FY 2023 State Homeland Security Program (SHSP)

Law Enforcement Terrorism Prevention Activities (LETPA)

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)

Assistance Listing:

97.067

Funding Opportunity Title

State Homeland Security Program Law Enforcement Terrorism Prevention Activities (LETPA)

Introduction

The Missouri Department of Public Safety (DPS) is pleased to announce the funding opportunity for the FY 2023 State Homeland Security Program (SHSP) Law Enforcement Terrorism Prevention Activities (LETPA). 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 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.

The 2022-2026 FEMA Strategic Plan outlines three goals designed to position FEMA to address the increasing range and complexity of disasters, support the diversity of communities we serve, and complement the nation's growing expectations of the emergency management community. The Homeland Security Grant Program (HSGP) supports FEMA's efforts to achieve equitable outcomes for those we serve (Goal 1) and to promote and sustain a prepared nation (Goal 3). We invite our stakeholders and partners to also adopt these priorities and join us in building a more prepared and resilient Nation.

Finally for FY 2023, DHS is focused on the criticality of information sharing and collaboration to building a national culture of preparedness and protecting against terrorism and other threats to our national security. The threats to our nation have evolved during the past two decades. We now face continuous cyber threats by sophisticated actors, threats to soft targets and crowded places, and threats from domestic violent extremists who currently pose the greatest terrorism threat to the nation. Therefore, for FY 2023, DHS has identified six priority areas related to the most serious threats to the nation.

Objective

The objective of the FY 2023 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, DHS/FEMA has evaluated the national risk profile and set priorities that help inform appropriate allocation of scarce security dollars. In assessing the national risk profile for FY 2023, six priority areas attract the most concern. The following are the six priority areas for FY 2023:

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

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

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

The table below provides a breakdown of the FY 2023 SHSP priorities, showing the core capabilities enhanced and lifelines supported, as well as examples of eligible project types for each area. A detailed description of allowable investments for each project type is included in the FY 2023 Preparedness Grants Manual. DHS/FEMA anticipates that in future years, national priorities will continue to be included and will be updated as the threats evolve and as capability gaps are closed. Applicants are strongly encouraged to begin planning to sustain existing capabilities through funding mechanisms other than DHS preparedness grants.

FY 2023 SHSP Priority Areas

Priority Areas	Core Capabilities	Lifelines	Example Project Types
National Priorities			

Enhancing cybersecurity	• 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 activities
	• Risk management for protection programs and activities
	• Long-term vulnerability reduction
	• Situational assessment
	• Infrastructure systems
	• Operational communications
		• Safety and security	• Cybersecurity risk assessments
			• Migrating online services to the ".gov" internet domain
			• Projects that address vulnerabilities identified in cybersecurity risk assessments
			  ○ Improving cybersecurity of critical infrastructure to meet minimum levels identified by the Cybersecurity and Infrastructure Agency (CISA) and the National Institute of Standards and Technology Cybersecurity Framework
			  ○ Cybersecurity training and planning

Enhancing the protection of soft targets crowded places	• Operational coordination
	• Public information and warning
	• Intelligence and information sharing
	• Interdiction and disruption
	• Screening, search, and detection
	• Access control and identity verification
	• Physical protective measures
	• Risk management for protection programs and activities
		• Safety and security	• Operational overtime
			• Physical security enhancements
			  ○ Closed-circuit television (CCRV) security cameras
			  ○ Security screening equipment for people and baggage
			  ○ Lighting
			  ○ Access controls
			  ○ Fencing, gates, barriers, etc.
			• Unmanned aircraft system detection technologies

Enhancing information and intelligence sharing and analysis	• Intelligence and information sharing • Interdiction and disruption • Planning • Public information and warning • Operational coordination	• Safety and security	• Fusion center operations • 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 officials and other entities designated by DHS in

