FY 2022 State Homeland Security Program (SHSP)

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

Introduction

The Missouri Office of Homeland Security is pleased to announce the funding opportunity for the FY 2022 State Homeland Security Program (SHSP). 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 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 2022, 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 2022, DHS has identified six priority areas related to the most serious threats to the nation.

Objective

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

Priorities

Given the evolving threat landscape, 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 2022, six priority areas attract the most concern. The following are the six priority areas for FY 2022:

1. Enhancing the protection of soft targets/crowded places
2. Enhancing information and intelligence sharing 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 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 2022 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 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 2022 SHSP Priority Areas

Priority Areas	Core Capabilities	Lifelines	Example Project Types
National Priorities			

Enhancing cybersecurity	• Cybersecurity
	• Intelligence and information sharing
	• Planning
	• Public information 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
			  o 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
			  o 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
			  o Closed-circuit television (CCRV) security cameras
			  o Security screening equipment for people and baggage
			  o Lighting
			  o Access controls
			  o 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	• 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

	• Operational coordination • Risk management for protection programs and activities		• Cooperation with DHS officials and other entities designated by DHS in 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 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
Enhancing Election Security	• Cybersecurity • Intelligence and information sharing • Planning • Long-term vulnerability reduction • Situational assessment • Infrastructure systems	• 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 • 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
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:
			  o Security Risk Management Plans
			  o Threat Mitigation Plans
			  o Continuity of Operations Plans
			  o 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	• Safety and security	• Protection of high-risk, high-consequence areas or systems that have been identified through risk assessments

	• Operational communications
	• Interdiction and disruption
	• Screening, search and detection
	• Access control and identity verification
	• Physical protective measures
			• Physical security enhancements
			  ○ Security cameras (CCTV)
			  ○ Security screening equipment for people and baggage
			  ○ Lighting
			  ○ Access Controls
			    ▪ Fencing, gates, barriers, etc.
			• Enhancing Weapons of Mass Destruction (WMD) and/or improvised explosive device (IED) prevention, detection, response and recovery capabilities
			• Chemical/Biological/Radiological/ Nuclear/Explosive (CBRNE) detection, prevention, response, and recovery equipment

Exercise	• Long-term vulnerability reduction • Operational coordination • Operational communications • Community resilience	• Safety and security	• Response exercises, including exercise planning with community-based organizations

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. **In FY 2022 SHSP application projects 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, 2022

> **Projected Period of Performance End Date**: August 31, 2024

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 Office of Homeland Security 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 Oversite Committee (RHSOC) to be eligible for LETPA funding. *State units of government are exempt from this requirement.*

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 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 EMAC, except for American Samoa and the Commonwealth of the Northern Mariana Islands, which are not required to belong to EMAC at this time. All assets supported in part or entirely with FY 2022 HSGP funding must be readily deployable and NIMS-typed when possible to support emergency or disaster operations per existing EMAC agreements. In addition, funding may be used for the sustainment of core capabilities that, while they may not be physically deployable, support national response capabilities, 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: May 20, 2022

    b. Application Submission Deadline: June 17, 2022, 5:00 p.m. CST

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

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

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

An application workshop with instructions on how to apply through the WebGrants System will be available on the DPS website, at the following link under Grant Applications and Forms, FY 2022 State Homeland Security Program (SHSP): https://dps.mo.gov/dir/programs/ohs/grantstraining/

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

1. **Contact Information Form**

2. **SHSP Project Package**

3. **Budget**

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

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

SHSP Funding Guidelines

Subrecipients must comply with all the requirements in 2 C.F.R. Part 200 (*Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards*). Funding guidelines established within this section support the five mission areas—Prevention, Protection, Mitigation, Response, and Recovery—and associated core capabilities within the Goal. Allowable projects made in support of the 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 [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 [Preparedness Grants Manual](#), and the terms and conditions of the award and must be consistent with the statutory authority for the award. Award funds may not be used for matching funds for any other federal awards, lobbying, or intervention in federal regulatory or adjudicatory proceedings. In addition, federal funds may not be used to sue the Federal Government or any other government entity. See the [Preparedness Grants Manual](#) for more information on funding restrictions and allowable costs.

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

   Recipients and subrecipients of FEMA federal financial assistance are subject to the prohibitions described in section 889 of the [John S. McCain National Defense Authorization Act for Fiscal Year 2019 (FY 2019 NDAA)](#), Pub. L. No. 115-232 (2018) and 2 C.F.R. §§ 200.216, 200.327, 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 (Interim) FEMA Policy #405-143-1](#), or superseding document.

