FY 2024 State and Local Cybersecurity Grant Program (SLCGP)

Notice of Funding Opportunity (NOFO)

Grant Issued By:

U.S. Department of Homeland Security (DHS), Federal Emergency Management Agency (FEMA), Grant Programs Directorate (GPD)

Grant Issued Through:

Missouri Department of Public Safety (DPS), Office of Homeland Security (OHS)

Assistance Listing:

97.137

Funding Opportunity Title:

State and Local Cybersecurity Grant Program (SLCGP)

Overview:

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

Considering the risk and potential consequences of cyber incidents, strengthening the cybersecurity practices and resilience of state, local and territorial (SLT) governments is an important homeland security mission and the primary focus of the SLCGP. Through funding from the Infrastructure Investment and Jobs Act, referred to as the Bipartisan Infrastructure Law (BIL), the SLCGP enables DHS to make targeted cybersecurity investments in SLT government agencies to strengthen the security of critical infrastructure and improve the resilience of services SLT governments provide their communities.

The FY 2024 SLCGP aligns with the National Cybersecurity Strategy by addressing three of the five pillars:
- Pillar One – Defend Critical Infrastructure
- Pillar Two – Disrupt and Dismantle Threat Actors
- Pillar Four – Invest in a Resilient Future

The FY 2024 SLCGP also addresses the 2020-2024 DHS Strategic Plan by helping DHS achieve Goal 3: Secure Cyberspace and Critical Infrastructure. This includes Objective 3.2: Strengthen the Security and Resilience of Critical Infrastructure.

Additionally, the FY 2024 SLCGP supports the [2022-2026 FEMA Strategic Plan](#), which outlines a bold vision with three ambitious goals, including Goal 3: Promote and Sustain a Ready FEMA and Prepared Nation, under which falls Objective 3.2: Posture FEMA to meet current and emergent threats.

The FY 2024 SLCGP also aligns with the [2023-2025 CISA Strategic Plan](#), which encompasses Goal 1: Cyber Defense, Goal 2: Risk Reduction and Resilience and Goal 3: Operational Collaboration.

Funding Sources:

There are three funding sources available for FY 2024 SLCGP applicants:

1) State and Local Cybersecurity Grant Program (SLCGP) – Rural: SLCGP 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. The FY 2024 SLCGP requires 25% of the funds be provided to rural areas.

2) State and Local Cybersecurity Grant Program (SLCGP) – Non-Rural: SLCGP 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.

3) State and Local Cybersecurity Grant Program (SLCGP) – State: SLCGP State funds are dedicated for state agency applicants.

Goals and Objectives:

Goal: The goal of SLCGP is to assist state and local governments with managing and reducing systemic cyber risk.

Objectives: Applicants are required to submit applications that address at least one of the following program objectives in their application:

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

Requested projects must align to at least one of the above listed objectives. For more information on the program goals, objectives, sub-objectives, and desired outcomes, please refer to Appendix A.

Priorities:

For the FY 2024 SLCGP, the state of Missouri has established the following eight priorities:

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

Applicants should consider requesting projects to address the established priorities before other cybersecurity initiatives. Projects that align to Missouri priorities will receive additional points during the application scoring process.

Period of Performance: 36 months

      Projected Period of Performance Start Date: February 1, 2025

      Projected Period of Performance End Date: January 31, 2028

Costs obligated or incurred prior to the grant period of performance or receipt and full execution of a grant Subaward Agreement will NOT be eligible to receive funding.

Funding Instrument: Grant

Allowable Amount: $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.

Cost Share of Match: 30% cost share requirement (cash [hard match] or in-kind [soft match])

DHS/FEMA/DPS/OHS administers cost-matching requirements in accordance with 2 C.F.R 200.306. To meet matching requirements, the 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. **The non-federal cost share requirement cannot be matched with other federal funds, unless specifically authorized by the legislation governing that other source of federal funding.**

Hard Match (Cash): Cash or hard matching includes cash spent for project-related costs. The allowable cash match must include costs that are necessary, reasonable, and allowable under the SLCGP.

