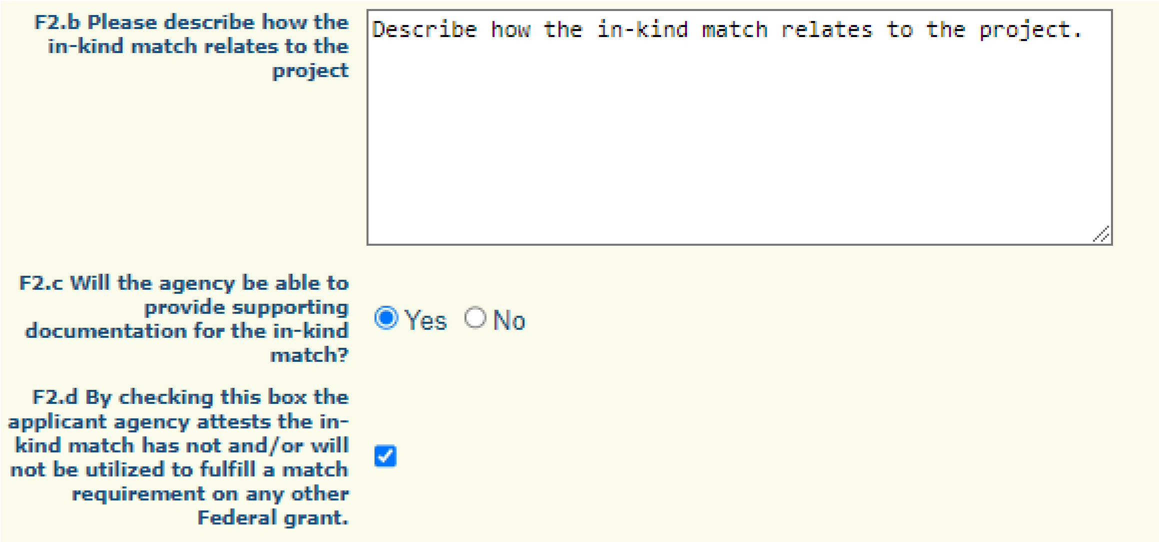
F2.a Please describe the in-kind match that will be utilized.

```
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 20% 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.

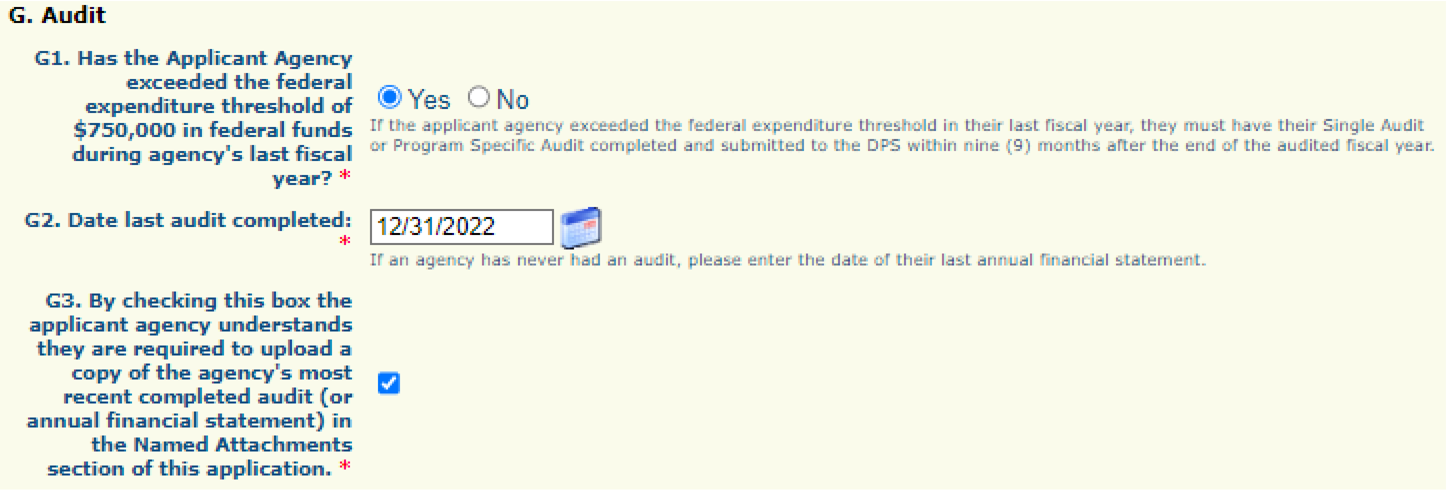
G. AUDIT

- 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 Attachment” form on the application

G. 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)

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 within nine (9) months after the end of the audited fiscal year.

