FY 2025 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 threats to the homeland from increasingly sophisticated criminal groups and nation-state actors. State, local, and territorial (SLT) entities stand at the forefront of cyber defense, enforcing laws, assisting the federal government in securing borders, cyberspace, and dismantling transnational criminal organizations. Cybersecurity threats, including ransomware intrusions, and widespread software vulnerabilities affecting SLT systems and critical infrastructure, are increasingly exploited by malicious actors, operating both domestically and abroad. To strengthen the essential partnership DHS maintains with its SLT partners in executing its mission, DHS is committed to supporting SLT efforts to combat cybersecurity threats and mitigate risks that endanger these vital functions.

Considering the risk and potential consequences of cyber incidents, the focus of the SLCGP is strengthening the cybersecurity practices and resilience of SLT governments. 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.

Funding Sources:

There are two funding sources available for FY 2025 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 2025 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.

Goals and Objectives:

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

Objectives: Applicants are required to submit applications that address 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 2025 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: 45 months

Projected Period of Performance Start Date: September 1, 2025

Projected Period of Performance End Date: May 31, 2029

****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 or Local Match: 40% 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, and allowable costs identified in the NOFO, etc. **The same contribution cannot be used if it is already used as match for another 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: $\frac{\$100,000}{60\%} = \$166,666.67$ Total Project Costs

40% x $166,666.67 = $66,666.67 Subrecipient Cost Share

Example 2: $\frac{\$200,000}{60\%} = \$333,333.33$ Total Project Costs

40% x $333,333.33 = $133,333.33 Subrecipient Cost Share

Eligible Applicants:

- Local governments as defined in 6 U.S.C. section 101(11) as
    - 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

Ineligible Applicants:

- Nonprofit organizations
- Private corporations
- Private educational institutions
- State units of government

Other Eligibility Criteria:

CISA Cybersecurity Performance Goals Assessment

Applicant agencies **MUST** have completed the CISA Cybersecurity Performance Goals (CPG) Assessment. The CISA's Cybersecurity Performance Goals (CPGs) are a set of voluntary, high-impact security practices designed to help organizations, particularly those in critical infrastructure, improve their cybersecurity posture. The CPGs are not a checklist, but rather a framework for prioritizing and implementing security measures to mitigate the most common and impactful cyber threats. CISA also provides tools and resources, like the Cybersecurity Evaluation Tool (CSET), to help organizations assess their progress and identify areas for improvement. The CSET can be accessed at the following link: https://www.cisa.gov/downloading-and-installing-cset. Please see the CISA CPG Assessment PowerPoint for step-by-step instructions to download the CSET and complete the CPG Assessment. The CPG Report **MUST** be uploaded in the Named Attachments Form of the application. **Note: The CISA CPG Report contains sensitive cybersecurity information. This report is exempt from release under the Missouri Sunshine Law (Section 610.021 (19) RSMo).** The requested project must align to closing gaps and/or strengthening capabilities in the agency's CISA CPG Assessment.

If an applicant agency is selected to receive FY 2025 SLCGP funds, the CISA CPG Assessment 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.

DPS GRANTS – STATE REQUIREMENTS

To be eligible for grant funding through the Missouri Department of Public Safety (DPS), agencies must be compliant with the requirements listed below (as applicable) at the time of application and if awarded funding, must maintain compliance throughout the grant period of performance.

LAW ENFORCEMENT REQUIREMENTS

These requirements below apply only to law enforcement agencies.
Each law enforcement agency shall certify compliance with these requirements below when applying for grants administered by the DPS.

Section 590.650 RSMo – Vehicle Stops Report

Pursuant to Section 590.650.3 RSMo, each law enforcement agency shall compile the data described in subsection 2 for the calendar year into a report to the attorney general and each law enforcement agency shall submit the report to the attorney general no later than March first of the following calendar year.

NOTE: Failure to submit the Vehicle Stops (Racial Profiling) Report will result in the automatic denial of 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.

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.

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

Pursuant to Section 590.1265 RSMo, 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 previous 12 months.

NOTE: Show Me Crime Reporting provides a no cost option for agencies to comply with Section 590.1265 RSMo. Agencies not currently compliant with Section 590.1265 RSMo will not be eligible to apply until they have registered with Show Me Crime Reporting and have begun submitting Use of Force reports.
https://showmecrime.mo.gov/CrimeReporting/ForcePage.html

Section 43.505 RSMo – Uniform Crime Reporting (UCR)

Pursuant to Section RSMo 43.505.3, 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.

Agencies not compliant at the time of application will be ineligible for funding.

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 previous 12 months.

NOTE: Show Me Crime Reporting provides a no cost option for agencies to comply with Section 43.505 RSMo. Agencies 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.