	• Risk management for protection programs and activities		intelligence, threat recognition, assessment, analysis, and mitigation • Identification, assessment, and reporting of threats of violence • Joint intelligence analysis training and planning with DHS officials and other entities designated by DHS
Combating domestic violent extremism	• Interdiction and disruption • Intelligence and information sharing • Planning • Public information and warning • Operational coordination • Risk management for protection programs and activities	• Safety and Security	• Open-source analysis of disinformation and misinformation campaigns, targeted violence and threats to life, including tips/leads, and online/social media-based threats • Sharing and leveraging intelligence and information, including open-source analysis • Execution and management of threat assessment programs to identify, evaluate, and analyze indicators and behaviors indicative of domestic violent extremists • Training and awareness programs (e.g., through social media, suspicious activity reporting [SAR] indicators and behaviors) to help prevent radicalization • Training and awareness programs (e.g., through social media, SAR indicators and behaviors) to educate the public on misinformation and disinformation campaigns and resources to help them identify and report potential instances of domestic violent extremism
Enhancing community preparedness and resilience	• Planning • Public information and warning • Community resilience • Risk management for protection programs and activities • Mass care services • Intelligence and information sharing • Risk and disaster resilience assessment • Long-term vulnerability reduction	• Safety and security	• Establish, train, and maintain Community Emergency Response Teams (CERT) and Teen CERT, with a focus on historically underserved communities, including procurement of appropriate tools, equipment and training aides: o Local delivery of CERT train-the-trainer and CERT Program Manager to build local program training and maintenance capacity • Provide continuity training, such as FEMA's Organizations Preparing for Emergency Needs training, to faith-based organizations, local businesses, and community-based organizations such as homeless shelters, food pantries, nonprofit medical providers and senior care facilities to bolster their resilience to all hazards

			• Partner with local school districts to deliver the Student Tools for Emergency Planning curriculum or other educational programming to guide students on how to create emergency kits and family communications plans • Partner with key stakeholders to assist with completing the Emergency Financial First Aid Kit or a similar tool to bolster the disaster centric and financial resilience of individuals and households • Execute *You are the Help Until the Help Arrives* workshops in concert with community based organizations to bolster individual preparedness • Target youth preparedness using FEMA programing such as Prepare with Pedro resources and Ready2Help • Promote community planning, coordination, and integration of children's needs during emergencies through workshops like FEMA's Integrating the Needs of Children • Community Mapping: identify community resources and characteristics in order to identify gaps in resources, identify hazards and vulnerabilities, and inform action to promote resilience • Provide training and awareness programs with key stakeholders (e.g., through social media, community and civic organizations) to educate the public on misinformation and disinformation campaigns to increase individual and community resilience. • Support integrated and cross-jurisdictional preparedness planning that considers how the community develops networks of information-sharing and collaboration among community-based organizations and government institutions to enable a quicker recovery from multiple threats, including terrorist actions.
Enhancing Election Security	• Cybersecurity • Intelligence and information sharing • Planning • Long-term vulnerability reduction	• Safety and Security	• Physical security planning support • Physical/site security measures – e.g., locks, shatter proof glass, alarms, etc. • General election security navigator support • Cyber navigator support

	• Situational assessment • Infrastructure systems • Operational coordination • Community resilience		• 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.
Enduring Needs			

Planning	• Planning
	• Risk management for protection programs and activities
	• Risk and disaster resilience assessment
	• Threats and hazards identification
	• Operational coordination
	• Community resilience
		• Safety and security	• Development of:
			  ○ Security Risk Management Plans
			  ○ Threat Mitigation Plans
			  ○ Continuity of Operations Plans
			  ○ Response Plans
			• 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
			• Revision of existing plans to strengthen community resilience in underserved communities

Training & Awareness	• Long-term vulnerability reduction • Public information and warning • Operational coordination • Situational assessment • Community resilience	• Safety and security	• Active shooter training • Intelligence analyst training • SAR and terrorism indicators/behaviors training • Security training for employees • Public awareness/preparedness campaigns • Joint training and planning with DHS officials and other entities designated by DHS • Cybersecurity training and planning • Sharing and leveraging intelligence and information • Targeted outreach and preparedness training for underserved communities in conjunction with community-based organizations

Equipment & Capital Projects	• Long-term vulnerability reduction • Infrastructure systems • Operational communications • Interdiction and disruption • Screening, search and detection • Access control and identity verification • Physical protective measures	• Safety and security	• Protection of high-risk, high-consequence areas or systems that have been identified through risk assessments • Physical security enhancements o Security cameras (CCTV) o Security screening equipment for people and baggage o Lighting o Access Controls ▪ Fencing, gates, barriers, etc. • Enhancing Weapons of Mass Destruction (WMD) and/or improvised explosive device (IED) prevention, detection, response and recovery capabilities o Chemical/Biological/Radiological/ Nuclear/Explosive (CBRNE) detection, prevention, response, and recovery equipment
Exercises	• Long-term vulnerability reduction • Operational coordination • Operational communications • Community resilience	• Safety and security	• 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. However, such projects may simultaneously support enhanced preparedness for disasters unrelated to acts of terrorism.