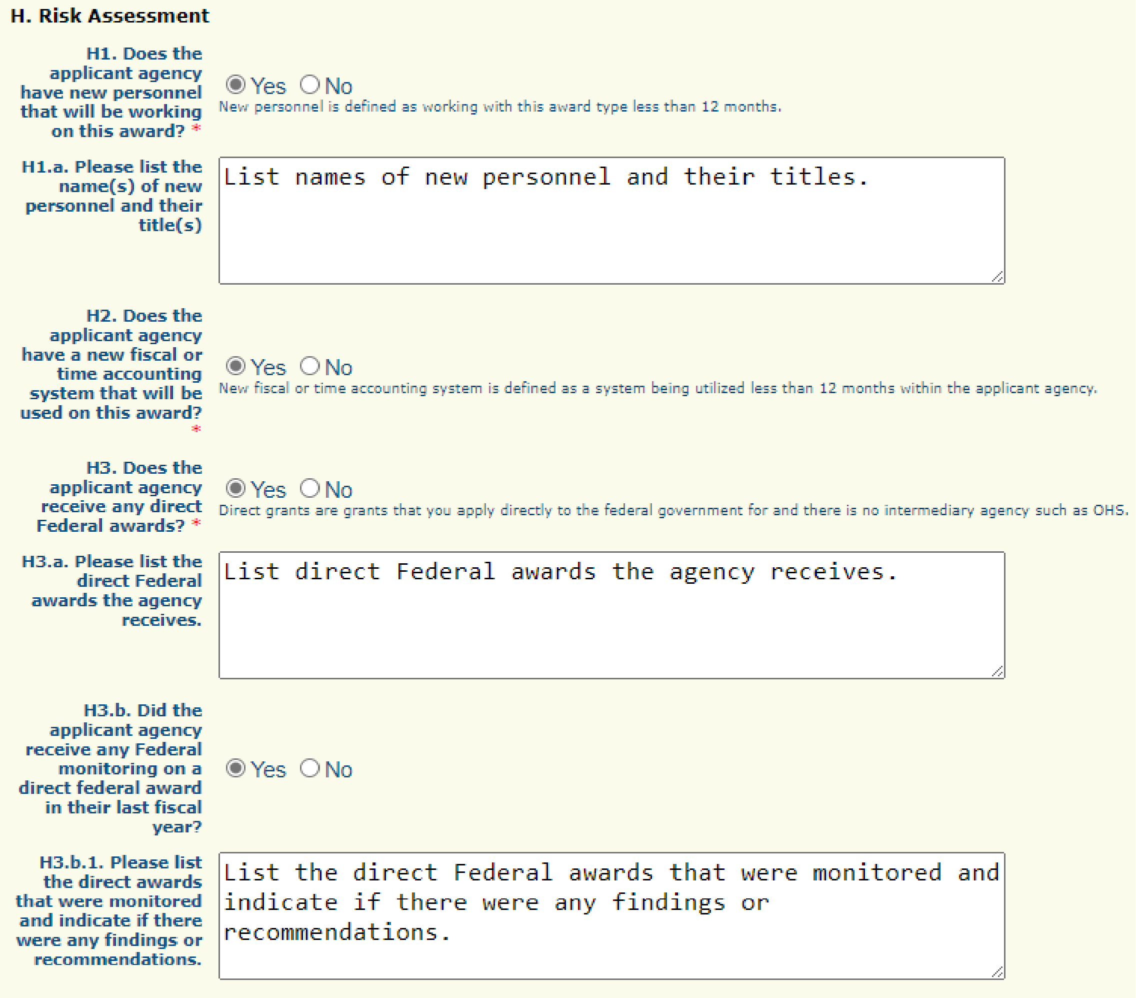
G2. Date last audit completed: * 12/31/2022

If an agency has never had an audit, please enter the date of their 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.

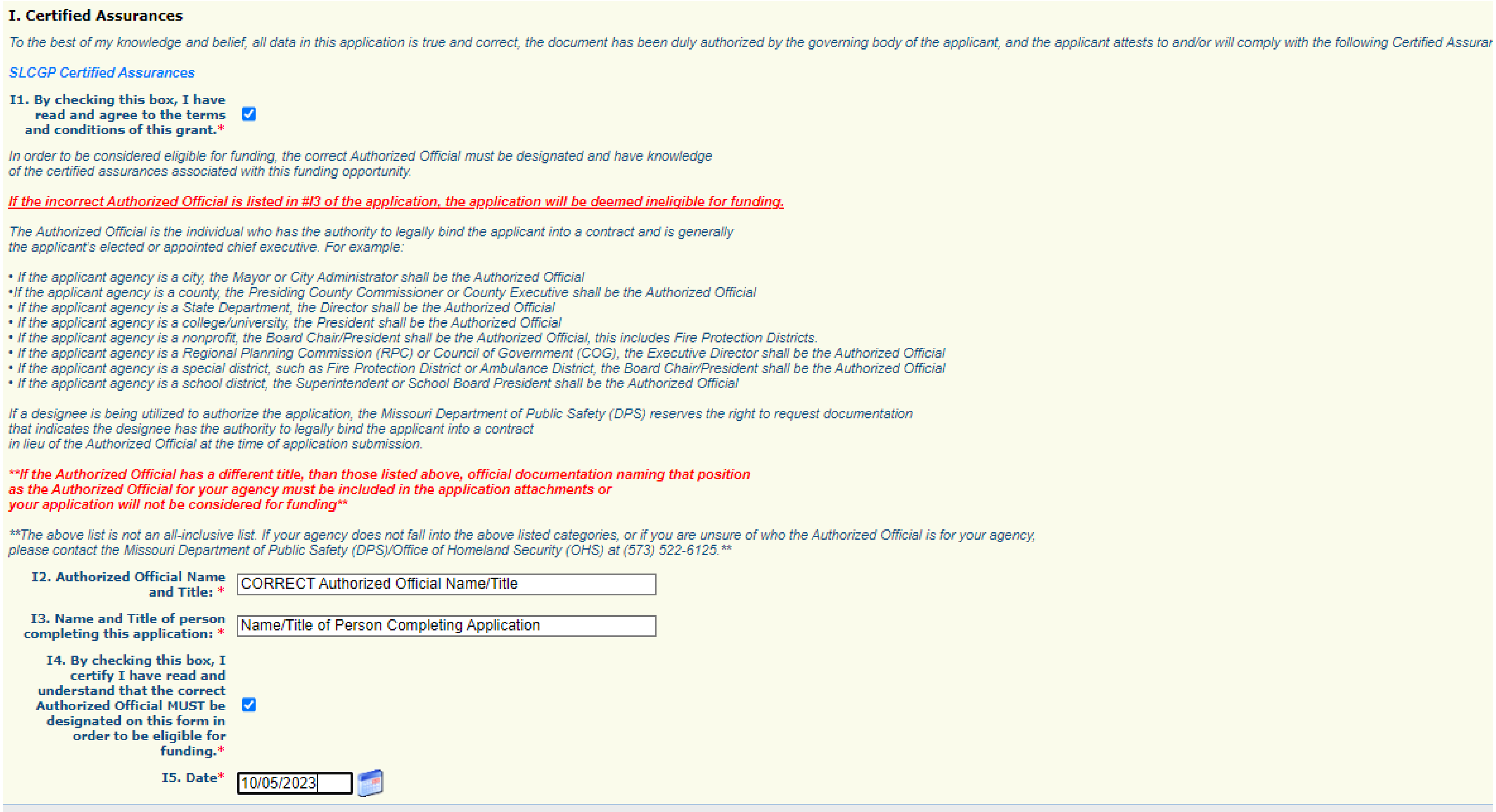
I. CERTIFIED ASSURANCES

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 Assurar

SLCGP Certified Assurances

I1. 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 #I3 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) 522-6125.

