



FY 2025 State Homeland Security Program (SHSP)

Regionalization

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

State Homeland Security Program (SHSP) Regionalization

Introduction

The Missouri Department of Public Safety (DPS)/Office of Homeland Security (OHS) is pleased to announce the funding opportunity for the FY 2025 State Homeland Security Program (SHSP) Regionalization. This state administered, but federally funded program, is made available through the Grants Programs Directorate (GPD) within the Federal Emergency Management Agency (FEMA).

Program Description

SHSP is designed to enhance the capabilities of state and local governments as well as nonprofits in preventing, protecting against, and responding to terrorist attacks. This program is a part of a comprehensive set of measures authorized by Congress and implemented by the Department of Homeland Security (DHS) to strengthen the nation's communities against potential terrorist threats.

SHSP aims to strengthen the nation's ability to prevent, prepare for, protect against, and respond to acts of terrorism and other threats.

Since its inception in 2003, SHSP has significantly enhanced the nation's preparedness. SHSP addresses evolving threats such as cybersecurity vulnerabilities and the protection of soft targets and crowded places. It represents a comprehensive approach to national security, fostering collaboration across all levels of government and within communities to build a safer, more resilient nation. Through, planning, training, equipment procurement, and exercises, the program ensures jurisdictions are prepared for a wide range of risks.

In recent years:

- Funding priorities have evolved to include cybersecurity, election security, and countering emerging national security threats.
- Key accomplishments include the development of interoperable communication systems, emergency response training, and investment in physical and cybersecurity measures.
- The program emphasizes strategic investments to address identified capability gaps, requiring alignment with Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR).

This support equips various jurisdictions with the necessary tools and resources to effectively manage and mitigate a wide range of threats and hazards, aligning with FEMA’s goal of building a secure and resilient nation.

Goals and Objectives

The SHSP aims to strengthen the ability of states to prevent, prepare for, protect against, and respond to acts of terrorism and other hazards. The goal of SHSP is to support state and local governments in building, enhancing, and sustaining the capabilities needed to prevent, prepare for, protect against, and respond to acts of terrorism. SHSP funding is intended to help state and local agencies address capability gaps identified through the Threat and Hazard Identification and Risk Assessment (THIRA)/Stakeholder Preparedness Review (SPR) process, as well as prioritize resources toward high-impact security focus areas, known as National Priority Areas (NPAs).

SHSP provides resources that support state and local governments in meeting the following objectives:

- Build and sustain core capabilities, including Law Enforcement Terrorism Prevention Activities (LETPA) and the NPAs
- Address capability gaps identified in their THIRA/SPR process
- Implement a comprehensive and coordinated approach to address enduring security needs of communities that includes planning, training and awareness campaigns, equipment and capital projects, and exercises

Priorities

SHSP supports the development and sustainment of core capabilities essential to achieving the National Preparedness Goal (NPG): “A secure and resilient Nation.” To ensure strategic focus, DHS has identified five NPAs that reflect the evolving risk landscape and national policy objectives. These priorities serve as a framework for targeting investments that build capacity, reduce risk, and promote cross-sector coordination. The FY 2025 NPAs are:

1. Enhancing the protection of soft targets/crowded places
2. Supporting Homeland Security Task Forces and fusion centers
3. Enhancing and integrating cybersecurity resiliency
4. Enhancing election security
5. Supporting Border Crisis Response and Enforcement

These NPAs are rooted in the core mission areas of the NPG – prevention, protection, mitigation, and response, and reflect a whole-of-government approach to homeland security.

There are several enduring security needs that crosscut the homeland security enterprise to which subrecipients should consider allocating funding across core capability gaps and national priorities. The following are enduring needs that help subrecipients implement a comprehensive approach to securing communities:

1. Effective planning
2. Training and awareness campaigns
3. Equipment and capital projects
4. Exercises

The table below provides a breakdown of the FY 2025 SHSP priorities, showing the core capabilities enhanced and lifelines supported, as well as examples of eligible project types for each area. More information on allowable investments for each project type is included in the [Preparedness Grants Manual](#).

DHS/FEMA expects that national priorities will continue to be included in future years, evolving as threats change and capability gaps are addressed. Applicants are strongly encouraged to start planning now to sustain existing capabilities using funding sources other than DHS preparedness grants.