DHS/FEMA/OHS also encourages SHSP subrecipients to participate in the THIRA/SPR process and prioritize grant funding to support closing capability gaps or sustaining capabilities that address national priorities and/or support enduring needs.

Law Enforcement Terrorism Prevention Activities (LETPA)

The FY 2023 Preparedness Grants Manual and Information Bulletin (IB) 473 include information on allowable activities for LETPA projects.

The National Prevention Framework describes those activities that should be executed upon the discovery of intelligence or information regarding an imminent threat to the homeland, to thwart an initial or follow-on terrorist attack and provides guidance to ensure the Nation is prepared to identify, prevent, avoid, or stop a threatened or actual act of terrorism. Activities outlined in the National Prevention Framework are eligible for use as LETPA-focused funds. Also, where capabilities are shared with the protection mission area, the National Protection Framework activities are also eligible. All other terrorism prevention activities proposed for funding under LETPA must be approved by the FEMA Administrator.

Period of Performance: 24 months

Projected Period of Performance Start Date: September 1, 2023

Projected Period of Performance End Date: August 31, 2025

Funding Instrument: Grant

Eligible Applicants:

The following entities are eligible to apply for FY 2023 LETPA funding:

- State Units of Government
- Local Units of Government
- Nongovernmental organizations, quasi-governmental organizations, and nonprofit organizations

APPLICANTS THAT INTEND TO APPLY FOR LETPA FUNDING MUST FIRST APPLY FOR THE REQUESTED PROJECT THROUGH THEIR RESPECTIVE REGIONAL HOMELAND SECURITY OVERSIGHT COMMITTEE (RHSOC) TO BE CONSIDERED ELIGIBLE FOR LETPA FUNDING.
State units of government are exempt from this requirement.

To be eligible for SHSP LETPA funding, the applicant agency must be compliant with the following statutes, as applicable and must maintain compliance throughout the grant period of performance:

- **Section 320.271 RSMo– Fire Department Registration**
  Pursuant to section 320.271 RSMo, All fire protection districts, fire departments, and all volunteer fire protection associations as defined in section 320.300 shall complete and file with the state fire marshal within sixty days after January 1, 2008, and annually thereafter, a fire department registration form provided by the state fire marshal.

- **Section 590.650 RSMo– Vehicle Stops Report**
  Pursuant to section 590.650.3 RSMo, (1) every law enforcement agency shall compile the data described in subsection 2 for the calendar year into a report to the attorney general and (2) each law enforcement agency shall submit the report to the attorney general no later than March first of the following calendar year.

  NOTE: It is the responsibility of the applicant to verify the submission of this report with the Attorney General's Office prior to submitting an application. Failure to submit the Racial Profiling Report will result in the automatic denial of the application. A copy of such report does not need to be submitted with the application.

- **Section 590.700 RSMo – Written Policy on Recording of Custodial Interrogations**

Pursuant to section 590.700.4 RSMo, each law enforcement agency shall adopt a written policy to record custodial interrogations of persons suspected of committing or attempting to commit felony crimes as outlined in subsection 2 of this section and shall certify adoption of such policy when applying for any grants administered by the Department of Public Safety.

NOTE: It is the responsibility of the applicant to ensure the prescribed written policy is in place prior to submitting an application.

- **Section 43.544 RSMo – Written Policy on Forwarding Intoxication-Related Traffic Offenses**
  Pursuant to section 43.544.1 RSMo, each law enforcement agency shall adopt a policy requiring arrest information for all intoxication-related traffic offenses be forwarded to the central repository as required by section 43.503 RSMo and shall certify adoption of such policy when applying for any grants administered by the Department of Public Safety.