I2. Authorized Official Name and Title: *	CORRECT Authorized Official Name/Title
I3. Name and Title of person completing this application: *	Name/Title of Person Completing Application
I4. 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.*	☑
I5. Date*	10/05/2023

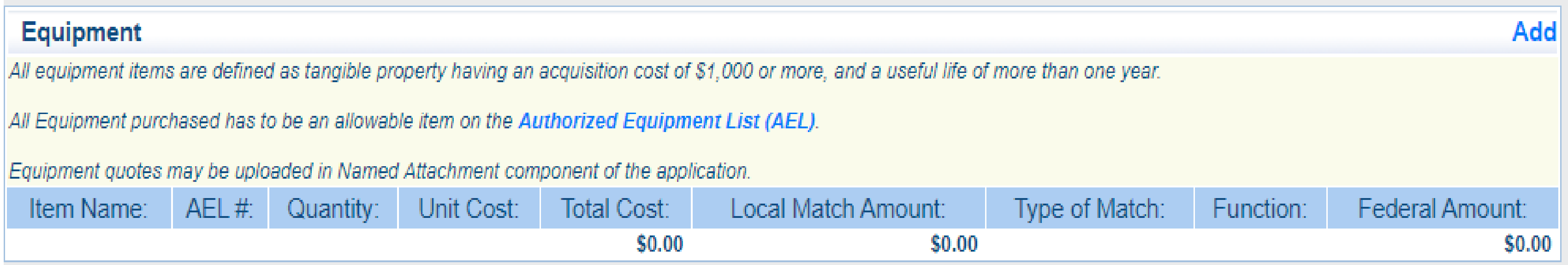
BUDGET

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

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

Budget Sections:

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



Equipment Add

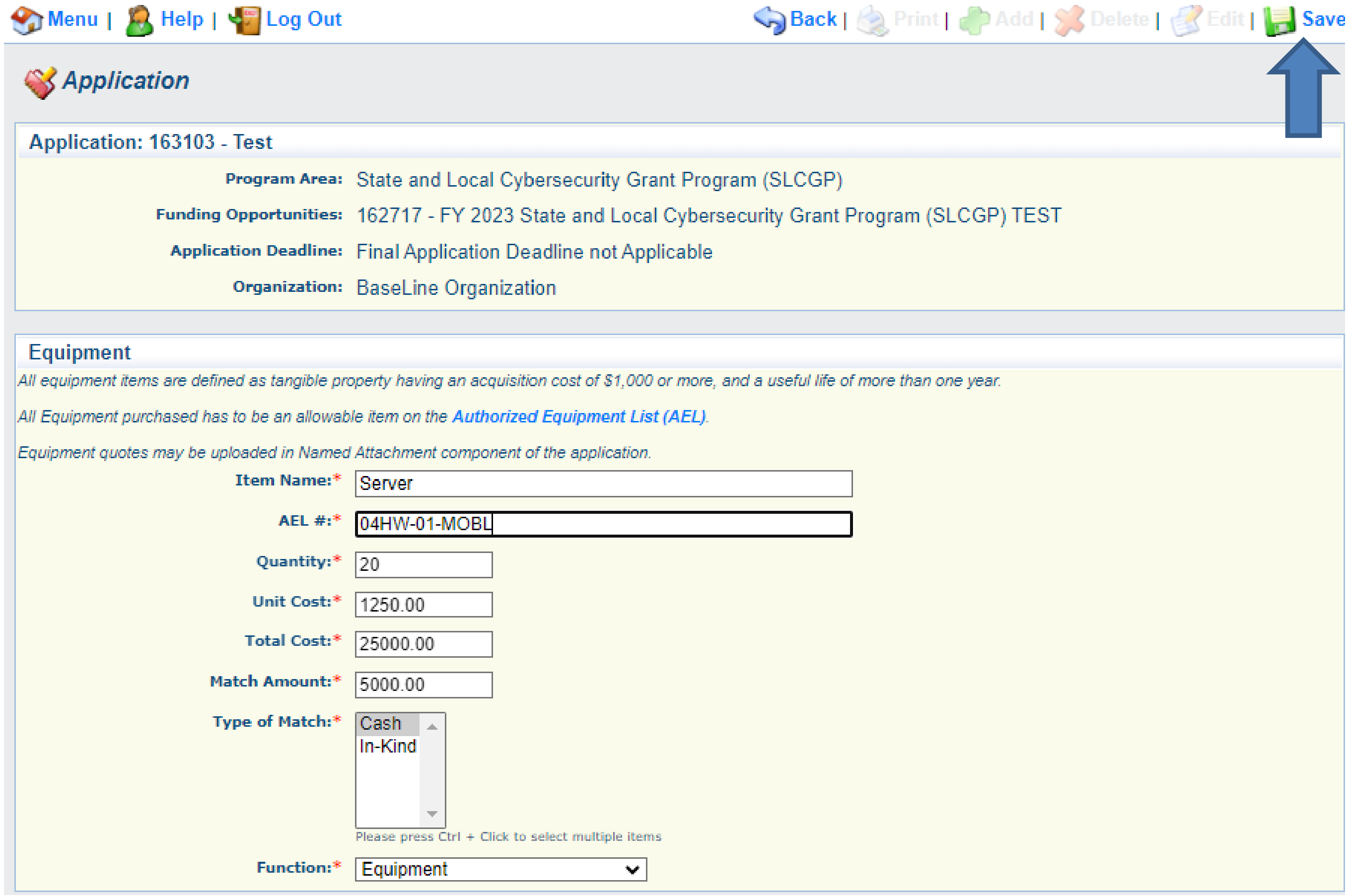
All equipment items are defined as tangible property having an acquisition cost of $1,000 or more, and a useful life of more than one year.

