FY 2022 State Homeland Security Program (SHSP)
Enhancing Cybersecurity Local Preparedness (ECSLP)
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:

97.067

Funding Opportunity Title

FY 2022 State Homeland Security Program – Enhancing Cybersecurity Local Preparedness (ECSLP)

Introduction

The Missouri Office of Homeland Security is pleased to announce the funding opportunity for the FY 2022 State Homeland Security Program (SHSP), Enhancing Cybersecurity Local Preparedness (ECSLP). This state administered, but federally funded program, is made available through the Grants Programs Directorate (GPD) and National Preparedness Directorate (NPD) within the Federal Emergency Management Agency (FEMA).

Program Description

SHSP ECSLP assists state and local efforts to build, sustain, and deliver the capabilities necessary to prevent, prepare for, protect against, and respond to, acts of terrorism in cybersecurity through projects that strengthen local cybersecurity preparedness by focusing on cybersecurity measures to help manage local risk and enhance Missouri's cybersecurity posture. These projects must close gaps and strengthen capabilities identified in an agencies' Nationwide Cybersecurity Review (NCSR) or other cybersecurity risk assessment.

Objective

The objective of the FY 2022 SHSP is to fund state and local efforts to prevent terrorism and prepare the Nation for threats and hazards that pose the greatest risk to the security of the United States.

Priorities

Given the evolving threat landscape, it is incumbent upon DHS/FEMA/OHS to continuously evaluate the national risk profile and set priorities that help ensure appropriate allocation of scarce security dollars. In assessing the national risk profile for FY 2022, six priority areas attract the most concern. The following are the six priority areas for FY 2022:

1. Enhancing the protection of soft targets/crowded places;
2. Enhancing information and intelligence sharing
3. Combating domestic violent extremism
4. **Enhancing cybersecurity**
5. Enhancing community preparedness and resilience
6. Enhancing election security

This grant program focuses only on the national priority of enhancing cybersecurity and must align to one of the Core Capabilities listed below.

- Cybersecurity
- Intelligence and information sharing
- Planning
- Public information and warning
- Operational coordination
- Screening, search, and detection
- Access control and identity verification
- Supply chain integrity and security
- Risk management for protection programs and activities
- Long-term vulnerability reduction
- Situational assessment
- Infrastructure systems
- Operational communications

DHS/FEMA/OHS strongly encourages SHSP subrecipients to participate in the THIRA (Threat and Hazard Identification and Risk Assessment)/SPR (Stakeholder Participation Report) process and prioritize grant funding to support closing capability gaps or sustaining capabilities that address national priorities and/or support enduring needs.

Period of Performance: 24 months

Projected Period of Performance Start Date: September 1, 2022

Projected Period of Performance End Date: August 31, 2024

Funding Instrument: Grant

Allowable Amount: $5,000.00 minimum award; $15,000 maximum award

Eligible Applicants:

The following Missouri entities are eligible to apply for the FY 2022 SHSP ECSLP funding opportunity:

- Local units of government
- Nongovernmental organizations, quasi-governmental organizations, and nonprofit organizations

Ineligible Applicants

- Entities located within the geographical boundaries of the St. Louis Urban Area Security Initiative (UASI), which includes the Missouri Counties of Franklin, Jefferson, St. Charles, St. Louis and St. Louis City are **NOT** eligible applicants.

- Entities located within the geographical boundaries of the Kansas City Urban Area Security Initiative (UASI), which includes the Missouri counties of Jackson, Cass, Platte, Clay, and Ray are **NOT** eligible applicants.

- State Agencies are **NOT** eligible applicants.

Other Eligibility Criteria

National Incident Management System (NIMS) Implementation

Prior to allocation of any Federal preparedness awards in FY 2022, subrecipients must ensure and maintain adoption and implementation of NIMS. The list of objectives used for progress and achievement reporting is on FEMA's website at NIMS Implementation and Training. Please see the Preparedness Grants Manual for more information on NIMS.

Emergency Management Assistance Compact (EMAC) Membership

In support of the National Preparedness Goal (the Goal), SHSP subrecipients must belong to, be in, or act as a temporary member of EMAC, except for American Samoa and the Commonwealth of the Northern Mariana Islands, which are not required to belong to EMAC at this time. All assets supported in part or entirely with FY 2022 HSGP funding must be readily deployable and NIMS-typed when possible to support emergency or disaster operations per existing EMAC agreements. In addition, funding may be used for the sustainment of core capabilities that, while they may not be physically deployable, support national response capabilities as defined under the Mitigation Mission Area of the Goal, and fusion centers.

Application and Submission Information

1. **Key Dates and Times**

    a. **Application Start Date:** August 25, 2022

b. Application Submission Deadline: September 15, 2022, 5:00 pm CST

c. 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.

As part of the FY 2022 SHSP ECSLP application, each eligible applicant must complete all application forms and provide all required documents:

1. **Contact Information Form**

2. **SHSP Project Package**

3. **Budget**

4. **Named Attachments**
   a. **Audit/Financial Statement (REQUIRED)**
   b. **Federal Fund Schedule (REQUIRED, if not included in Audit)**
   c. **Quote or Cost Basis**
   d. **Other Supporting Documentation**

Each application must only include one project, and all requested funding in the application must be directly associated to that specific project.