  NOTE: It is the responsibility of the applicant to ensure the prescribed written policy is in place prior to submitting an application.

- **Section 590.1265 RSMo – Police Use of Force Transparency Act of 2021**
  Use of force incidents reporting standards and procedures, publication of report data, analysis report. Each law enforcement agency shall certify compliance with section 590.1265 RSMo when applying for any grants administered by the Department of Public Safety. *For purposes of grant eligibility, law enforcement agencies will be considered non-compliant if they have not submitted Use of Force reports for three or months in the prior twelve month period.*

- **Section 43.505 RSMo – National Incident-Based Reporting System (NIBRS)** ***formerly Uniform Crime reporting (UCR)***
  Pursuant to section 43.505 RSMo Uniform Crime Reporting system – duties of department – violations, penalty: Each law enforcement agency is required to submit crime incident reports to the department of public safety on forms or in the format prescribed by the department and submit any other crime incident information which may be required by the Department of Public Safety. ***Agencies that are not compliant at the time of application will only be eligible for grant funds 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 prior twelve month period..*

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

- **Section 590.030 RSMo – Rap Back Program Participation**
  Pursuant to section 590.030 RSMo, all law enforcement agencies shall enroll in the state and federal Rap Back programs on or before January 1, 2022 and continue to remain enrolled. The law enforcement agency shall take all necessary steps to maintain officer enrollment for all officers commissioned with that agency in the Rap Back programs. An officer shall submit to being fingerprinted at any law enforcement agency upon commissioning and for as long as the officer is commissioned with that agency. Each law enforcement agency shall certify compliance with section 590.030 RSMo when accepting any grants administered by the Department of Public Safety.

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. The list of objectives used for progress and achievement reporting is on FEMA's website at NIMS Implementation and Training.

Please see the FY 2023 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 2023 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 14, 2023

   b. Application Submission Deadline: September 8, 2023, 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.

An application workshop with instructions on how to apply through the WebGrants System will be available on the DPS website in the Grant Applications and Forms section.

As part of the FY 2023 SHSP LETPA application, each eligible applicant must complete all application forms and provide all required documents:

1. **Contact Information Form**
2. **SHSP LETPA Project Package**
3. **Interoperable Communications Form**
4. **Budget**
5. **Named Attachments**
   a. **Audit/Financial Statement (REQUIRED)**
   b. **Quote or Cost Basis**
   c. **Training Request Form**
   d. **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.

LETPA projects will only be considered allowable if they were initially applied for through the SHSP Regionalization program and meet all other LETPA criteria. ***State agency projects are exempt from this requirement.***

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 mission areas—Prevention, Protection, Mitigation, and Response—and associated core capabilities within the Goal. Allowable projects made in support of the 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 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 FY 2023 Preparedness Grants Manual. This includes, among other requirements that costs 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 FY 2023 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 FY 2023 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 on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services #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 FY 2023 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. Law Enforcement Terrorism Prevention Activities Allowable Costs

Costs across all categories of POETE (Planning, Organization, Equipment, Training, and Exercise) are allowable.

Allowable LETPA expenditures are discussed in the following documents:

- Grant Programs Directorate Information Bulletin (IB) No. 485 Fiscal Year 2023 Law Enforcement Terrorism Prevention Activity Supplemental Guidance to the Homeland Security Grant Program Notice of Funding Opportunity
- Grant Programs Directorate Information Bulletin (IB) No. 473 Supplemental Guidance for Law Enforcement Terrorism Prevention Activity Expenditures
- FY 2023 Preparedness Grants Manual (Appendix A)
- National Prevention Framework
- National Protection Framework where capabilities are shared with the protection mission area

In particular, applicants should consider investing in projects such as:

- Maturation, and enhancement of designated state and major urban area fusion centers, including information sharing and analysis, threat recognition, terrorist interdiction, and intelligence analyst training and salaries (subject to certain conditions);
- Regional counterterrorism training programs for small, medium, and large jurisdictions to exchange information and discuss the current threat environment, lessons learned, and best practices to help prevent, protect against, and mitigate acts of terrorism;
- Support for coordination of regional full-scale training exercises (federal, state, and local law enforcement participation) focused on terrorism-related events; and
- Law enforcement Chemical, Biological, Radiological, Nuclear, and high yield Explosives detection and response capabilities, such as bomb detection/disposal capability deployment, sustainment, or enhancement, including canine teams, robotics platforms, and x-ray technology.