Projects listed in the table below may be useful in preparing for disasters unrelated to terrorism, as long as they also support the primary goals of preventing, preparing for, protecting against, or responding to acts of terrorism.

FY 2025 SHSP Priority Areas

National Priorities		
Priority Areas	Core Capabilities	Example Project Types
Enhancing the Protection of Soft Targets/Crowded Places	<ul style="list-style-type: none"> • Operational coordination • Public information and warning • Intelligence and information sharing • Interdiction and disruption • Screening, search, and detection • Access control and identify verification • Physical protective measures • Risk management for protection programs and activities 	<ul style="list-style-type: none"> • Operational overtime • Physical security enhancements <ul style="list-style-type: none"> ○ Security cameras (closed-circuit television [CCTV]) ○ Security screening equipment for people and baggage ○ Lighting ○ Access controls ○ Fencing, gates, barriers, etc. ○ UAS and detection technologies
Enhancing Cybersecurity	<ul style="list-style-type: none"> • Cybersecurity • Intelligence and information sharing • Planning • Public information and warning • Operational coordination • Screening, search, and detection 	<ul style="list-style-type: none"> • Cybersecurity risk assessments • Migrating online services to the “.gov” internet domain • Projects that address vulnerabilities identified in cybersecurity risk assessments <ul style="list-style-type: none"> ○ Improving cybersecurity of critical infrastructure to meet minimum levels identified by the Cybersecurity and Infrastructure Security Agency and the National Institute of Standards and

	<ul style="list-style-type: none"> • Access control and identify verification • Supply chain integrity and security • Risk management for protection programs and activities • Long-term vulnerability reduction • Situational assessment • Infrastructure systems • Operational communications 	<p>Technology Cybersecurity Framework (Version 1.1)</p> <ul style="list-style-type: none"> ○ Adoption of cybersecurity performance goals (CISA’s Cross-Sector Cybersecurity Performance Goals) • Cybersecurity training, planning, and exercises
Supporting Homeland Security Task Forces and Fusion Centers	<ul style="list-style-type: none"> • Intelligence and information sharing • Interdiction and disruption • Public information and warning • Operational coordination • Risk management for protection programs and activities 	<ul style="list-style-type: none"> • Establishing or enhancing multi-agency Homeland Security Task Forces (HSTFs), including operational coordination centers • Enhancing capabilities and integration with local fusion centers • Procurement of technology or equipment to support surveillance, communications, and data analysis • Development of standard operating procedures for information sharing, joint operations, and immigration enforcement coordination • Personnel training, credentialing, and certification to improve interoperability and mission alignment • Intelligence analysis, reporting, and suspicious activity monitoring • Exercises and simulations focused on joint operations, intelligence sharing, or interdiction/disruption of criminal or smuggling networks • Community engagement efforts to foster trust and encourage threat reporting • Information sharing with all DHS components; fusion centers; other operational investigative, and analytic entities; and other federal law enforcement and intelligence entities • Cooperation with DHS and other entities in intelligence, threat recognition, assessment, analysis, and mitigation • Identification, assessment, and reporting of threats of violence • Intelligence analysis training, planning, and exercises • Coordinating the intake, triage, analysis, and reporting of tips/leads and suspicious activity, to include coordination with the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI)
Enhancing Election Security	<ul style="list-style-type: none"> • Cybersecurity • Intelligence and information sharing • Planning • Long-term vulnerability reduction • Situational assessment • Infrastructure systems 	<ul style="list-style-type: none"> • Prioritize compliance with the VVSG 2.0 established by the U.S. Election Assistance Commission • Complete testing through a VSTL accredited by the U.S. Election Assistance Commission • Physical security planning and exercise support • Physical/site security measures – e.g., locks, shatter proof glass, alarms, access controls, etc. • General election security navigator support