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

BUDGET – CASH MATCH



Application: 163103 - Test

Program Area:	State and Local Cybersecurity Grant Program (SLCGP)
Funding Opportunities:	162717 - FY 2023 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:*	Server
AEL #:*	04HW-01-MOBL
Quantity:*	20
Unit Cost:*	1250.00
Total Cost:*	25000.00
Match Amount:*	5000.00
Type of Match:*	Cash In-Kind Please press Ctrl + Click to select multiple items
Function:*	Equipment

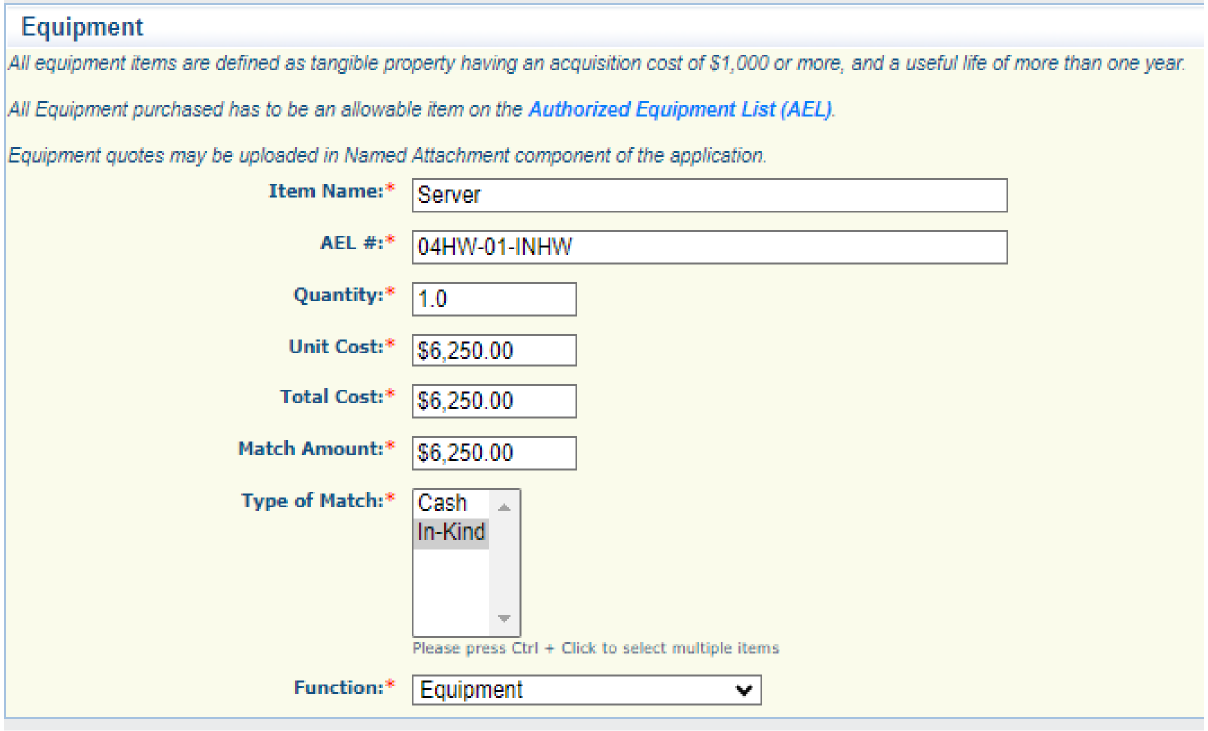
- The Federal amount of funds requested will automatically calculate based on the amount entered for match
- Total Cost = Local Match Amount + Federal Amount Requested.
- 20% match requirement for FY23 SLCGP.
- The screenshot on this slide shows a cash match example.
- NOTE - You will only include the 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



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.