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

   Effective August 13, 2020, FEMA recipients and subrecipients **may not** use any FEMA funds under open or new awards to:

a. Procure or obtain any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology of any system;

b. Enter into, extend, or renew a contract to procure or obtain any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology of any system; or

c. Enter into, extend, or renew contracts with entities that use covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system.

I. Replacement Equipment and Services

FEMA grant funding may be permitted to procure replacement equipment and services impacted by this prohibition, provided the costs are otherwise consistent with the requirements of the NOFO and the Preparedness Grants Manual.

II. Definitions

Per section 889(f)(2)-(3) of the FY 2019 NDAA and 2 C.F.R. § 200.216, covered telecommunications equipment or services means:

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

ii.   For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);

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

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

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

2. 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 of operations 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 v2. 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.

Please see the [Preparedness Grants Manual](#) for additional information on planning costs.

3. Organization

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 SAA and must be made available to the recipient's respective FEMA HQ Program Analyst upon request.
- Migrating online services to the ".gov" internet domain.

Organizational activities under SHSP include:

Operational Overtime Costs

Operational overtime costs are allowed under this program. Prior to use of funds for operational overtime, subrecipients must receive approval from DHS/FEMA/OHS.

In support of efforts to enhance capabilities for detecting, deterring, disrupting, and preventing acts of terrorism and other catastrophic events, operational overtime costs are allowable for increased protective security measures at critical infrastructure sites or other high-risk locations and to enhance public safety during mass gatherings and high-profile events. SHSP subrecipients are urged to consider using grant funding to support soft target preparedness activities. SHSP funds may be used to support select operational expenses associated with increased security measures in the authorized categories cited in the table below, but this table is not exhaustive. FEMA/OHS retains the discretion to approve other types of requests that do not fit within one of the categories of the table.

	Category	Description
1	**National Terrorism Advisory System (NTAS)**	Security measures in response to an <u>increase in the threat level</u> under the NTAS to an "elevated" or "imminent" alert status. FEMA Information Bulletin No. 367, <u>Impact of National Terrorism Advisory System on Homeland Security Grant Programs</u>, remains applicable; therefore, advance authorization from FEMA is not required. Refer to <u>https://www.dhs.gov/topic/ntas</u> for additional information on the NTAS.
2	**National Security Special Event (NSSE)**	Security measures for a <u>designated</u> NSSE. NSSEs are events of national or international significance deemed by DHS to be a potential target for terrorism or other criminal activity.
3	**Special Event Assessment Rating (SEAR) Level 1 through Level 4 Events**	Security measures required for SEAR Level 1 through Level 4 events as designated by DHS and included in the DHS National Special Events List, as defined below: • SEAR 1: A significant event with national and/or international importance that may require extensive federal interagency support; • SEAR 2: A significant event with national and/or international importance that may require some level of federal interagency support. • SEAR 3: An event of national and/or international importance that requires only limited federal support. • SEAR 4: An event with limited national importance that is managed at state and local level. NOTE: In cases where a threat of terrorism can be associated with a SEAR Level 5 event, the event planners should coordinate with their state or territory Homeland Security Advisor to seek re-adjudication of the SEAR rating. Operational overtime for security measures associated with such events will be considered for approval by FEMA/OHS if re-adjudication results in a SEAR 1 through 4 rating.
4	**States of Emergency**	Declarations of states of emergency by the Governor <u>associated with a terrorism-related threat or incident</u>. This excludes Presidentially declared major disasters or emergencies where federal funding support for the