Soft Match (In-kind): Soft match refers to contributions of the reasonable value of property or services in lieu of cash which benefit a federally assisted project or program. This type of match may only be used if not restricted or prohibited by program statute, regulation, or guidance and must be supported with source documentation. Only property or services that comply with program guidance and/or program regulations, are allowable. In other words, 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.**

Cost share can be calculated using the formula below:

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

30% x $142,857.14 = $42,857.14 Subrecipient Cost Share

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

30% x $285,714.29 = $85,714.29 Subrecipient Cost Share

Eligible Applicants:

- Local governments as defined in 6 U.S.C. section 101(13) as

    o 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

    o A rural community, unincorporated town or village, or other public entity

- State units of government

Ineligible Applicants:

- Nonprofit organizations

- Private corporations

- Private educational institutions

Other Eligibility Criteria:

Nationwide Cybersecurity Review (NCSR)

Applicant agencies **MUST** have completed the 2024 Nationwide Cybersecurity Review (NCSR). 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. The NCSR must be completed and results received at the time of application submission. The NCSR Completion

Certificate **MUST** be uploaded in the Named Attachments Form of the application. The requested project must align to closing gaps and/or strengthening capabilities in the agency's NCSR.

The 2024 NCSR can be completed by visiting the following link: https://www.cisecurity.org/ms-isac/services/ncsr. The following documents are available to assist in completion of the NCSR:

- NCSR FAQs
- NCSR One Page Overview
- NCSR General User Guide
- NCSR Assessment Demo
- NCSR Completion Certificate Instructions

Please note: New user accounts will be created within 2-4 business days of completing the registration form. It may take approximately 4-6 hours to complete the NCSR and the agency should allow up to two weeks to receive the results. If your agency has previously completed the NCSR, majority of the responses will be pre-populated and responses can be updated as applicable. **Please ensure you complete the NCSR in advance of the application deadline.**

If an applicant agency is selected to receive FY 2024 SLCGP funds, the NCSR must be completed annually, throughout the grant period of performance.

DPS/OHS Cybersecurity Program

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 (i.e., Missouri Office of Homeland Security (OHS), Missouri Information Analysis Center (MIAC), St. Louis Fusion Center, Kansas City Regional Fusion Center) at the time of application submission to be eligible for funding. Entities can subscribe to the DPS/OHS Cybersecurity Program by emailing securityintel@mshp.dps.mo.gov with your name, agency/entity, title, desk phone, work phone, and email address.

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.

- **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 <u>prior</u> 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 <u>prior</u> to submitting an application.

- **Section 590.1265 RSMo** – **Police Use of Force Transparency Act of 2021**
  Pursuant to section 590.1265 RSMo Use of force incidents reporting standards and procedures, publication of report data, analysis report. Each law enforcement agency shall report data submitted under subsection 3 of this section to the department of public safety. *For purposes of grant eligibility, law enforcement agencies will be considered non-compliant if they have not submitted Use of Force reports for three or more months in the past twelve months..*

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

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

- **Section 590.030 RSMo** – **Rap Back Program Participation**
  Pursuant to section 590.030 RSMo, all law enforcement agencies shall enroll in the state and federal Rap Back programs on or before January 1, 2022 and continue to remain enrolled. The law enforcement agency shall take all necessary steps to maintain officer enrollment for all officers commissioned with that agency in the Rap Back programs. An officer shall submit to

being fingerprinted at any law enforcement agency upon commissioning and for as long as the officer is commissioned with that agency. Each law enforcement agency shall certify compliance with section 590.030 RSMo when accepting any grants administered by the Department of Public Safety.

Application and Submission Information:

1. **Key Dates and Times**

   a. Application Start Date: October 18, 2024

   b. Application Submission Deadline: December 4, 2024 5:00 p.m. CST

2. **Agreeing to Terms and Conditions of the Award**

By submitting an application, applicants agree to comply with the requirements of this NOFO and the terms and conditions of the award, should they receive an award.

Applications will only be accepted through the Missouri Department of Public Safety (DPS) online WebGrants System. https://dpsgrants.dps.mo.gov/index.do

An application workshop with instructions on how to apply through the WebGrants System will be available on the DPS website, at the following link under Grant Applications and Forms, FY 2024 State and Local Cybersecurity Grant Program (SLCGP): https://dps.mo.gov/dir/programs/ohs/grantstraining/

As part of the FY 2024 SLCGP application, each eligible applicant must complete all application forms and provide all required documents:

1. **Contact Information Form**

2. **SLCGP Project Package**

3. **Budget**

4. **Named Attachments**
   a. **Audit/Financial Statement (REQUIRED)**
   b. **Quote or Cost Basis (REQUIRED)**
   c. **2024 NCSR Completion Certificate (REQUIRED)**
   d. **Other Supporting Documentation (up to 5 attachments)**

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.