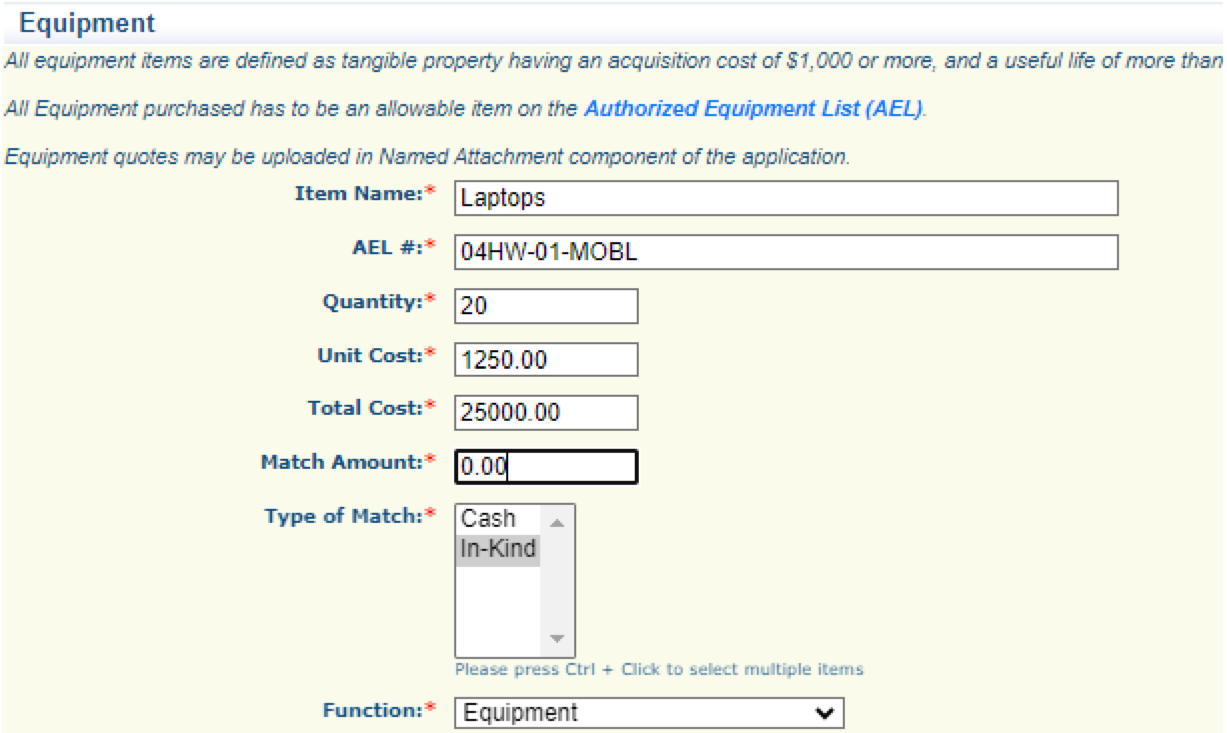
All Equipment purchased has to be an allowable item on the Authorized Equipment List (AEL).

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

Item Name:*	Server
AEL #:*	04HW-01-INHW
Quantity:*	1.0
Unit Cost:*	$6,250.00
Total Cost:*	$6,250.00
Match Amount:*	$6,250.00
Type of Match:*	Cash In-Kind Please press Ctrl + Click to select multiple items
Function:*	Equipment

- 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



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

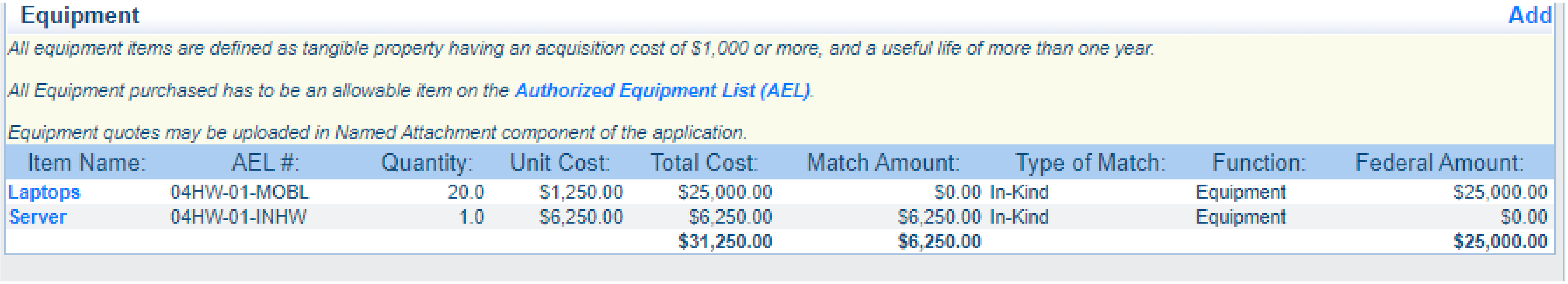
*All Equipment purchased has to be an allowable item on the **Authorized Equipment List (AEL)**.*

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

Item Name:*	Laptops
AEL #:*	04HW-01-MOBL
Quantity:*	20
Unit Cost:*	1250.00
Total Cost:*	25000.00
Match Amount:*	0.00
Type of Match:*	Cash [✓ In-Kind] Please press Ctrl + Click to select multiple items
Function:*	Equipment

- 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



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:	AEL #:	Quantity:	Unit Cost:	Total Cost:	Match Amount:	Type of Match:	Function:	Federal Amount:
Laptops	04HW-01-MOBL	20.0	$1,250.00	$25,000.00	$0.00	In-Kind	Equipment	$25,000.00
Server	04HW-01-INHW	1.0	$6,250.00	$6,250.00	$6,250.00	In-Kind	Equipment	$0.00
				$31,250.00	**$6,250.00**			**$25,000.00**

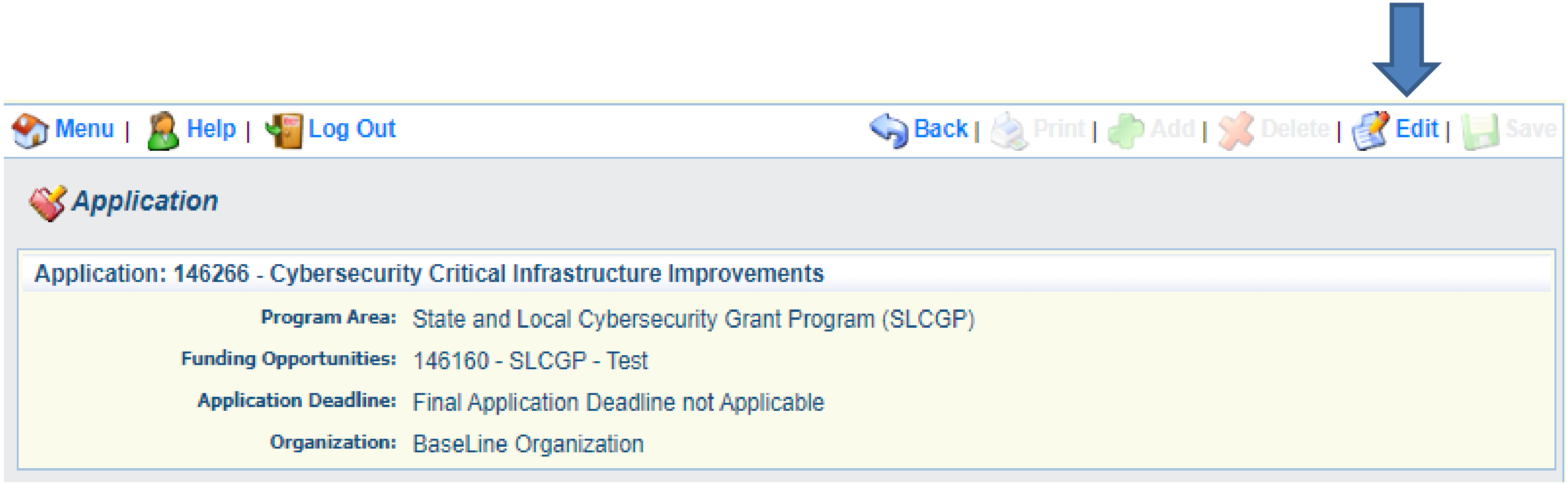
- The screen above shows an example of what the in-kind match (server) and the requested items to purchase with grant funds (laptops) would look like when utilizing in-kind match.