SHSP Funding Guidelines

Subrecipients must comply with all the requirements in 2 C.F.R. Part 200 (*Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards*). Funding guidelines established within this section support the five mission areas—Prevention, Protection, Mitigation, Response, and Recovery—and associated core capabilities within the Goal. Allowable projects made in support of the Enhancing cybersecurity national priority, must have a nexus to terrorism preparedness and fall into the categories of planning, organization, exercises, training, or equipment aligned to closing capability gaps or sustaining capabilities identified in the State THIRA/SPR.

Multiple Purpose or Dual-Use of Funds

For SHSP, many activities that support the achievement of core capabilities related to the national priorities and terrorism preparedness may simultaneously support enhanced preparedness for other hazards unrelated to acts of terrorism. However, all SHSP funded projects must assist subrecipients in achieving core capabilities related to preventing, preparing for,

protecting against, or responding to acts of terrorism per section 2008(c) of the *Homeland Security Act of 2002* [6 U.S.C. § 609(c)].

Funding Restrictions and Allowable Costs:

All costs charged to awards covered by this NOFO must comply with the Uniform Administrative Requirements, Cost Principles, and Audit Requirements at 2 C.F.R. Part 200, unless otherwise indicated in the NOFO, the terms and conditions of the award, or the Preparedness Grants Manual. This includes that costs, among other requirements, must be incurred, and products and services must be delivered, within the period of performance of the award. *See* 2 C.F.R. § 200.403(h) (referring to budget periods, which for FEMA awards under this program is the same as the period of performance).

Federal funds made available through this award may be used for the purpose set forth in this NOFO, the Preparedness Grants Manual, and the terms and conditions of the award and must be consistent with the statutory authority for the award. Award funds may not be used for matching funds for any other federal awards, lobbying, or intervention in federal regulatory or adjudicatory proceedings. In addition, federal funds may not be used to sue the Federal Government or any other government entity. See the Preparedness Grants Manual for more information on funding restrictions and allowable costs.

1. **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 for 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).

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

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. § 200.471.

2. Allowable Costs

This grant only allows for projects that strengthen local cybersecurity preparedness by focusing on cybersecurity measures to help manage local risk and enhance Missouri's cybersecurity posture. The requested project must close gaps and strengthen capabilities

identified in an agencies' Nationwide Cybersecurity Review (NCSR) or other cybersecurity risk assessment. **The applicant will be required to attest in the application, the requested project works to close gaps and strengthen capabilities identified in their agencies' NCSR or other cybersecurity risk assessment. The NCSR or other cybersecurity risk assessment is subject to review by the Missouri Office of Homeland Security (OHS).**

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.

The 21 allowable prevention, protection, mitigation, response, and recovery equipment categories for HSGP are listed on the Authorized Equipment List (AEL). Some equipment items require prior approval from DHS/FEMA/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.

Unless otherwise stated, all equipment must meet all mandatory regulatory and/or DHS/FEMA/OHS-adopted standards to be eligible for purchase using these funds. In addition, subrecipients will be responsible for obtaining and maintaining all necessary certifications and licenses for the requested equipment.

28 C.F.R. Part 23 Guidance

DHS/FEMA/OHS requires that any information technology system funded or supported by these funds comply with 28 C.F.R. Part 23, Criminal Intelligence Systems Operating Policies if this regulation is determined to be applicable. Additionally, please see 28 C.F.R. Part 23 requirements that pertain to fusion centers at https://www.dhs.gov/homeland-security-grant-program-hsgp.

Unallowable Costs

- Per FEMA policy, the purchase of weapons and weapon accessories, including ammunition, is not allowed with HSGP funds.
- Grant funds may not be used for the purchase of equipment not approved by DHS/FEMA/OHS. Grant funds must comply with IB 426 and may not be used for the purchase of the following equipment: firearms; ammunition; grenade launchers; bayonets; or weaponized aircraft, vessels, or vehicles of any kind with weapons installed.
- Unauthorized exercise-related costs include:
    - Reimbursement for the maintenance or wear and tear costs of general use vehicles (e.g., construction vehicles), medical supplies, and emergency response apparatus (e.g., fire trucks, ambulances).
    - Equipment that is purchased for permanent installation and/or use, beyond the scope of the conclusion of the exercise (e.g., electronic messaging sign).

Administrative and National Policy Requirements

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

In addition to the information regarding DHS Standard Terms and Conditions and Ensuring the Protection of Civil Rights, see the Preparedness Grants Manual for additional information on administrative and national policy requirements including the following:

- Environmental Planning and Historic Preservation (EHP) Compliance
- FirstNet
- National Incident Management System (NIMS) Implementation
- SAFECOM Guidance on Emergency Communications Grants

DHS Standard Terms and Conditions

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

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.

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.

Contact Information:

Additional information and resources can be located on the Missouri Department of Public (DPS) Safety, Office of Homeland Security (OHS) website

WebGrants System, application submission site

Missouri Office of Homeland Security Staff

Debbie Musselman
Grants Specialist
(573) 751-5997
Debbie.Musselman@dps.mo.gov

Maggie Glick
Grants Specialist
(573) 522-6125
Maggie.Glick@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