Funding Restrictions and Allowable Costs:

All costs charged to federal awards (including both federal funding and any non-federal matching or cost sharing funds) must comply with applicable statutes, rules and regulations, and policies, this NOFO, and the terms and conditions of the federal award. They must also comply with the the Uniform Administrative Requirements, Cost Principles, and Audit Requirements at 2 C.F.R. Part 200, unless otherwise indicated in the NOFO or the terms and conditions of the federal award. This includes, among

other requirements that costs must be incurred, and products and services must be delivered, within the budget period.

Allowable Costs:

There are five allowable expense categories as listed below:

1. Planning
2. Organization
3. Equipment
4. Training
5. Exercise

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. The requested project **MUST**:

- Close gaps and strengthen capabilities identified in the agencies' Nationwide Cybersecurity Review (NCSR)
- Align with the Missouri Comprehensive Cybersecurity Plan (CCP) which can be accessed in the WebGrants System during completion of the application
- Align with at least one of the FY 2024 SLCGP Objectives (FY 2024 SLCGP Objectives can be found in Appendix A)

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.

Planning:

Planning costs are allowable under this program. SLCGP funds may be used for planning activities that support the FY 2024 SLCGP objectives, Missouri Comprehensive Cybersecurity Plan (CCP), and closing gaps and strengthening capabilities in the applicant's NCSR.

Organization:

Organization costs are allowable under this program. 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, equipment, training, and exercise (POETE) activities. Personnel expenses may include, but are 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.

Equipment:

Equipment costs are allowable under this program. 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.

Subrecipients will be responsible for obtaining and maintaining all necessary certifications and licenses for the requested equipment. Investments in emergency communications systems and equipment must meet applicable SAFECOM Guidance recommendations. Such investments must coordinated with the Statewide Interoperability Coordinator (SWIC) and the State Interoperability Governing Body (SIGB) to ensure interoperability and long-term compatibility.

SLCGP funds may be used to purchase maintenance contracts or agreements, warranty coverage, licenses, and user fees in support of a system or equipment. These contracts may exceed the period of performance if they are purchased incidental to the original purchase of the system or equipment as long as the original purchase of the system or equipment is consistent with that which is typically provided for, or available through, these types of agreements, warranties, or contracts. When purchasing a stand-alone warranty or extending an existing maintenance contract on an already-owned piece of equipment system, coverage purchased may not exceed the period of performance of the award used to purchase the maintenance agreement or warranty, and it may only cover equipment purchased with SLCGP funds or for equipment dedicated for SLCGP-related purposes. As with warranties and maintenance agreements, this extends to licenses and user fees as well.

The use of SLCGP grant funds for maintenance contracts, warranties, repair or replacement costs, upgrades, and user fees are allowable, unless otherwise noted. Except for maintenance plans or extended warranties purchased incidental to the original purchase of the equipment, the period covered by maintenance or warranty plan must not exceed the POP of the specific grant funds used to purchase the plan or warranty.

Training:

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

Some training activities require Environmental and Historic Preservation (EHP) Review, including exercises, drills, or trainings that require any type of land, water, or vegetation disturbance or building of temporary structures or that are not located at facilities designed to conduct training and exercises. Additional information on training requirements and EHP review can be found online at https://www.fema.gov/media-library/assets/documents/90195.

Exercise:

Exercise costs are allowable under this program. Exercises conducted with grant funding should be managed and conducted consistent with 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.

Some exercise activities require Environmental and Historic Preservation (EHP) Review, including exercises, drills, or trainings that require any type of land, water, or vegetation disturbance or building of temporary structures or that are not located at facilities designed to conduct training and exercises. Additional information on training requirements and EHP review can be found online at https://www.fema.gov/media-library/assets/documents/90195.

Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services

Subrecipients and their contractors must comply with the prohibitions set forth in Section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232 (2018) (FY 2019 NDAA) and 2 C.F.R. §§ 200.216, 200.327, 200.471, and Appendix II to 2 C.F.R. Part 200. The FY 2019 NDAA and these regulations, as they apply to subrecipients and their contractors, provide for two distinct prohibitions: (1) prevent the use of federal award funds to procure or obtain covered telecommunications equipment or services; and (2) prevent the use of federal award funds to contract with an entity that uses such covered telecommunications equipment or services.

Guidance is available at Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services (Interim) FEMA Policy #405-143-1.

Additional guidance is available at Contract Provisions Guide: Navigating Appendix II to Part 200 – Contract Provisions for Non-Federal Entity Contracts Under Federal Awards (fema.gov).