Additional examples of allowable LETPA projects include but are not limited to:

- Coordination between fusion centers and other intelligence, operational, analytic, or investigative efforts including, but not limited to JTTFs, Field Intelligence Groups (FIGs), High-Intensity Drug Trafficking Areas (HIDTA), Regional Information Sharing Systems (RISS) Centers, criminal intelligence units, real-time crime analysis centers and DHS intelligence, operational, analytic, and investigative entities;
- Implementation and maintenance of the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI), including training for front-line personnel on identifying and reporting suspicious activities, tips/leads, and online/social media-based threats, as well as the execution and management of threat assessment programs to identify, evaluate, and analyze indicators and behaviors indicative of terrorism, targeted violence, threats to life, and other criminal activity;
- Management and operation of activities that support the execution of the intelligence process and fusion centers, including but not limited to: Fusion Liaison Officer (FLO) programs, security programs to protect the facility, personnel, and information, and the protection of privacy, civil rights, and civil liberties;
- Implementation of the "If You See Something, Say Something®" campaign to raise public awareness of indicators of terrorism and terrorism-related crime and associated efforts to increase the sharing of information with public and private sector partners, including nonprofit organizations. Note: DHS requires that all public and private sector partners wanting to implement and/or expand the DHS "If You See Something, Say Something®" campaign using grant funds work directly with the DHS Office of Partnership and Engagement (OPE) to ensure all public awareness materials (e.g., videos, posters, tri-folds, etc.) are consistent with DHS's messaging and strategy for the campaign and compliant with the initiative's trademark, which is licensed to DHS by the New York Metropolitan Transportation Authority. Coordination with OPE, through the Campaign's Office (seesay@hq.dhs.gov), must be facilitated by the FEMA HQ Preparedness Officer;
- Increase physical security, through law enforcement personnel and other protective measures, by implementing preventive and protective measures at critical infrastructure sites or at-risk nonprofit organizations;
- Building and sustaining preventive radiological and nuclear detection capabilities, including those developed through the Securing the Cities initiative;
- Integration and interoperability of systems and data, such as computer aided dispatch (CAD) and record management systems (RMS), to facilitate the collection, evaluation, and assessment of suspicious activity reports, tips/leads, and online/social media-based threats; and
- Development of countering violent extremism programs, projects, and initiatives, addressing prevention, intervention, and diversion efforts, including training on roles of law enforcement and how to effectively partner with law enforcement; developing and promoting training specifically for law enforcement executives and frontline officers on potential behaviors and indicators of violent extremism and how to appropriately analyze and report them; supporting community and law enforcement engagement strategies such as table top exercises, roundtable events, town hall meetings, and peer to peer activities; funding for existing and/or expansion of law enforcement community relations efforts, support for the development of community

engagement plans, and joint projects to increase the awareness of violent extremist threats and community mitigation solutions.

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/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/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. Such investments must be coordinated with the SWIC and the State Interoperability Governing Body (SIGB) to ensure interoperability and long-term compatibility.

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 Criminal Justice/Law Enforcement (CJ/LE) Unit, Office of Homeland Security (OHS) Radio Interoperability Guidelines. The Missouri Interoperability Center (MIC) will review all communications equipment applications to ensure they comply with the Radio Interoperability Guidelines. **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, (855) 466-7946 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).

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. As noted in Section B of FEMA Policy 207-22-0002, Prohibited or Controlled Equipment Under FEMA Awards, certain equipment is prohibited and is not allowable under SHSP. Grant funds under this program may not be used for the purchase of equipment not approved by DHS/FEMA. For example, the purchase of tracked armored vehicles, camouflage uniforms, weapons, and weapons accessories, including ammunition, is generally not allowed with SHSP funds.

For some controlled equipment that is allowable under the SHSP, additional documentation, justifications, reviews, and approvals are required, including but not limited to proof of policies and procedures to safeguard individuals' privacy, civil rights, and civil liberties.