	<ul style="list-style-type: none"> Operational coordination Community resilience 	<ul style="list-style-type: none"> Cybersecurity risk assessments, training, and planning Projects that address vulnerabilities identified in cybersecurity risk assessments Iterative backups, encrypted backups, network segmentation, software to monitor/scan, and endpoint protection Distributed Denial of Service protection Migrating online services to the “.gov” internet domain Online harassment and targeting prevention services Public awareness/preparedness campaigns discussing election security and integrity measures Long-term vulnerability reduction and community resilience
Supporting Border Crisis Response and Enforcement	<ul style="list-style-type: none"> Community resilience Operational coordination Risk management for protection programs and activities 	<ul style="list-style-type: none"> Staffing support to expand 287(g) screening operations within correctional facilities Operational overtime costs directly tied to 287(g) screening, processing, and enforcement activities Training programs for state and local law enforcement officers in immigration law, civil rights protections, and 287(g) procedures Development or enhancement of information-sharing platforms between ICE and local agencies Procurement of screening, detection, and communications technology to support immigration enforcement activities Establishing secure and dedicated communication networks with ICE Field Offices Conducting joint training exercises with ICE and local law enforcement to test operational coordination Support for facilities upgrades, such as creating dedicated interview rooms and secure processing spaces Community engagement and public briefings to promote transparency and understanding of 287(g) operations and protections
Enduring Needs		
Priority Areas	Core Capabilities	Example Project Types
Planning	<ul style="list-style-type: none"> Planning Risk management for protection programs and activities Risk and disaster resilience assessment Threats and hazards identification Operational coordination Community resilience 	<ul style="list-style-type: none"> Development of: <ul style="list-style-type: none"> Security Risk Management Plans Threat Mitigation Plans Continuity of Operations Plans Response Plans Vulnerability Assessments Efforts to strengthen governance integration between/among regional partners Joint training and planning with DHS officials and other entities designated by DHS Cybersecurity training and planning
Training & Awareness	<ul style="list-style-type: none"> Long-term vulnerability reduction Public information and warning Operational coordination Situational assessment 	<ul style="list-style-type: none"> Active shooter training Intelligence analyst training SAR and terrorism indicators/behaviors training Security training for employees Public awareness/preparedness campaigns Cybersecurity training and planning

	<ul style="list-style-type: none"> • Community resilience 	<ul style="list-style-type: none"> • Sharing and leveraging intelligence and information
Equipment & Capital Projects	<ul style="list-style-type: none"> • Long-term vulnerability reduction • Infrastructure systems • Operational communications • Interdiction and disruption • Screening, search and detection • Access control and identity verification • Physical protective measures 	<ul style="list-style-type: none"> • Protection of high-risk, high-consequence areas or systems that have been identified through risk assessments • Physical security enhancements <ul style="list-style-type: none"> ○ Security cameras (CCTV) ○ Security screening equipment for people and baggage ○ Lighting ○ Access Controls <ul style="list-style-type: none"> ▪ Fencing, gates, barriers, etc. • Enhancing Weapons of Mass Destruction (WMD) and/or improvised explosive device (IED) prevention, detection, and response capabilities <ul style="list-style-type: none"> ○ Chemical/Biological/Radiological/Nuclear/Explosive detection, prevention, and response equipment
Exercise	<ul style="list-style-type: none"> • Long-term vulnerability reduction • Operational coordination • Operational communications • Community resilience 	<ul style="list-style-type: none"> • Response exercises, including exercise planning with community-based organizations

All SHSP projects must have a demonstrated nexus to achieving target capabilities relating to preventing, preparing for, protecting against, and responding to acts of terrorism. At the same time, these projects can also help improve preparedness for other types of disasters.

DHS/FEMA//DPS/OHS also encourages SHSP subrecipients to participate in the THIRA/SPR process and prioritize grant funding to building capability and/or closing capability gaps or sustaining capabilities that address national priorities and/or support enduring needs. **In FY 2025 SHSP project applications that align to National Priorities will receive extra points during the application scoring process.**

Period of Performance: 24 months

Projected Period of Performance Start Date: September 1, 2025

Projected Period of Performance End Date: August 31, 2027

Funding Instrument: Grant

Eligible Applicants:

- Local units of government
- State units of government
- Nongovernmental organizations, quasi-governmental organizations (e.g., RPC’s and COG’s), nonprofit organizations (e.g., Red Cross)

Applicants must designate their respective geographic area (Region A thru I) in the WebGrants System, the Missouri Department of Public Safety’s online electronic portal. For additional information regarding geographic areas, applicants are encouraged to contact the Regional Planning Commission

(RPC)/Councils of Government (COG) that provides administrative support for their specific region. A regional map and direct links to the RPC/COG information are available at <http://www.dps.mo.gov/dir/programs/ohs/regionalization/?h=0> or by contacting the Missouri Department of Public Safety (DPS)/Office of Homeland Security (OHS) at (573) 522-6125.