FEMA subrecipients **may not** use any FEMA funds under open or new awards to:

a. 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;

b. 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

c. 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.

I. **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.

II. **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:

i. Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation, (or any subsidiary or affiliate of such entities);

ii. 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);

iii. Telecommunications or video surveillance services provided by such entities or using such equipment; or

iv. Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the People's Republic of China.

Examples of the types of products covered by this prohibition include phones, internet, video surveillance, and cloud servers when produced, provided, or used by the entities listed in the definition of "covered telecommunications equipment or services." See 2 C.F.R. § 200.471b.

Unallowable Costs:

For FY 2024 SLCGP, grant funds may not be used for the following:

- Spyware;
- Construction;
- Renovation;
- To pay a ransom;
- For recreational or social purposes;
- To pay for cybersecurity insurance premiums;
- To acquire land or to construct, remodel, or perform alterations of buildings or other physical facilities (This prohibition does not include minor building modifications necessary to install and connect grant-purchased equipment that do not substantially affect a building's structure, layout, systems, or critical aspects of a building's safety, or otherwise materially increase the value or useful life of a building);
- For any purpose that does not address cybersecurity risks or cybersecurity threats on information systems owned or operated by, or on behalf of, the eligible entity that receives the grant or a local government within the jurisdiction of the eligible entity;
- To supplant state or local funds; however, this shall not be construed to prohibit the use of funds from a grant under this NOFO for otherwise permissible uses on the basis that the SLT has previously used SLT funds to support the same or similar purposes; and
- For any subrecipient cost-sharing contribution

Required 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

The DPS/OHS Cybersecurity Team has resources available to assist with these benchmarks. If assistance is needed, please contact the OHS Cybersecurity Team by phone at 573-526-0153 or by email at securityintel@mshp.dps.mo.gov.

Required Services and Memberships

If awarded funding, all SLCGP subrecipients are required to participate in a limited number of free services by CISA/DPS/OHS. For these required services and memberships, please note that participation is not required for submission and approval of a grant but is a post-award requirement.

Cyber Hygiene Services

Vulnerability Scanning evaluates external network presence by executing continuous scans of public, static, Internet Protocols for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts.

To register for this service, email vulnerability@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services – SLCGP" to get started. Indicate in the body of your email that you are requesting this service as part of the SLCGP. For more information, visit CISA's Cyber Hygiene Information Page.

Administrative and National Policy Requirements:

In addition to the requirements in this section and in this NOFO, FEMA/DPS/OHS may place specific terms and conditions on individual awards in accordance with 2 C.F.R. Part 200.

DHS Standard Terms and Conditions:

All successful applicants for DHS grant and cooperative agreements are required to comply with DHS Standards Terms and Conditions, which are available online at: DHS Standard Terms and Conditions.

The applicable DHS Standard Terms and Conditions will be those in effect at the time the award was made. What terms and conditions will apply for the award will be clearly stated in the award package at the time of the award.

Ensuring the Protection of Civil Rights:

As the Nation works towards achieving the National Preparedness Goal, it is important to continue to protect the civil rights of individuals. Subrecipients must carry out their programs and activities, including those related to the building, sustainment, and delivery of core capabilities, in a manner that respects and ensures the protection of civil rights for protected populations.

Federal civil rights statutes, such as Section 504 of the Rehabilitation Act of 1973 and Title VI of the Civil Rights Act of 1964, along with DHS and FEMA regulations, prohibit discrimination on the basis of race, color, national origin, sex, religion, age, disability, limited English proficiency, or economic status

in connection with programs and activities receiving federal financial assistance from FEMA, as applicable.

The DHS Standard Terms and Conditions include a fuller list of the civil rights provisions that apply to subrecipients. These terms and conditions can be found in the DHS Standard Terms and Conditions. Additional information on civil rights provisions is available at https://www.fema.gov/about/offices/equal-rights/civil-rights.

Monitoring and oversight requirements in connection with subrecipient compliance with federal civil rights laws are also authorized pursuant to 44 C.F.R. Part 7 or other applicable regulations.

In accordance with civil rights laws and regulations, subrecipients must ensure the consistent and systematic fair, just, and impartial treatment of all individuals, including individuals who belong to underserved communities that have been denied such treatment.

Environmental Planning and Historic Preservation (EHP) Compliance:

As a federal agency, FEMA is required to consider the effects of its actions on the environment and historic properties to ensure that all activities and programs funded by FEMA, including grant-funded projects, comply with federal EHP laws, Executive Orders, regulations, and policies, as applicable.