FIRE AGENCY REQUIREMENT

This requirement applies only to fire agencies.

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.

EMS REQUIREMENTS

These requirements apply only to EMS agencies.

Section 190.105 RSMo – Ambulance License

Pursuant to Section 190.105 RSMo, no person, either as owner, agency or otherwise, shall furnish, operate, conduct, maintain, advertise, or otherwise be engaged in or profess to be engaged in the business or service of the transportation of patients by ambulance in the air, upon the streets, alleys, or any public way or place of the state of Missouri unless such person holds a currently valid license from the department for an ambulance service pursuant to the provisions of sections 190.001 RSMo to 190.245.

NOTE: If the applicant agency is an ambulance service, a copy of the license certificate as required by section 190.105 RSMo MUST be submitted in the Named Attachments component of the application.

Section 190.133 RSMo – Emergency Medical Response Agency License

Pursuant to Section 190.133(4) RSMo, no person or entity shall hold itself out as an emergency medical response agency that provides advanced life support or provide the services of an emergency medical response agency that provides advanced life support unless such person or entity is licensed by the state of Missouri Department of Health and Senior Services.

NOTE: If the applicant agency is an emergency medical response agency, a copy of the license certificate as required by section 190.133(4) RSMo MUST be submitted in the Named Attachments component of the application.

Application and Submission Information:

1. **Key Dates and Times**

   a. Application Start Date: April 13, 2026

   b. Application Submission Deadline: May 20, 2026 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 2025 State and Local Cybersecurity Grant Program (SLCGP): https://dps.mo.gov/dir/programs/ohs/grantstraining/

As part of the FY 2025 SLCGP application, each eligible applicant must complete all application forms and provide all required documents:

1. **Contact Information**

2. **DPS Grants State Requirements**

3. **SLCGP Project Package**

4. **Budget**

5. **Named Attachments**
    a. **Audit/Financial Statement (REQUIRED)**
    b. **Quote or Cost Basis (REQUIRED)**
    c. **CISA CPG Report (REQUIRED)**
    Note: The CISA CPG Report contains sensitive cybersecurity information. This report is exempt from release under the Missouri Sunshine Law (Section 610.021 (19) RSMo).
    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.

General Funding Requirements:

Costs charged to federal awards (including federal and non-federal cost share funds) must comply with applicable statutes, rules, and regulations, policies, this NOFO, and 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. 2 C.F.R. § 200.403(h).

Subrecipients may not use federal funds or any cost share funds for the following activities:

1. Matching or cost sharing requirements for other federal grants and cooperative agreements (see 2 C.F.R. § 200.306).
2. Lobbying or other prohibited activities under 18 U.S.C. § 1913 or 2 C.F.R. § 200.450.
3. Prosecuting claims against the federal government or any other government entity (see 2 C.F.R. § 200.435).

Subrecipients may use SLCGP funding to perform minor modifications that do not substantially affect a building's structure, layout, or systems, affect critical aspects of a building's safety, or otherwise materially increase the value or useful life of the building. The prohibition would also apply to the non-federal cost-sharing requirement borne by the subrecipient.

Examples of the types of minor modifications that could be allowable with SLCGP funding, and the non-federal cost share are listed below:

- Fastening equipment to walls where it does not become a permanent fixture (such as hanging a server rack with servers on a wall).
- Replacing an outdated existing electrical or internet outlet into which the equipment will connect.
    - For example, replacing an electrical outlet would involve turning off power, unscrewing a cover plate and outlet itself, pulling the outlet from the electrical box, disconnecting wires from the old outlet, connecting the wires to the new outlet, placing the new outlet in the electrical box, securing it with screws, reattaching the cover plate, and turning the power back on. This work very clearly does not involve a substantial change to the building and does not comprise an alteration.

- Installing new cabling.
- Replacing existing cabling.
- Moving cabling.
- Installing and connecting information system equipment to the building's network and power supply and internet.
- Making a hole in the wall to attach the equipment to the building's network, power, or internet.

Minor modifications may be permitted under the SLCGP subject to Environmental and Historic Preservation (EHP) review.

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' CISA Cybersecurity Performance Goals (CPG) Assessment
- 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 2025 SLCGP Objectives (FY 2025 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 2025 SLCGP objectives, Missouri Comprehensive Cybersecurity Plan (CCP), and closing gaps and strengthening capabilities in the applicant's CISA CPG Assessment.

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, and 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 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 CISA CPG Assessment 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/emergency-managers/practitioners/environmental-historic.

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/emergency-managers/practitioners/environmental-historic.

