

Eligible Activity - LETPA Descriptions

(HSGD Compilation of References - September 2016)

Descriptions	Source
Countering Violent Extremism	
<p>Development of countering violent extremism (CVE) programs, projects, and initiatives, addressing prevention, intervention, and diversion efforts, including training on roles of law enforcement and how to effectively partner with law enforcement; developing and promoting training specifically for law enforcement executives and frontline officers on potential behaviors and indicators of violent extremism and how to appropriately analyze and report them; supporting community and law enforcement engagement strategies such as table top exercises, roundtable events, town hall meetings, and peer to peer activities; funding for existing and expansion of law enforcement community relations efforts, support for the development of community engagement plans, and joint projects to increase the awareness of violent extremist threats and community mitigation solutions.</p>	2
Critical Infrastructure Safety	
<p>Critical Infrastructure Safety- LETPP funds for organizational costs to support select operational expenses associated with increased security measures at critical infrastructure sites in the following authorized categories:</p> <ul style="list-style-type: none"> • Backfill and overtime expenses for staffing State or local emergency operations centers (EOCs) and/or fusion centers • Hiring of contracted security for critical infrastructure sites • Public safety overtime • National Guard deployments to protect critical infrastructure sites, including all resources that are part of the standard National Guard deployment package • Increased border security activities in coordination with U.S. Customs and Border Protection (CBP), as outlined in G&T Information Bulletin #135 	4
Target Hardening	3
Forensics and Attribution	
<p>Forensics and Attribution - Conduct forensic analysis and attribute terrorist acts (including the means and methods of terrorism) to their source(s), to include forensic analysis as well as attribution for an attack and for the preparation for an attack in an effort to prevent initial or follow-on acts and/or swiftly develop counter-options.</p> <p>Critical Tasks</p> <ul style="list-style-type: none"> • Preserve the crime scene and conduct site exploitation for intelligence collection. • Conduct crime scene investigation. • Conduct forensic evidence examination, including biometric and DNA analysis. • Conduct CBRNE material analysis. • Conduct digital media, network exploitation, and cyber technical analysis. • Assess capabilities of perpetrating terrorists and compare with known terrorist capabilities and methods of operation. • Conduct investigations to identify the perpetrator(s), conspirator(s), and sponsorship. • Interview witnesses, potential associates, and/or perpetrators. • Analyze intelligence and forensics results to refine/confirm investigative leads. • Fuse intelligence, law enforcement information, and technical forensic conclusions to develop attribution assessments. • Interpret and communicate attribution results, confidence levels, and their significance to national decision makers. 	1

Eligible Activity - LETPA Descriptions

(HSGD Compilation of References - September 2016)

Fusion Centers	
Maturation and enhancement of designated state and major urban area fusion centers, including information sharing and analysis, threat recognition, and terrorist interdiction. Efforts to enhance coordination between criminal intelligence and real time crime analysis units, to include Joint Terrorism Task Forces (JTFs), Field Intelligence Groups (FIGs), High Intensity Drug Trafficking Areas (HIDTAs), and Regional Information Sharing Systems (RISS).	2
Establishing, enhancing, and staffing with appropriately qualified personnel State, local, and regional fusion centers that comply with the guidelines established under section 210A(i) of the Homeland Security Act of 2002, as amended.	3
<p>Establishment / Enhancement of Fusion Centers</p> <ul style="list-style-type: none"> • Development of a statewide fusion process that corresponds with the Global Justice / Homeland Security Advisory Council (HSAC) Fusion Center Guidelines, which can be accessed at http://it.ojp.gov/documents/fusion_center_guidelines.pdf. • Achievement of a baseline level of capability as defined by the Fusion Capability Planning Tool. Grantees are encouraged to use the Fusion Capability Planning Tool to determine and prioritize areas of improvement, as well as develop strategies to overcome shortfalls. Jurisdictions are encouraged to prioritize the expenditure of LETTP funds to address identified areas of improvement. 	4
Intelligence and Information Sharing	
<p>Intelligence and Information Sharing - Identify, develop, and provide timely, accurate, and actionable information resulting from the planning, direction, collection, exploitation, processing, analysis, production, dissemination, evaluation, and feedback of available information concerning physical and cyber-threats to the United States, its people, property, or interests; the development, proliferation, or use of WMDs; or any other matter bearing on U.S. national or homeland security by local, state, tribal, territorial, and Federal governments and other stakeholders. Information sharing is the ability to exchange intelligence, information, data, or knowledge among government or private sector entities, as appropriate.</p> <p>Critical Tasks</p> <ul style="list-style-type: none"> • Planning and Direction: Establish the intelligence and information requirements of the consumer. <ul style="list-style-type: none"> ▪ Rapidly reprioritize law enforcement and intelligence assets as necessary and appropriate. ▪ Engage with public and private sector partners in order to determine what intelligence and information assets may be available for reprioritization. ▪ Obtain additional information through avenues such as law enforcement deployment, questioning of witnesses and suspects, increased surveillance activity, and community policing and outreach. • Collection: Gather the required raw data to produce the desired finished intelligence and information products. <ul style="list-style-type: none"> ▪ Gather/collect information via law enforcement operations, suspicious activity reporting, surveillance, community engagement, and other activities and sources as necessary. • Exploitation and Processing: Convert raw data into comprehensible information. • Analysis and Production: Integrate, evaluate, analyze, and prepare the processed information for inclusion in the finished product. • Dissemination: Deliver finished intelligence and information products to the consumer and others as applicable. <ul style="list-style-type: none"> ▪ Develop appropriately classified/unclassified products to disseminate threat information to local, state, tribal, territorial, Federal, international, private sector, nonprofit sector, faith-based organizations, and public partners. 	1