Subrecipients proposing projects that have the potential to impact the environment, including, but not limited to, the construction of communication towers, modification or renovation of existing buildings, structures, and facilities, or new construction including replacement of facilities, must participate in the FEMA EHP review process. The EHP review process involves the submission of a detailed project description along with any supporting documentation requested by FEMA in order to determine whether the proposed project has the potential to impact environmental resources including, but not limited to, threatened or endangered species and historic properties; and identify mitigation measures and/or alternative courses of action that may lessen any impact to those resources.

In some cases, FEMA is also required to consult with other regulatory agencies and the public in order to complete the review process. Federal law requires EHP review to be completed before federal funds are released to carry out proposed projects. FEMA may not be able to fund projects that are not in compliance with applicable EHP laws, Executive Orders, regulations, and policies. FEMA may recommend mitigation measures and/or alternative courses of action to lessen any impact to environmental resources and bring the project into compliance with EHP requirements.

Guidance on the EHP process is found at Environmental Planning and Historic Preservation. The site contains links to various documents including those identifying agency EHP responsibilities and program requirements, such as implementation of the National Environmental Policy Act and other EHP laws, regulations, and Executive Orders. DHS and FEMA EHP policy is also found in the EHP Directive and Instruction.

All FEMA actions, including grant-funded actions, must comply with National Flood Insurance Program criteria or ay more restrictive federal, state, or local floodplain management standards or building code (44 C.F.R. section 9.11(d)(6)).

The GPD EHP screening form is located at https://www.fema.gov/sites/default/files/documents/fema_ehp-screening_form_ff-207-fy-21-100_5-26-2021.pdf. Additionally, all subrecipients under this funding opportunity are required to

comply with the FEMA GPD EHP Policy Guidance, FEMA Policy #108-023-1, available at
https://www.fema.gov/sites/default/files/documents/fema_gpd-ehp-policy-guidance.pdf.

SAFECOM Guidance Compliance:

All entities using SLCGP funding to support emergency communications investments are required to
comply with the SAFECOM Guidance on Emergency Communications Grants (SAFECOM Guidance).
The SAFECOM Guidance provides current information on emergency communications policies, eligible
costs, best practices, and technical standards for state and local recipients investing federal funds in
emergency communications projects. It is also designed to promote and align with the National
Emergency Communications Plan (NECP). Conformance with the SAFECOM Guidance helps ensure
that federally funded investments are compatible, interoperable, resilient, and support national goals and
objectives for improving emergency communications.

Applicants should use the SAFECOM Guidance during planning, development, and implementation of
emergency communications projects and in conjunction with other planning documents.

Contact Information:

Additional information and resources can be located on the Missouri Department of Public Safety, Office of Homeland Security website: https://dps.mo.gov/dir/programs/ohs/grantstraining/

WebGrants System, application submission site: https://dpsgrants.dps.mo.gov/index.do

For project specific questions, please contact the Missouri Department of Public Safety (DPS)/Office of Homeland Security (OHS) Cybersecurity Program by phone at 573-526-0153 or email at securityintel@mshp.dps.mo.gov

For grant or WebGrants specific questions, please contact the DPS Grants. Contact information for the grants team is listed below.

DPS Grants:

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

Joni McCarter
Program Manager
(573) 526-9020
Joni.mccarter@dps.mo.gov

Kelsey Saunders
Administrative Assistant
(573) 522-6125
Kelsey.saunders@dps.mo.gov

Appendix A Goals and Objectives

The program objectives for the SLCGP are as follows: (1) develop and establish appropriate governance structures, as well as develop, implement, or revise cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations; (2) ensure state and local agencies understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments; (3) implement security protections commensurate with risk (outcomes of Objectives 1 & 2); and (4) ensure organization personnel are appropriately trained in cybersecurity, commensurate with their responsibilities.

These program objectives are further divided into sub-objectives and outcomes, as well as sample evidence of implementation are provided to assist the reader.

Goal of the SLCGP: Assist state and local governments with managing and reducing systemic cyber risk.