Applicants that intend to apply for Law Enforcement Terrorism Prevention Activities (LETPA) funding must first apply for the requested project through their respective Regional Homeland Security Oversight Committee (RHSOC) to be eligible for LETPA funding. If the project is not recommended for funding or only partially funded by the RHSOC, the application will automatically be considered for LETPA funding. *State units of government are exempt from this requirement.*

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 unless the grant allows funds to be utilized to assist the agency to become compliant.

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.

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. For information regarding the application process in these counties, please contact the East-West Gateway Council of Governments <https://www.ewgateway.org> or (314) 421-4220.

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. For information regarding the application process in these counties, please contact Mid-America Regional Council (MARC) at <http://www.marc.org> or (816) 474-4240.

Other Eligibility Criteria:

National Incident Management System (NIMS) Implementation

Prior to allocation of any federal preparedness awards, subrecipients must ensure and maintain adoption and implementation of NIMS, including implementation of important operational systems defined under NIMS, such as the Incident Command System (ICS). The list of objectives used for progress and achievement reporting is on FEMA's website at <https://www.fema.gov/emergency-managers/nims/implementation-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 the EMAC. All assets supported in part or entirely with FY 2025 SHSP 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, such as Geographic/Geospatial Information Systems (GIS), interoperable communications systems, 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 7, 2025

b. Application Submission Deadline: August 22, 2025, 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 located at: <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 Homeland Security Program (SHSP) Regionalization:
<https://dps.mo.gov/dir/programs/ohs/grantstraining/>.

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

1. Contact Information Form

2. DPS Grants State Requirements

3. **Interoperable Communications Form**
4. **SHSP Project Package**
5. **Budget**
6. **Named Attachments**
 - a. **Audit/Financial Statement (REQUIRED)**
 - b. **Quote or Cost Basis**
 - c. **Other Supporting Documentation (up to 5 attachments)**

Each application must only include one project, and all requested funding in the application must be directly associated to that specific project. **Applications should NOT include both sustainment and build/enhance projects. If your project involves both sustaining an existing capability and building/enhancing a capability, you MUST submit two separate applications, one for the sustainment project, and one for the build/enhance 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 four of the five mission areas—Prevention, Protection, Mitigation, and Response—and associated core capabilities within the Goal. While Recovery is part of the Goal, it is not explicitly part of the SHSP. Allowable investments made in support of national priorities, as well as other capability-enhancing projects must have a nexus to terrorism preparedness and fall into the categories of planning, organization, exercises, training, or equipment, aligned to building capability, closing capability gaps, and/or sustaining capabilities as defined by CPG 201: THIRA/SPR Guide – 3rd Edition ([Comprehensive Preparedness Guide \(CPG\) 201, 3rd Edition](#)). Requested projects must support a deployable/shareable resource or be a regional asset. A deployable resource is an asset that is physically mobile and can be used anywhere in the United States and territories via Emergency Management Assistance Compacts or other mutual aid/assistance agreements. Shareable resources are those that can be utilized as a local, state, regional, or national capability, but is not physically deployable.

Multiple Purpose or Dual-Use of Funds

Please see the [Preparedness Grants Manual](#) for information on multiple purpose or dual-use of funds under SHSP.

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, the [Preparedness Grants Manual](#), 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:

- Matching or cost sharing requirements for other federal grants and cooperative agreements (see 2 C.F.R. § 200.306).

- Lobbying or other prohibited activities under 18 U.S.C. § 1913 or 2 C.F.R. § 200.450.
- Prosecuting claims against the federal government or any other government entity (see 2 C.F.R. § 200.435).

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

Please see the [Preparedness Grants Manual](#) for information on prohibitions on expending funds on covered telecommunications and surveillance equipment and services.

Allowable Costs

1. Planning

SHSP funds may be used for a range of emergency preparedness and management planning activities such as those associated with the development, review, and revision of the THIRA, SPR, continuity plans, and other planning activities that support the Goal and placing an emphasis on updating and maintaining a current Emergency Operations Plan (EOP) that conforms to the guidelines outlined in [Comprehensive Preparedness Guide \(CPG\) 101 v3](#). Planning efforts can also include conducting risk and resilience assessments on increasingly connected cyber and physical systems, on which security depends, using the [Infrastructure Resilience Planning Framework](#) and related Cybersecurity and Infrastructure Security Agency (CISA) resources.