Eligible Activity - LETPA Descriptions

(HSGD Compilation of References - September 2016)

<ul style="list-style-type: none"> • Feedback and Evaluation: Acquire continual feedback during the intelligence cycle that aids in refining each individual stage and the cycle as a whole. • Assessment: Continually assess threat information to inform continued prevention operations and ongoing response activities. 	
<ul style="list-style-type: none"> • Information sharing and analysis • Threat recognition • Paying salaries and benefits for personnel, including individuals employed by the grant recipient on the date of the relevant grant application, to serve as qualified intelligence analysts 	3
<p>Information Sharing and Intelligence Analysts</p> <ul style="list-style-type: none"> • Overtime costs are allowable for personnel to participate in information, investigative, and intelligence sharing activities specifically related to homeland security. This includes activities such as anti-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. • Funds may be used to hire new staff and/or contractor positions to serve as intelligence analysts to enable information/intelligence sharing capabilities. 	4
Interdiction and Disruption	
<p>Interdiction and Disruption - Delay, divert, intercept, halt, apprehend, or secure threats and/or hazards.</p> <p>Critical Tasks</p> <ul style="list-style-type: none"> • Interdict conveyances, cargo, and persons associated with an imminent terrorist threat or act. • Prevent terrorist entry into the United States and its territories. • Prevent movement and operation of terrorists within the United States. • Render safe and dispose of CBRNE hazards in multiple locations and in all environments consistent with established protocols. • Disrupt terrorist financing or prevent other material support from reaching its target. • Prevent terrorist acquisition and transfer of CBRNE materials, precursors, and related technology. • Conduct antiterrorism operations in the United States. • Conduct tactical counterterrorism operations in the United States, potentially in multiple locations and in all environments. • Strategically deploy assets to interdict, deter, or disrupt threats from reaching potential target(s). 	1
<p>Enhanced Law Enforcement Operations - Overtime expenses consistent with a State Homeland Security Plan, including for the provision of enhanced law enforcement operations in support of Federal agencies, including for increased border security and border crossing enforcement.</p>	3
<p>Terrorist interdiction</p>	3
Operational Coordination	
<p>Operational Coordination - Establish and maintain a unified and coordinated operational structure and process that appropriately integrates all critical stakeholders and supports the execution of core capabilities.</p> <p>Critical Tasks</p> <ul style="list-style-type: none"> • Collaborate with all relevant stakeholders. • Ensure clear lines and modes of communication among participating organizations and jurisdictions, both horizontally and vertically. • Facilitate effective intelligence and information sharing. • Define and communicate clear roles and responsibilities relative to courses of action. 	1

Eligible Activity - LETPA Descriptions

(HSGD Compilation of References - September 2016)