Requirements for Small Unmanned Aircraft System

All requests to purchase Small Unmanned Aircraft Systems (sUAS) with FEMA grant funding must comply with FEMA Policy 207-22-0002, Prohibited or Controlled Equipment Under FEMA Awards, and also include a description of the policies and procedures in place to safeguard individuals' privacy, civil rights, and civil liberties of the jurisdiction that will purchase, take title to or otherwise use the sUAS equipment. sUAS policies are not required at the time of application but must be received and approved by FEMA prior to obligating SHSP funds. All grant-funded procurements must be executed in a manner compliant with federal procurement standards at 2 C.F.R. §§ 200.317 – 200.327. For subrecipients that use SHSP funds for sUAS, FEMA advises that there is a general privacy concern related to the use of the equipment if the data the devices collect is transmitted to servers not under the control of the operator. It has been reported that some manufacturers of sUAS encrypt data and send that data to servers outside the United States. The U.S. Department of Homeland Security's Privacy Office suggests the subrecipient fully explore data transmission and storage issues with vendors to reduce the possibility of data breaches.

Additionally, the Joint Explanatory Statement (JES) accompanying the FY 2023 DHS Appropriations Act further requires subrecipients to certify they have reviewed the Industry Alert on Chinese Manufactured Unmanned Aircraft Systems, and completed a risk assessment that considers the proposed use of foreign-made sUAS to ascertain potential risks (e.g., privacy, data breaches, cybersecurity, etc.) related to foreign-made versus domestic sUAS.

Acquisition and Use of Technology to Mitigate UAS (Counter-UAS)

In August 2020, FEMA was alerted of an advisory guidance document issued by DHS, the Department of Justice, the Federal Aviation Administration, and the Federal Communications Commission: Interagency Legal Advisory on UAS Detection and Mitigation Technologies. The purpose of the advisory guidance document is to help non-federal public and private entities better understand the federal laws and regulations that may apply to the use of capabilities to detect and mitigate threats posed by UAS operations (i.e., Counter-UAS or C-UAS).

The Departments and Agencies issuing the advisory guidance document, and FEMA, do not have the authority to approve non-federal public or private use of UAS detection or mitigation capabilities, nor do they conduct legal reviews of commercially available product compliance with those laws. The advisory does not address state and local laws nor potential civil liability, which UAS detection and mitigation capabilities may also implicate.

It is strongly recommended that, prior to the testing, acquisition, installation, or use of UAS detection and/or mitigation systems, entities seek the advice of counsel experienced with both federal and state criminal, surveillance, and communications laws. Entities should conduct their own legal and technical analysis of each UAS detection and/or mitigation

system and should not rely solely on vendors' representations of the systems' legality or functionality. Please also see the DHS press release on this topic for further information: Interagency Issues Advisory on Use of Technology to Detect and Mitigate Unmanned Aircraft Systems | Homeland Security (dhs.gov).

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 equipment not approved by DHS/FEMA/OHS. Grant funds must comply with FEMA Policy 207-22-0002, 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 FY 2023 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 Standards 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.

Environmental Planning and Historic Preservation (EHP) Compliance

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

In some cases, FEMA is also required to consult with other regulatory agencies and the public in order to complete the review process. Federal law required 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 incompliance with applicable EHP laws, Executive Orders, regulations, and policies.

DHS and FEMA EHP policy is found in directives and instructions available on the FEMA.gov EHP page, the FEMA website page that includes documents regarding EHP responsibilities and program requirements, including implementation of the National Environmental Policy Act and other EHP regulations and Executive Orders.

The GPD EHP screening form is located at EHP Form. Additionally, all subrecipients under this funding opportunity are required to comply with the FEMA GPD EHP Policy Guidance, FEMA Policy #108-023-1.

Contact Information:

Additional information and resources can be located on the Missouri Department of Public Safety, Office of Homeland Security website.

Applications must be submitted through the Missouri Department of Public Safety's WebGrants System.

Department of Public Safety Contacts:

Debbie Musselman
Grants Specialist
(573) 526-9203
Debbie.Musselman@dps.mo.gov

Chelsey Call
Grants Supervisor
(573) 526-9203
Chelsey.Call@dps.mo.gov

Kelsey Saunders
Grant Support Specialist
(573) 522-6125
Kelsey.Saunders@dps.mo.gov

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