		proposed grant-funded activity is made available through the FEMA Public Assistance program or other federal disaster grants.
5	**National Critical Infrastructure Prioritization Program (NCIPP)**	Protection of Level 1 and Level 2 facilities identified through DHS's NCIPP <u>based on a terrorism-related threat</u> to critical infrastructure.
6	**Directed Transit Patrols**	Targeted security patrols in airports and major transit hubs <u>based on a terrorism-related threat</u> to transportation systems.
7	**Other Related Personnel Overtime Costs**	Overtime costs may be authorized for personnel assigned to directly support any of the security activities relating to the categories above. Examples include firefighters and emergency medical services personnel; public works employees who may be responsible for installing protective barriers and fencing; public safety personnel assigned to assist with event access and crowd control; emergency communications specialists; backfill and overtime for staffing state or major urban area fusion centers; state Active Duty National Guard deployments to protect critical infrastructure sites, including all resources that are part of the standard National Guard deployment package (note: consumable costs, such as fuel expenses, are not allowed except as part of the standard National Guard deployment package); contract security services for critical infrastructure sites; participation in Regional Resiliency Assessment Program activities, increased border security initiatives in coordination with USBP, etc.
8	**Operational Support to a Federal Agency**	Overtime costs are allowable for personnel to participate in information, investigative, and intelligence sharing activities related to homeland security/terrorism preparedness and specifically requested by a federal agency. Allowable costs are limited to overtime associated with federally requested participation in eligible activities, including anti-terrorism task forces, Joint Terrorism Task Forces (JTTFs), Area Maritime Security Committees (as required by the *Maritime Transportation Security Act of 2002*), DHS Border Enforcement Security Task Forces, and Integrated Border Enforcement Teams. In addition, reimbursement for operational overtime law enforcement activities related to combating transnational crime organizations in support of efforts to enhance capabilities for detecting, deterring, disrupting, and preventing acts of terrorism is an allowable expense under SHSP on a case-by-case basis. Grant funding can only be used in proportion to the federal man-hour estimate and only after funding for these activities from other federal sources (i.e., FBI JTTF payments to state and local agencies) has been exhausted.

Please see the Preparedness Grants Manual for additional information on organization costs.

4. **Personnel**

Personnel hiring, overtime, and backfill expenses are permitted under this grant to perform allowable HSGP planning, training, exercise, and equipment activities. Personnel may include but are not limited to training and exercise coordinators, program managers for activities directly associated with SHSP funded activities, intelligence analysts, and Statewide Interoperability Coordinators (SWICs).

Please see the Preparedness Grants Manual for additional information on personnel costs.

5. Equipment

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

For personal protective equipment (PPE), recipients are encouraged to give procurement preference to domestic manufacturers of PPE or PPE raw materials to the maximum practicable and allowed by law.

Grant funds may be used for the procurement of medical countermeasures. Procurement of medical countermeasures must be conducted in collaboration with state, city, or local health departments that administer federal funds from the Department of Health and Human Services for this purpose and with existing Metropolitan Medical Response System committees where available, to sustain their long-term planning for appropriate, rapid, and local medical countermeasures, including antibiotics and antidotes for nerve agents, cyanide, and other toxins. Procurement must have a sound threat-based justification with an aim to reduce the consequences of mass casualty incidents during the first crucial hours of a response. Prior to procuring pharmaceuticals, subrecipients must have in place an inventory management plan to avoid large periodic variations in supplies due to coinciding purchase and expiration dates. Subrecipients are encouraged to enter into rotational procurement agreements with vendors and distributors. Purchases of pharmaceuticals must include a budget for the disposal of expired drugs within each fiscal year's Period of Performance (POP) for HSGP. The cost of disposal cannot be carried over to another FEMA/OHS grant or grant period.

EMS electronic patient care data systems should comply with the most current data standard of the National Emergency Medical Services Information System (www.NEMSIS.org).

Please see the Preparedness Grants Manual for more information on equipment costs.

General Purpose Equipment

HSGP 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 HSGP must be shareable through 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:

- Law enforcement vehicles
- Emergency medical services (EMS) equipment and vehicles
- Fire service equipment and vehicles, to include hose, pump accessories, and foam concentrate for specialized 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 HSGP. As discussed below, certain equipment is "prohibited" and is not allowable under HSGP. For some controlled equipment that is allowable under the HSGP, 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.

Grant funds under this program may not be used for the purchase of equipment not approved by DHS/FEMA. The purchase of tracked armored vehicles, camouflage uniforms, weapons and weapons accessories, including ammunition, is not allowed with HSGP funds. Grant funds under this program must also comply with IB 426 and may not be used for the purchase of the following equipment:

- Firearms
- Ammunition
- Grenade launchers
- Bayonets
- Weaponized aircraft, vessels, or vehicles of any kind with weapons installed

Requirements for Small Unmanned Aircraft System

All requests to purchase Small Unmanned Aircraft Systems (sUAS) with FEMA grant funding must comply with IB 426 and IB 438 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 HSGP 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

HSGP 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 2022 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: https://www.dhs.gov/publication/interagency-legal-advisory-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: https://www.dhs.gov/news/2020/08/17/interagency-issues-advisory-use-technology-detect-and-mitigate-unmanned-aircraft.