2. Organization

Organization costs are allowed under this program only as described in this funding notice and the [Preparedness Grants Manual](#).

Applicants must justify proposed expenditures of SHSP funds to support organization activities within their application submission. Organizational activities include:

- Program management
- Development of whole community partnerships, through groups such as Citizen Corp Councils
- Structures and mechanisms for information sharing between the public and private sector
- Implementing models, programs, and workforce enhancement initiatives to address ideologically inspired radicalization to violence in the homeland
- Tools, resources, and activities that facilitate shared situational awareness between the public and private sectors
- Operational Support
- Utilization of standardized resource management concepts such as typing, inventorying, organizing, and tracking to facilitate the dispatch, deployment, and recovery of resources before, during, and after an incident
- Responding to an increase in the threat level under the National Terrorism Advisory System (NTAS) or needs resulting from a National Special Security Event
- Paying salaries and benefits for personnel to serve as qualified Intelligence Analysts. Per the *Personnel Reimbursement for Intelligence Cooperation and Enhancement of Homeland Security Act (PRICE Act)*, Pub. L. No. 110-412, § 2, codified in relevant part, as amended, at 6 U.S.C. § 609(a), SHSP funds may be used to hire new staff and/or contractor positions to serve as intelligence analysts to enable information/intelligence sharing capabilities, as well as support

existing intelligence analysts previously covered by SHSP funding. *See* 6 U.S.C. § 609(a). To be hired as an intelligence analyst, staff and/or contractor personnel must meet at least one of the following criteria:

- Complete training to ensure baseline proficiency in intelligence analysis and production within six months of being hired; and/or,
- Previously served as an intelligence analyst for a minimum of two years either in a federal intelligence agency, the military, or state and/or local law enforcement intelligence unit.
- All fusion center analytical personnel must demonstrate qualifications that meet or exceed competencies identified in the Common Competencies for state, local, and tribal intelligence analysts, which outlines the minimum categories of training needed for intelligence analysts. A certificate of completion of such training must be on file with the DPS/OHS and must be made available to the recipient's respective FEMA HQ Program Analyst upon request.
- Migrating online services to the ".gov" internet domain.

3. Equipment

Equipment costs are allowed under this program only as described in this funding notice and the [Preparedness Grants Manual](#).

The 21 allowable prevention, protection, mitigation, and response equipment categories for SHSP are listed on the [Authorized Equipment List](#) (AEL). Some equipment items require prior approval from FEMA/DPS/OHS before obligation or purchase of the items. Please reference the grant notes for each equipment item to ensure prior approval is not required or to ensure prior approval is obtained if necessary.

Unless otherwise stated, all equipment must meet all mandatory regulatory and/or FEMA/DPS/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. Investments in emergency communications systems and equipment must meet applicable [SAFECOM Guidance on Emergency Communications Grants \(SAFECOM Guidance\) recommendations](#). Such investments must be coordinated with the SWIC and the State Interoperability Governing Body (SIGB) to ensure interoperability and long-term compatibility. For personal protective equipment (PPE), subrecipients are encouraged to give procurement preference to domestic manufacturers of PPE or PPE raw materials to the maximum practicable and allowed by law.

Some allowable equipment items have specific requirements to be eligible for funding. Those with specific requirements are listed below. **Please note, the items listed below are not the only eligible equipment items.**

- Interoperability Equipment (Portables/Handhelds, Mobiles, Repeaters, Base Stations, etc.)

All interoperable communications equipment must meet the Missouri Department of Public Safety, Office of the Director, DPS Grants [Radio Interoperability Guidelines](#). The Missouri Interoperability Center (MIC) will review all communications equipment applications to ensure they comply with the [Radio Interoperability Guidelines](#). **Quotes that are compliant with the Radio Interoperability Guidelines MUST be submitted in the Named Attachments component of the application. Applications that do not meet these guidelines will not be eligible for funding.**

NOTE: Agencies seeking any type of radio or radio-related accessory are encouraged to contact the Missouri Interoperability Center by phone at (573) 522-1714 or by email at moswin.sysadmin@dps.mo.gov to ensure compliance with the Radio Interoperability Guidelines and the appropriate communication devices are purchased for the department's needs. The Missouri Interoperability Center staff can also provide helpful information regarding the department's ability to access the MOSWIN and how to articulate such within the grant application.

