FY 2021 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), Office of Homeland Security (OHS)

Assistance Listing:

97.067

Funding Opportunity Title

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

Introduction

The Missouri Office of Homeland Security is pleased to announce the funding opportunity for the FY 2021 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, respond to, and recover from acts of terrorism.

The 2018-2022 FEMA Strategic Plan creates a shared vision for reducing the risks posed by terrorism and sets an ambitious, yet achievable, path forward to unify and further professionalize emergency management across the country. Homeland Security Grant Program (HSGP) supports the goals of Building a Culture of Preparedness and Readying the Nation for Catastrophic Disasters. We invite our stakeholders and partners to also adopt these priorities and join us in building a more prepared and resilient Nation, as preparedness is a shared responsibility and

funding should support priorities that are most impactful and demonstrate the greatest return on investment.

For FY 2021, DHS is focused on the criticality of information sharing and collaboration to building a national culture of preparedness and protecting against terrorism and other emerging threats to our national security. DHS and its homeland security mission were born from the "failures among federal agencies and between the federal agencies and state and local authorities to share critical information related to the threat of terrorism" prior to the September 11, 2001, attacks. The threat profile has changed in the past two decades – we now face continuous cyber threats by sophisticated actors, threats to soft targets and crowded places, threats from domestic violent extremists, and threats from new and emerging technologies. But information sharing and cooperation among state, local, and tribal authorities and federal agencies, including all DHS officials, is just as vital, and perhaps even more vital, today. Therefore, for FY 2021, DHS has identified five priority areas, tied to some of the most serious threats that they would like to see addressed by state and local governments. Perhaps most importantly, we will be focused on forging partnerships to strengthen information sharing and collaboration in each of these priority areas and looking for recipients to remove barriers to communication and cooperation with DHS and other federal agencies.

Objective

The objective of the FY 2021 SHSP is to fund state and local efforts to prevent terrorism and prepare the Nation for threats and hazards that pose the greatest risk to the security of the United States.

Priorities

Given the evolving threat landscape, it is incumbent upon DHS/FEMA/OHS to continuously evaluate the national/state risk profile and set priorities that help ensure appropriate allocation of scarce security dollars. In assessing the national risk profile for FY 2021, five priority areas attract the most concern. The following are the five priority areas for FY 2021:

1. Enhancing cybersecurity
2. Enhancing the protection of soft targets/crowded places;
3. Enhancing information and intelligence sharing and cooperation with federal and state agencies, including DHS/OHS;
4. Combating domestic violent extremism;
5. Addressing emergent threats (e.g., transnational criminal organizations, unmanned aircraft systems [UASs], weapons of mass destruction [WMD], etc.)

Likewise, there are several enduring security needs that crosscut the homeland security enterprise, and to which that States 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 2021 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/OHS anticipate 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 other funding mechanisms.

FY 2021 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 Security Agency (CISA) 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	• Safety and security	• Operational overtime • Physical security enhancements o Closed-circuit television (CCTV) security cameras o Security screening equipment for people and baggage o Lighting o Access controls o Fencing, gates, barriers, etc.

	• Access control and identity verification • Physical protective measures • Risk management for protection programs and activities		
Enhancing information and intelligence sharing and analysis, and cooperation with federal agencies, including DHS	• Intelligence and information sharing • Interdiction and disruption • Planning • Public information and warning • Operational coordination • Risk management for protection programs and activities	• 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 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 • Screening, search and detection • Physical protective measures • 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 campaigns and resources to help them identify and report potential instances of domestic violent extremism
Addressing Emergent Threats, such as the activities of Transnational Criminal Organizations, open source threats, and threats from UAS and WMD	• Interdiction & disruption • Screening, search and detection • Physical protective measures	• Safety and security	• Sharing and leveraging intelligence and information • UAS detection technologies • Enhancing WMD and/or improvised explosive device (IED) prevention,

	• Intelligence and information sharing • Planning • Public Information and Warning • Operational Coordination		detection, response and recovery capabilities ○ Chemical Biological Radiological Nuclear and Explosive (CBRNE) detection, prevention, response, and recovery equipment
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
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
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 ○ Security cameras (CCTV) ○ Security screening equipment for people and baggage ○ Lighting ○ Access Controls ▪ Fencing, gates, barriers, etc.
Exercises	• Long-term vulnerability reduction • Operational coordination • Operational communications	• Safety and security	• Response exercises

	• Community resilience		

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 2021 SHSP application projects that align to National Priorities will receive extra points during the application scoring process.**

Law Enforcement Terrorism Prevention Activities (LETPA)

Per section 2006 of the *Homeland Security Act of 2002*, as amended (6 U.S.C. § 607), DHS/FEMA is required to ensure that at least 25 percent of grant funding appropriated for grants awarded under HSGP's authorizing statute are used for LETPAs. DHS/FEMA meets this requirement, in part, by requiring all recipients allocate at least 25 percent of the combined HSGP funds allocated under SHSP and UASI towards LETPAs, as defined in 6 U.S.C. § 607. The LETPA allocation can be from SHSP, UASI, or both. The 25 percent LETPA allocation may be met by funding projects in any combination of the five national priority areas identified above and any other investments.