BUDGET

- **Cost Share or Match:** 20% 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 20% match is included in your budget, your application will be deemed <u>INELIGIBLE</u>****

BUDGET

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

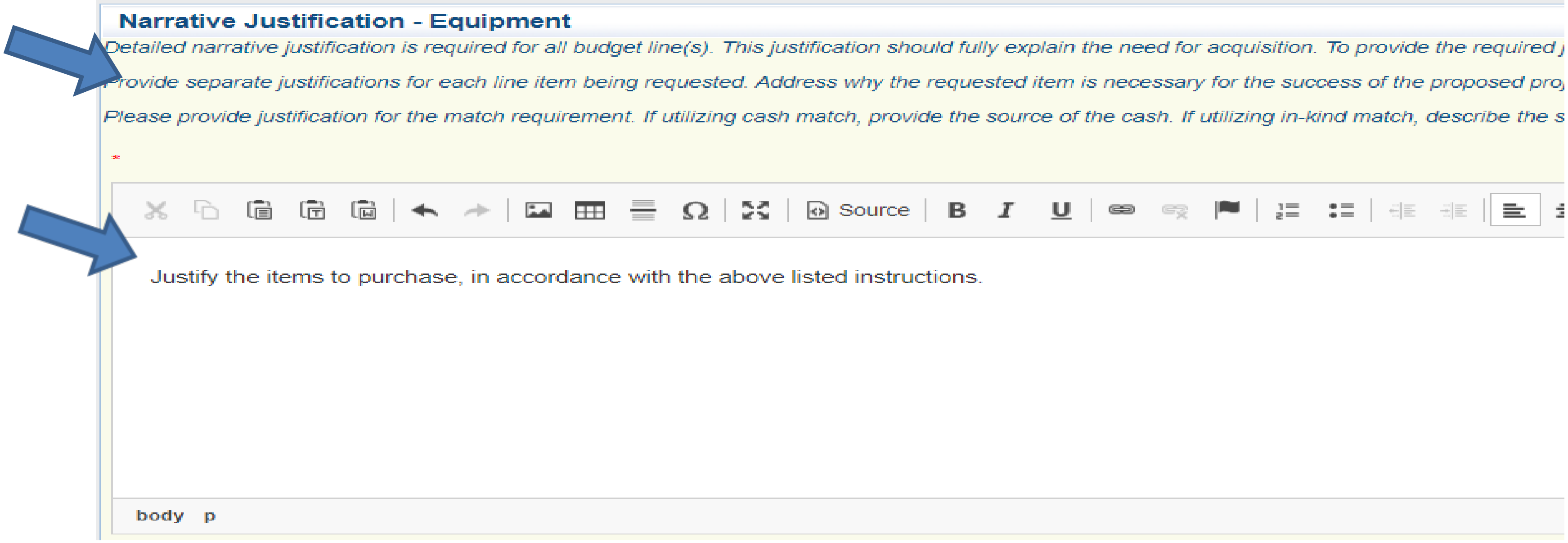


Application: 146266 - Cybersecurity Critical Infrastructure Improvements

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 j

Provide separate justifications for each line item being requested. Address why the requested item is necessary for the success of the proposed proj

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

*

Justify the items to purchase, 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 20% 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 20% 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

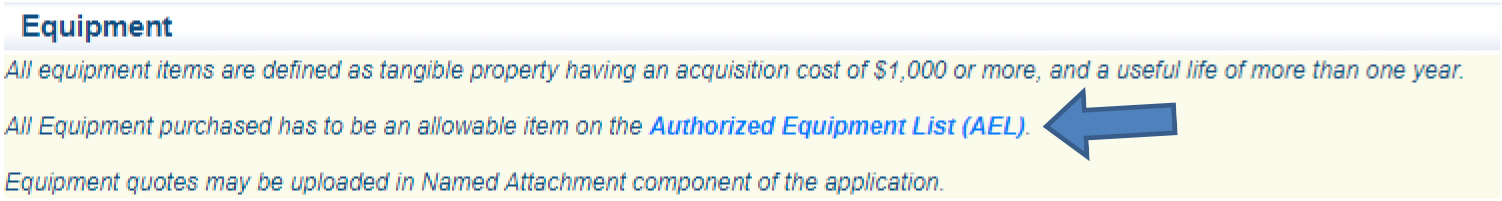
- Travel Costs
  - Meal per diem rates cannot exceed the rates approved by the Missouri Office of Administration
    - https://oa.mo.gov/accounting/state-employees/travel-portal-information/meals-per-diem
  - Mileage rates cannot exceed the state rates approved by the Missouri Office of Administration