6. Training

Allowable training-related costs under HSGP 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). Training conducted using HSGP 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. Any training or training gaps, including training related to under-represented diverse populations that may be more impacted by disasters, including children, seniors, individuals with disabilities or access and functional needs, individuals with diverse culture and language use, individuals with lower economic

capacity and other underserved populations, should be identified in an IPP and addressed in the state or high-risk urban area training cycle. Emergency preparedness training related to those training gaps, including related to under-represented, diverse populations that may be more impacted by disasters, is allowable. Subrecipients are encouraged to use existing training rather than developing new courses. When developing new courses, subrecipients are encouraged to apply the Analyze, Design, Develop, Implement, and Evaluate (ADDIE) model of instructional design.

Subrecipients are also encouraged to utilize FEMA's National Preparedness Course Catalog. Trainings include programs or courses developed for and delivered by institutions and organizations funded by FEMA. This includes the Center for Domestic Preparedness (CDP), the Emergency Management Institute (EMI), and FEMA's Training Partner Programs, including the Continuing Training Grants (CTG), the National Domestic Preparedness Consortium (NDPC), the Rural Domestic Preparedness Consortium (RDPC), and other partners.

The catalog features a wide range of course topics in multiple delivery modes to meet FEMA's mission scope as well as the increasing training needs of federal, state, local, territorial, and tribal audiences. The catalog can be accessed at http://www.firstrespondertraining.gov/.

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

Please see the Preparedness Grants Manual for more information on training costs.

7. Exercises

Exercises conducted with grant funding should be managed and conducted consistent with Homeland Security Exercise and Evaluation Program (HSEEP). HSEEP guidance for exercise design, development, conduct, evaluation, and improvement planning is located at https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep.

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

Please see the Preparedness Grants Manual for more information on exercise costs.

8. Travel

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

9. Construction and Renovation

Construction and renovation costs to achieve capability targets related to preventing, preparing for, protecting against, or responding to acts of terrorism are allowed under this program. For construction and renovation costs to be allowed, they must be specifically approved by DHS/FEMA in writing prior to the uses of any program funds. Applicants must use the Environmental Planning and Historical Preservation (EHP) approval process. Limits on the total amount of grant funding that may be used for construction or renovation may apply.

Please see the Preparedness Grants Manual for more information on construction and renovation costs.

10. Maintenance and Sustainment

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

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

Grant funds are intended to support the Goal by funding projects that build and sustain the core capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and recover from those threats that pose the greatest risk to the security of the Nation. In order to provide recipients the ability to meet this objective, the policy set forth in FEMA's IB 379, Guidance to State Administrative Agencies to Expedite the Expenditure of Certain DHS/FEMA Grant Funding, initially for FY 2007-2011, allows for the expansion of eligible maintenance and sustainment costs which must be in (1) direct support of existing capabilities; (2) must be an otherwise allowable expenditure under the applicable grant program; (3) be tied to one of the core capabilities in the five mission areas contained within the Goal, and (4) shareable through the EMAC. Additionally, eligible costs may also be in support of equipment, training, and critical resources that have previously been purchased with either federal grant or any other source of funding other than FEMA preparedness grant program dollars.

Please see the Preparedness Grants Manual for more information on maintenance and sustainment costs.

11. Critical Emergency Supplies

Critical emergency supplies, such as shelf stable products, water, and medical equipment and supplies are an allowable expense under SHSP.

Please see the Preparedness Grants Manual for more information.

12. Secure Identification

Secure identification costs are allowed under this program. Please see the Preparedness Grants Manual for more information.

28 C.F.R. Part 23 Guidance

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

Unallowable Costs

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

Administrative and National Policy Requirements

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

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

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

DHS Standard Terms and Conditions

All successful applicants for DHS grant and cooperative agreements are required to comply with DHS 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 is located at https://www.fema.gov/media-library/assets/documents/90195. Additionally, all subrecipients under this funding opportunity are required to comply with the FEMA GPD EHP Policy Guidance, FEMA Policy #108-023-1, available at https://www.fema.gov/media/library/assets/documents/85376.

Contact Information:

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

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

Office of Homeland Security:

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

Maggie Glick
Administrative Assistant
(573) 522-6125
Maggie.glick@dps.mo.gov