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 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: October 1, 2021

Projected Period of Performance End Date: September 30, 2023

Funding Instrument: Grant

Eligible Applicants:

The following entities are eligible to apply for FY 2021 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.***

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.

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 2021 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: August 10, 2021

   b. Application Submission Deadline: August 31, 2021, 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

A pre-recorded webinar 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 2021 State Homeland Security Program (SHSP):
https://dps.mo.gov/dir/programs/ohs/grantstraining/
As part of the FY 2021 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 (REQUIRED)**
   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.

LETPA projects will only be considered allowable if they were initially applied for through the RHSOC SHSP Regionalization program and meet all other LETPA criteria. ***(Projects completed at the State level 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 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.

The SHSP supports investments that improve the ability of regions to:

- Prevent a threatened or an actual act of terrorism;
- Protect citizens, residents, visitors, and assets against the threats that pose the greatest risk to the security of the United States;
- Mitigate the loss of life and property by lessening the impact of future catastrophic events;
- Respond quickly to save lives, protect property and the environment, and meet basic human needs in the aftermath of a catastrophic incident; and/or
- Recover through a focus on the timely restoration, strengthening, accessibility, and revitalization of infrastructure, housing, and a sustainable economy, as well as the health, social, cultural, historic, and environmental fabric of communities affected by a catastrophic incident, and do so in a manner that engages the whole community while ensuring the protection of civil rights.

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, 200.326, 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.

For additional guidance, please refer to Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services (Interim).

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. Law Enforcement Terrorism Prevention Activities Allowable Costs

Activities eligible for the use of Law Enforcement Terrorism Prevention Activities (LETPA) focused funds include but are not limited to:

- Maturation, enhancement, and sustainment of designated state and major urban area fusion centers, including information sharing and analysis, threat recognition, terrorist interdiction, and training/ hiring of intelligence analysts;
- 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 (HIDTAs), 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 intelligence process and fusion centers, including but not limited to: Fusion Center 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 the 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 site 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.

3. 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.

4. 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. 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 increase in the threat level under the NTAS to an "elevated" or "imminent" alert status. FEMA Information Bulletin No. 367, Impact of National Terrorism Advisory System on Homeland Security Grant Programs, remains applicable; therefore, advance authorization from FEMA is not required. Refer to https://www.dhs.gov/topic/ntash for additional information on the NTAS.
2	**National Security Special Event (NSSE)**	Security measures for a designated 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 associated with a terrorism-related threat or incident. 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 based on a terrorism-related threat to critical infrastructure.
6	**Directed Transit Patrols**	Targeted security patrols in airports and major transit hubs based on a terrorism-related threat 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.

Personnel Costs. 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 (SWIC).

For further details, refer to Information Bulletin No. 421b, Clarification on the Personnel Reimbursement for Intelligence Cooperation and Enhancement of Homeland Security Act of 2008 (Public L. No. 110–412 – the PRICE Act),), October 30, 2019, or contact their FEMA Preparedness Officer. HSGP funds may not be used to support the hiring of any personnel to fulfill traditional public health and safety duties nor to supplant traditional public health and safety positions and responsibilities. The following definitions apply to personnel costs:

- *Hiring*. State and local entities may use grant funding to cover the salary of newly hired personnel who are exclusively undertaking allowable DHS/FEMA grant activities as specified in this guidance. This may not include new personnel who are hired to fulfill any non-DHS/FEMA program activities under any circumstances. Hiring will always result in a net increase of Full Time Equivalent (FTE) employees.
- *Overtime*. These expenses are limited to the additional costs that result from personnel working over and above 40 hours of weekly work time as the direct result of their performance of DHS/FEMA-approved activities specified in this guidance. Overtime associated with any other activity is not eligible.
- *Backfill-Related Overtime*. Also called "Overtime as Backfill," these expenses are limited to overtime costs that result from personnel who are working overtime (as identified above) to perform the duties of other personnel who are temporarily assigned to DHS/FEMA-approved activities outside their core responsibilities. Neither overtime nor backfill expenses are the result of an increase of FTE employees.
- *Supplanting*. Grant funds will be used to supplement existing funds and will not replace (supplant) funds that have been appropriated for the same purpose. Applicants or subrecipients may be required to supply documentation certifying that a reduction in non-federal resources occurred for reasons other than the receipt or expected receipt of federal funds.

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 DHS/FEMA/OHS before obligation or purchase of the items. Please reference the grant notes for each equipment item to ensure prior approval is not required or to ensure prior approval is obtained if necessary.

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

Requirements for Small Unmanned Aircraft System
All applications to request the purchase of 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.

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. 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 the National Training and Education Division's National Preparedness Course Catalog. Trainings include programs or courses developed for and delivered by institutions and organizations funded by DHS/FEMA/National Training and Education Division (NTED). 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.

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.

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. 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.

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

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:
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