    - 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 20% 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 is provided in the instructions



Equipment

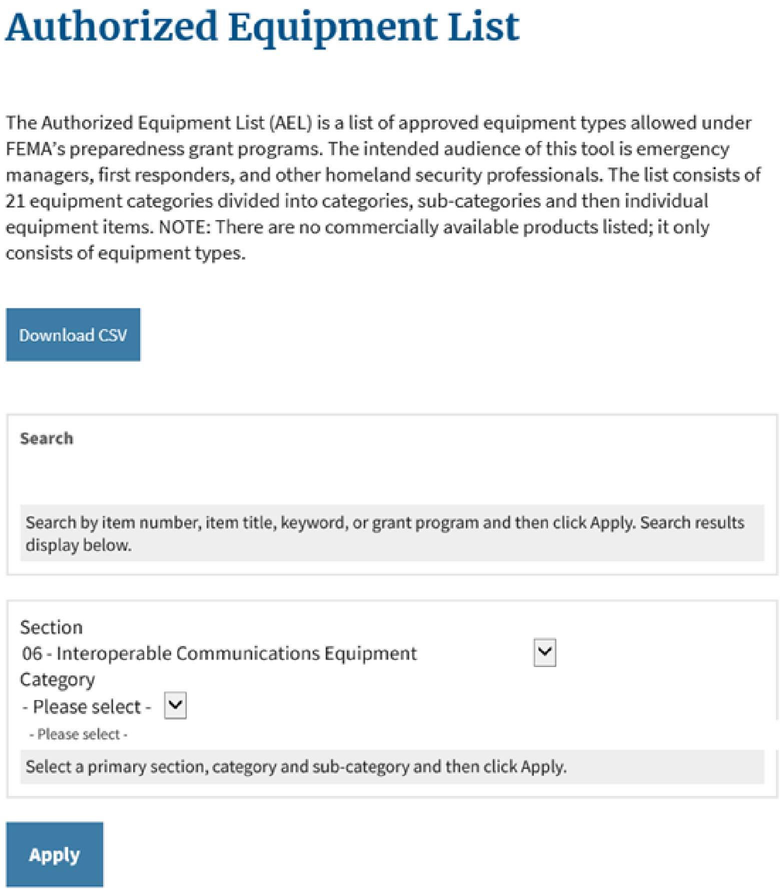
All equipment items are defined as tangible property having an acquisition cost of $1,000 or more, and a useful life of more than one year.

*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.

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.

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 20% 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 20% 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 20% 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

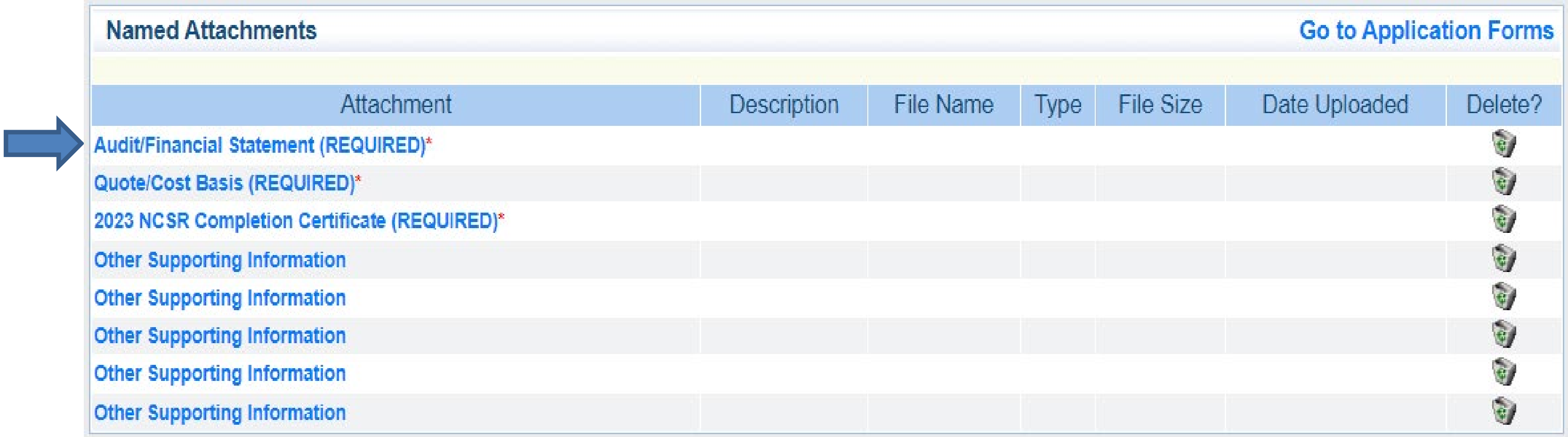
NAMED ATTACHMENTS

All attachments must be included in this section

- Required Attachments
  - Audit/Financial Statement
  - Quote/Cost Basis
  - 2023 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



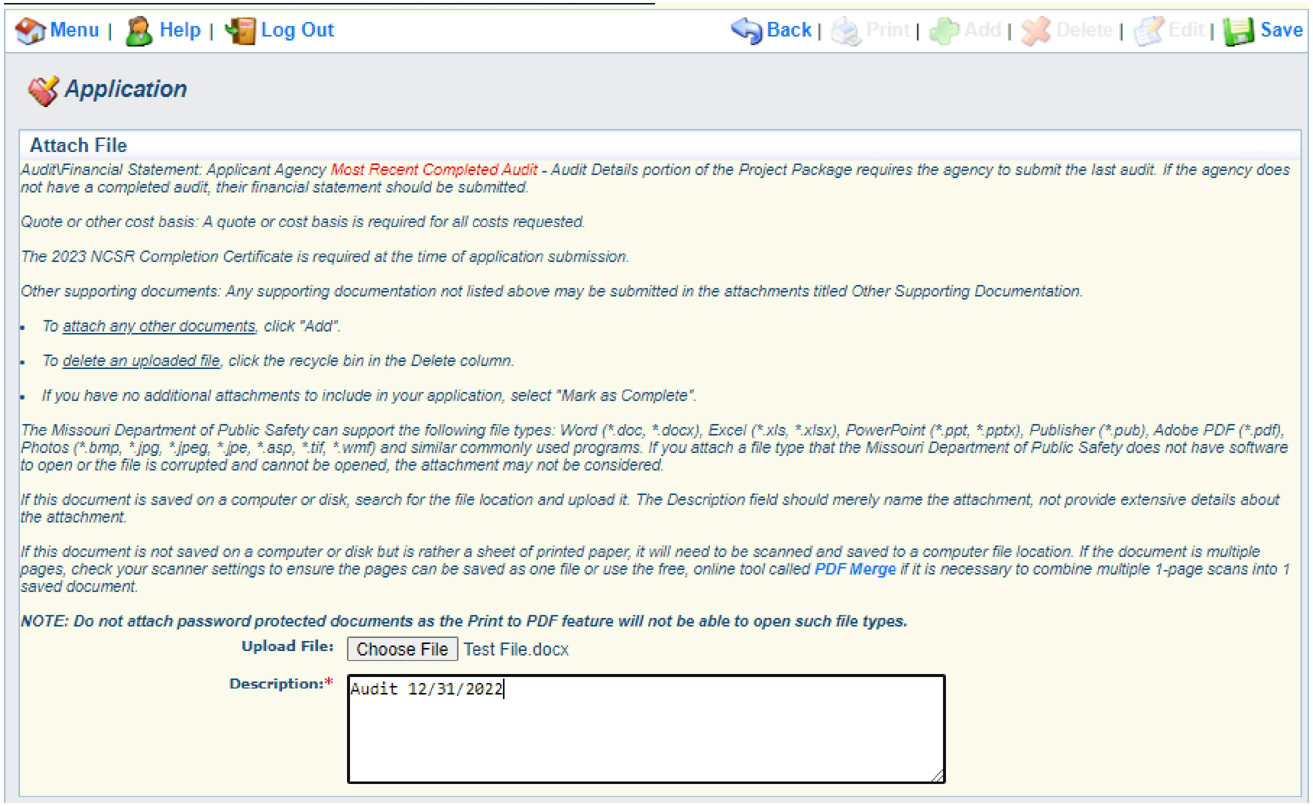
Named Attachments

Attachment	Description	File Name	Type	File Size	Date Uploaded	Delete?
Audit/Financial Statement (REQUIRED)*						🗑
Quote/Cost Basis (REQUIRED)*						🗑