- Mobile Data Terminals (MDTs) / Mobile Data Computers (MDCs) Requirements

Agencies seeking funding for mobile data terminals should research the type of computer being requested. The Missouri Department of Public Safety is aware that non-ruggedized laptops and tablets are typically not durable enough for road patrol purposes and therefore not the best use of funds.

- Body-Worn Cameras

Agencies seeking funding for Body-Worn Cameras (BWCs) must have policies and procedures in place related to equipment usage, data storage and access, privacy considerations, and training. Subrecipients of funding for Body-Worn Cameras must supply the Missouri Department of Public Safety with a copy of such policy(s) and procedure(s) at the time of claim submission.

- Body Armor

Funds may be used to purchase body armor at any threat level designation, make, or model from any distributor or manufacturer, as long as the body armor has been tested and found to comply with the latest applicable National Institute of Justice (NIJ) ballistic or stab standards, which can be found online at <https://www.nij.gov/topics/technology/body-armor/Pages/standards.aspx>.

Body armor or armor vests must also be “uniquely fitted vests” which means protective (ballistic or stab-resistant) armor vests that conform to the individual wearer to provide the best possible fit and coverage, through a combination of:

- (1) Correctly sized panels and carrier, determined through appropriate measurement and
- (2) Properly adjusted straps, harnesses, fasteners, flaps, or other adjustable features.

The requirement that body armor be “uniquely fitted” does not require body armor that is individually manufactured based on the measurements of an individual wearer.

In addition, body armor purchased must be made in the United States.

Agencies seeking funding for body armor are required to have a written “mandatory wear” policy in effect. There are no requirements regarding the nature of the policy other than it being a mandatory wear policy for all uniformed officers while on duty. Subrecipients of funding for body armor must supply the Missouri Department of Public Safety with a copy of such policy at the time of claim submission.

- License Plate Readers

Agencies purchasing license plate reader (LPR) equipment and technology with grant funds administered by the Missouri Department of Public Safety, must adhere to the following requirements:

- a. LPR vendors chosen by an agency must have an MOU on file with the MSHP Central Vendor File as developed and prescribed by the Missouri Department of Public Safety pursuant to 11 CSR 30-17
- b. Prior to purchasing LPR services, the agency should verify the vendor's MOU status with the MSHP CJIS Division by emailing mshphelpdesk@mshp.dps.mo.gov
- c. Share LPR data through the MoDEx process with statewide sharing platforms (i.e., MULES)
- d. Enable LPR data sharing with other Missouri Law Enforcement agencies and enforcement support entities within the selected vendor's software. Examples include, but are not limited to fusion centers, drug task forces, special investigations units, etc.
- e. Connect to the Missouri State Highway Patrol's Automated License Plate Reader (ALPR) File Transfer Protocol Access Program. This program provides the information necessary to provide a NCIC and/or MULES hit when used in conjunction with a License Plate Reader (LPR) device. An MOU must be on file with the Access Integrity Unit (AIU) for the vendor and the law enforcement agency and a registration process must be completed
- f. Agency shall have a license plate reader policy and operation guideline prior to the implementation of LPRs. Reimbursements will not be made on the project until the policy has been provided to the Missouri Department of Public Safety
- g. If LPR will be installed on Missouri Department of Transportation right-of-way(s) agency must request installation through the Missouri Department of Public Safety. Once approved, agency must adhere to the Missouri Department of Transportation's guidelines regarding installation of LPR's on Missouri Department of Transportation right-of-way(s)

- Turnout Gear

Agencies seeking funding for turnout gear must have a policy to document cleaning and maintenance processes and procedures for turnout gear. Subrecipients of funding for turnout gear must supply the Missouri Department of Public Safety with a copy of such policy(s) and procedure(s) at the time of claim submission.

Small Unmanned Aircraft Systems (sUAS) and critical emergency supply costs are allowable under this program. See the [Preparedness Grants Manual](#) for more information.