Prohibitions on Covered Equipment or Services

Subrecipients, their contractors, and subcontractors must comply with the prohibitions set forth in Section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019, which restricts the purchase of covered telecommunications and surveillance equipment and services. Please see 2 C.F.R. §§ 200.216, 200.327, 200.471 and Appendix II to 2 C.F.R. Part 200, and FEMA Policy #405-143-1 – Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services for more information.

Unallowable Costs:

For FY 2025 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;
- Costs associated with the Center for Internet Security (e.g., Multi-State Information Sharing and Analysis Center (MS-ISAC) and Election Infrastructure Information Sharing and Analysis (EI-ISAC)), including but not limited to membership fees and services;
- 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 uses; and
- For any subrecipient cost-sharing contribution
- To acquire land or to construct, remodel, or perform alterations of buildings or other physical facilities (This prohibition does not include minor building modifications; see Minor Modifications Information Bulletin No. 523) Unallowed alterations include permanent modifications that substantially affect the building's structure, layout, or systems, affect critical

aspects of a building's safety (such as structural integrity, fire safety systems), or other modifications that materially increase the value or useful life of the building.

- Examples of the types of alterations that are unallowable with SLCGP funding, or the non-federal cost share, are listed below:
  - Updating an electrical system to a building which involves work to enhance or modernize the electrical infrastructure, such as replacing electrical panels, upgrading old or unsafe wiring, and replacing circuit breakers. This type of work is likely a modification that substantially affects the building's systems and thus would comprise an alteration.
  - Installing new walls or reconfiguring existing ones.
  - Affixing equipment in such a way that it becomes a permanent part of a building (as this would result in the equipment no longer being personal property).

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.

Presidential Executive Orders

Subrecipients must comply with the requirements of Presidential Executive Orders related to grants (also known as federal assistance and financial assistance), the full text of which are incorporated by reference.

DHS Standard Terms and Conditions:

A subrecipient under this funding opportunity must comply with the DHS Standards Terms and Conditions in effect as of the time of the federal award. The DHS Standard Terms and Conditions are available online: 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.

A subrecipient under this funding opportunity must comply with the FY 2025 Department of Homeland Security Standard Terms and Conditions, v. 3 (Apr. 18, 2025), with the exception Paragraph C.IX (Communication and Cooperation with the Department of Homeland Security and Immigration Officials) and paragraph C.XVII(2)(a)(iii)(Anti-Discrimination Grant Award Certification regarding immigration). Paragraphs C.IX and C.XVII(2)(a)(iii) do not apply to any federal award under this funding opportunity. The FY 2025 Department of Homeland Security Standard Terms and Conditions, v. 3 (Apr. 18, 2025) are available at https://www.dhs.gov/sites/default/files/2025-08/2025_0418_fy2025_dhs_terms_and_conditions_version_3.pdf.

Environmental Planning and Historic Preservation (EHP) Compliance:

The federal government is required to consider effects of its actions on the environment and historic properties to ensure that activities, grants, and programs funded by FEMA, comply with federal EHP laws, Executive Orders, regulations, and policies.

Subrecipients proposing projects with the potential to impact the environment or cultural resources, such as the modification or renovation of existing buildings, structures, and facilities, and/or new construction and/or replacement of buildings, structures, and facilities, must participate in the FEMA EHP review process. This includes conducting early engagement to help identify EHP resources, such as threatened or endangered species, historic properties, or communities with environmental concerns; submitting a detailed project description with supporting documentation to determine whether the proposed project has the potential to impact EHP resources; and, identifying mitigation measures and/or alternative courses of action that may lessen impacts to those resources.

FEMA is sometimes 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 impacts to EHP resources and bring the project into EHP compliance.

EHP Guidance is found at Environmental Planning and Historic Preservation. The site contains links to documents 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 grants, must comply with National Flood Insurance Program (NFIP) criteria or any more restrictive federal, state, or local floodplain management standards or building code (44 C.F.R. section 9.11(d)(6)). For actions located within or that may affect a floodplain or wetland, the following alternatives must be considered: a) no action; b) alternative locations; and c) alternative actions,

including alternative actions that use natural features or nature-based solutions. Where possible, natural features and nature-based solutions shall be used. If not practicable as an alternative on their own, natural features and nature-based solutions may be incorporated into actions and minimization measures.

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.

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:

Sue Ann Surface
Grants Specialist
(573) 751-5951
Sueann.Surface@dps.mo.gov

Joanne Talleur
Lead Grants Specialist
(573) 522-2851
Joanne.Talleur@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
Grant Support Specialist
(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 SLT 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 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 and those most likely to be exploited.	Organization has a plan to manage vulnerabilities based on those with the highest criticality, internet-facing vulnerabilities, 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