Program Objective	Program Sub-Objective(s)	Outcome(s)	Evidence of Implementation Example
1. Develop and establish appropriate governance structures, as well as develop, implement, or revise cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations	1.1: Establish cybersecurity governance structures and implement a program to evaluate maturity of the cybersecurity program aligned to Cybersecurity Performance Goals established by CISA and the National Institute of Standards and Technology (NIST).	1.1.1 Participants have established and documented a uniform cybersecurity governance structure that is accountable to organizational leadership and works together to set the vision for cyber risk management.	Organization has a cybersecurity defense concept of operations, with responsibilities assigned to specific organizational roles.
		1.1.2 Participants have identified senior officials to enable whole-of organization coordination on cybersecurity policies, processes and procedures.	
	1.2 Develop, implement, or revise, and test cybersecurity plans, including cyber incident response plans, with clearly defined roles and responsibilities.	1.2.1 Develop, implement, or revise and exercise cyber incident response plans.	Organization conducts annual table-top and full-scope exercises that include practical execution of restoration and recovery processes to test approved cybersecurity plans. Conducting these exercises allow

Program Objective	Program Sub-Objective(s)	Outcome(s)	Evidence of Implementation Example
			organizations to test approved cybersecurity plans. Conducting these exercises allow organizations to test approved cybersecurity plans to identify, protect, detect, respond to and recover from cybersecurity incidents, in line with the NIST Cybersecurity Framework, and demonstrates process to incorporate lessons learned from the exercise into their cybersecurity program.
	1.3 Asset (e.g., devices, data, software) protections and recovery actions are prioritized based on the asset's criticality and business value.	1.3.1 Ensure that systems and network functions are prioritized and reconstituted according to their impact to essential functions.	Organizations conducts a regular business impact assessment to prioritize which systems must be protected and recovered first.
Program Objective	**Program Sub-Objective(s)**	**Outcome(s)**	**Evidence of Implementation Example**
2. SLT agencies understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation and structured assessments	2.1 Physical devices and systems, as well as software platforms and applications, are inventoried.	2.1.1 Establish and regularly update asset inventory.	Organization maintains and regularly updates an asset inventory list.
	2.2 Cybersecurity risk to the organization's operations and assets are understood.	2.2.1 Conduct an annual cyber risk assessment to identify cyber risk management gaps and areas for improvement.	Organization annually completes the Nationwide Cybersecurity Review (NCSR).
	2.3 Vulnerability scans are performed, and a risk-based vulnerability management plan is developed and implemented.	2.3.1 Participate in CISA's Vulnerability Scanning service, part of the Cyber Hygiene program.	Organization is an active participant in CISA's Cyber Hygiene Program
		2.3.2 Effectively manage vulnerabilities by prioritizing mitigation of high impact vulnerabilities	Organization has a plan to manage vulnerabilities based on those with the highest criticality, internet-facing vulnerabilities,

		and those most likely to be exploited.	as well as known exploited vulnerabilities identified in CISA's Known Exploited Vulnerabilities Catalog.
	2.4 Capabilities are in place to monitor assets to identify cybersecurity events.	2.4.1 State and local agencies are able to analyze network traffic and activity transiting or traveling to or form information systems, applications, and user accounts to understand baseline activity and identify potential threats.	Not Applicable
	2.5 Processes are in place to action insights derived from deployed capabilities.	2.5.1 State and local agencies are able to respond to identified events and incidents, document root cause, and share information with partners.	Not Applicable
Program Objective	**Program Sub-Objective(s)**	**Outcome(s)**	**Evidence of Implementation Example**
3. Implement security protections commensurate with risk (Outcomes of goals 1 & 2).	3.1 State and local agencies adopt fundamental cybersecurity best practices.	3.1.1 Implement multi-factor authentication (MFA), prioritizing privileged users, Internet-facing systems, and cloud accounts.	The organization implements MFA for all remote access and privileged accounts.
	3.2 Reduce gaps identified through assessment and planning process and apply increasingly sophisticated security protections commensurate with risk.	3.2.1 Individual participants address items identified through assessments and planning process.	Not Applicable
		3.2.2 State and local entities improve cybersecurity ecosystem by collaborating to address items identified through assessments and planning process (e.g., regional and intra-state efforts).	Not Applicable

Program Objective	Program Sub-Objective(s)	Outcome(s)	Evidence of Implementation Example
4. Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.	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.	4.1.1 Organization requires regular ongoing phishing training, awareness campaigns are conducted, and organization provides role-based cybersecurity awareness training to all employees.	Not Applicable
		4.1.2 Organization has dedicated resources and funding available for its cybersecurity professionals to attend technical trainings and conferences.	Not Applicable
	4.2 Organization has adopted the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.	4.2.1 Organization has established cyber workforce development and training plans, based on the NICE Cybersecurity Workforce Framework.	Not Applicable