General Purpose Equipment

SHSP allows expenditures on general purpose equipment if it aligns to and supports one or more core capabilities identified in the Goal and has a nexus to terrorism preparedness. General purpose equipment, like all equipment funded under the SHSP must be shareable through the EMAC and allowable under 6 U.S.C. § 609, and any other applicable provision of the Homeland Security Act of 2002, as amended. Examples of such general-purpose equipment may include:

- Emergency medical services (EMS) equipment and vehicles
- Fire service equipment and vehicles, to include hose, pump accessories, and foam concentrate for specialized chemical/biological/radiological/nuclear/explosive (CBRNE) response

- Interoperability of data systems, such as computer aided dispatch (CAD) and record management systems (RMS)
- Office equipment for staff engaged in homeland security program activity

Controlled Equipment

For decades, the federal government has provided equipment to state, local, and tribal law enforcement agencies (LEAs) through federal grants. Some federal grant programs have assisted LEAs as they carry out critical missions to keep the American people safe. The equipment acquired by LEAs through these programs includes administrative equipment, such as office furniture and computers. Some federal grant programs also may include military and military-styled equipment, firearms, and tactical vehicles provided by the government, including property covered under 22 C.F.R. Part 121 and 15 C.F.R. Part 774 (collectively, “controlled equipment”).

However, not all equipment that is considered controlled equipment is allowable under the SHSP. Grant funds under this program may not be used for the purchase of equipment not approved by DHS/FEMA/DPS/OHS. For example, the purchase of tracked armored vehicles, camouflage uniforms, weapons, and weapons accessories, including ammunition, is generally not allowed with SHSP funds.

DHS/FEMA will continue to collaborate with federal agency partners to ensure that there is a consistent and reasonable approach to the restrictions placed on certain equipment expenditures while continuing to support these investments when there is a justifiable need. Further DHS/FEMA will continue to maintain an awareness of the evolving policy developments related to certain equipment expenditures and keep grant subrecipients up to date on future developments.

4. Training and Exercises

Training and exercise costs are allowed under this program as described in this funding notice and the [Preparedness Grants Manual](#). Subrecipients are encouraged to consider tuition-free courses offered by FEMA first, before investing in training. For more information and a catalog of courses please refer to the [National Preparedness Course Catalog at the National Training and Education Division \(NTED\)](#). Allowable training-related costs under SHSP include the establishment, support, conduct, and attendance of training specifically identified under the SHSP program and/or in conjunction with emergency preparedness training by other federal agencies (e.g., HHS and Department of Transportation [DOT]). Training conducted using SHSP funds should address a performance gap identified through an Integrated Preparedness Plan (IPP) or other assessments (e.g., National Emergency Communications Plan [NECP] Goal Assessments) and contribute to building a capability that will be evaluated through a formal exercise. When developing new courses, subrecipients are encouraged to apply the Analyze, Design, Develop, Implement, and Evaluate (ADDIE) model of instructional design.

5. Travel

Domestic travel costs are allowed under this program, as provided for in this NOFO. International travel is not an allowable cost under this program unless approved in advance by DHS/FEMA/DPS/OHS.

6. Maintenance and Sustainment

Maintenance and sustainment related costs are allowed under this program only as described in the [Preparedness Grants Manual](#).

Unallowable Costs

Per FEMA policy, the purchase of weapons and weapons accessories, including ammunition, is not allowed with SHSP funds. Grant funds 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).

SHSP funds may not be used to support the hiring of sworn public safety officers for the purposes of fulfilling traditional public safety duties or to supplant traditional public safety positions and responsibilities.

Administrative and National Policy Requirements

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.

In accordance with [Executive Order 14305, Restoring American Airspace Sovereignty \(June 6, 2025\)](#), and to the extent allowed by law, eligible state and local grant subrecipients under this NOFO are permitted to purchase unmanned aircraft systems, otherwise known as, drones, or equipment or services for the detection, tracking, or identification of drones and drone signals, consistent with the legal authorities of state and local agencies. Subrecipients must comply with all applicable federal, state, and local laws and regulations, and adhere to any statutory requirements on the use of federal funds for such unmanned aircraft systems, equipment, or services.

DHS Standard Terms and Conditions

A subrecipient under this funding opportunity must comply with the DHS Standard Terms and Conditions in effect of the date of the federal award. The DHS Standard Terms and Conditions are available at [DHS Standard Terms and Conditions](#).

Environmental Planning and Historic Preservation (EHP) Compliance

See the [Preparedness Grants Manual](#) for information on EHP compliance.

Contact Information:

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

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

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

Kristin Kayser
Grants Specialist
(573) 751-3438
Kristin.Kayser@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
DPS Grants Support Specialist
(573) 522-6125
Kelsey.Saunders@dps.mo.gov