2023 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
  - 2023 NCSR Completion Certificate

NAMED ATTACHMENTS

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



Application

Attach File

Audit\Financial 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.

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

The 2023 NCSR Completion Certificate is required at the time of application submission.

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.

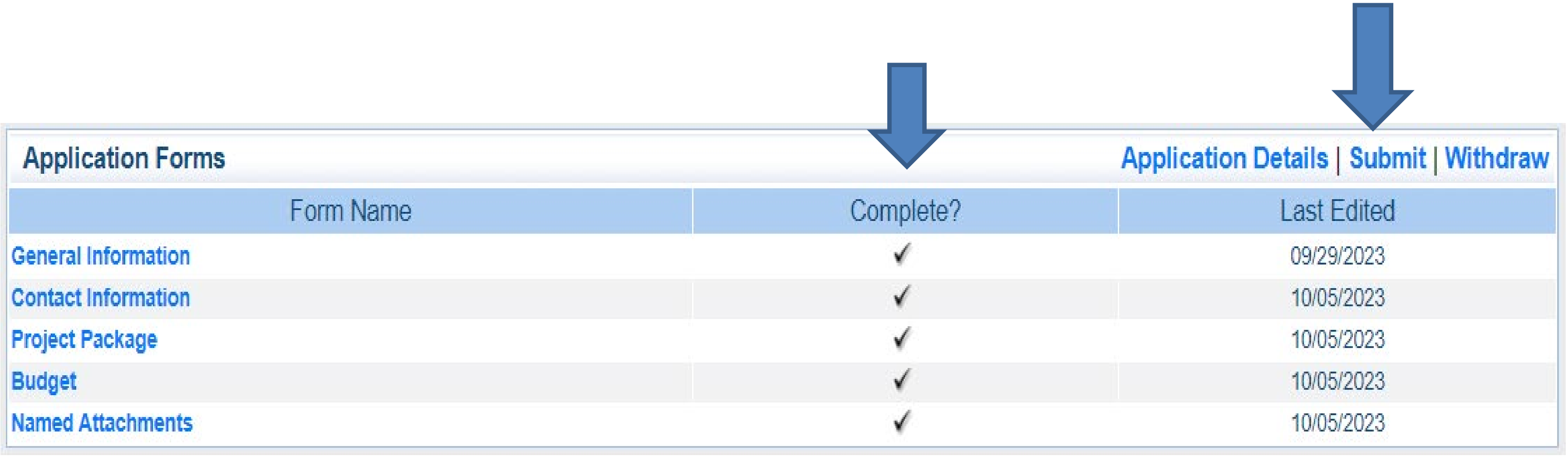
NOTE: Do not attach password protected documents as the Print to PDF feature will not be able to open such file types.

Upload File: Choose File Test File.docx

Description:* Audit 12/31/2022

SUBMISSION

- All forms **must be** <u>marked complete</u> in order to submit the application
- When everything is complete, select "Submit"



Application Forms

Application Details | Submit | Withdraw

Form Name	Complete?	Last Edited
General Information	✓	09/29/2023
Contact Information	✓	10/05/2023
Project Package	✓	10/05/2023
Budget	✓	10/05/2023
Named Attachments	✓	10/05/2023

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