<ul style="list-style-type: none"> • Integrate and synchronize actions of participating organizations and jurisdictions to ensure unity of effort. • Determine priorities, objectives, strategies, and resource allocations. • Coordinate activities across and among all levels of government and with critical nonprofit and private sector partners to prevent imminent terrorist threats and/or conduct law enforcement investigative and response activities after an act of terrorism. 	
Planning	
<p>Planning - Conduct a systematic process engaging the whole community as appropriate in the development of executable strategic, operational, and/or tactical-level approaches to meet defined objectives.</p> <p>Critical Tasks</p> <ul style="list-style-type: none"> • Initiate a time-sensitive, flexible planning process that builds on existing plans and incorporates real-time intelligence. • Make appropriate assumptions to inform decision makers and counterterrorism professionals' actions to prevent imminent attacks on the homeland. • Evaluate current intelligence and coordinate the development of options as appropriate. • Identify possible terrorism targets and vulnerabilities. • Identify law enforcement, intelligence, diplomatic, private sector, economic, and/or military options designed to prevent, deter, or disrupt imminent terrorist attacks on the homeland and imminent follow-on attacks. • Present courses of action to decision makers to locate, interdict, deter, disrupt, or prevent imminent attacks on the homeland and imminent follow-on attacks. • Implement, exercise, and maintain plans to ensure continuity of operations. 	1
<p>Planning Activities</p> <ul style="list-style-type: none"> • Hiring an IT specialist to plan, develop, and implement the IT applications necessary for the fusion center • Developing and planning for information/intelligence sharing groups • Hiring contractors and consultants to make recommendations on the development of the fusion center • Conducting point vulnerability analyses and assessments • Soft target security planning (public gatherings) • Developing border security operations plans in coordination with CBP • Developing, implementing, and reviewing Area Maritime Security Plans for ports, waterways, and coastal areas • Updating and refining threat matrices • Integrating and coordinating private sector participation with fusion center activities • Acquiring systems allowing connectivity to State, local, and Federal data networks, such as the National Crime Information Center (NCIC) and Integrated Automated Fingerprint Identification System (IAFIS), as appropriate • Designing and developing State and local geospatial data systems • Costs associated with the implementation and adoption of NIMS • Developing related terrorism prevention activities • Integrating and coordinating private sector participation with fusion center activities 	4

Eligible Activity - LETPA Descriptions

(HSGD Compilation of References - September 2016)

Public Information and Warning	
<p>Public Information and Warning - Deliver coordinated, prompt, reliable, and actionable terrorism-related information to the whole community through the use of clear, consistent, accessible, and culturally and linguistically appropriate methods to effectively relay information regarding any threat and the actions being taken and the assistance being made available, as appropriate.</p> <p>Critical Tasks</p> <ul style="list-style-type: none"> • Increase public awareness of indicators of terrorism and terrorism-related crime; for example, through the “If You See Something, Say Something”™ public awareness program. • Refine and consider options to release pre-event information publicly, and take action accordingly. • Protect information so as not to compromise ongoing prevention operations (e.g., intelligence activities and investigations). • Share prompt and actionable messages, to include NTAS Alerts, with the public and other stakeholders, as appropriate, to aid in the prevention of imminent follow-on terrorist attacks. • Use all appropriate communication means, such as the Integrated Public Alert and Warning System (IPAWS) and social media. 	1
Screening, Search, and Detection	
<p>Screening, Search, and Detection - Identify, discover, or locate terrorist threats through active and passive surveillance and search procedures. This may include the use of systematic examinations and assessments, bio-surveillance, sensor technologies, or physical investigation and intelligence.</p> <p>Critical Tasks</p> <ul style="list-style-type: none"> • Locate persons and networks associated with imminent terrorist threats. • Develop and engage an observant Nation (i.e., individuals and families; communities; NGOs; private sector entities; and local, state, tribal, and territorial partners). • Screen and/or scan inbound and outbound persons, baggage, mail, cargo, and conveyances using technical, nontechnical, intrusive, and nonintrusive means without unduly hampering commerce. • Apply additional measures for high-risk persons, conveyances, or items. <p>Conduct physical searches.</p> <ul style="list-style-type: none"> • Conduct chemical, biological, radiological, nuclear, and explosive (CBRNE) surveillance search and detection operations. • Conduct ambient and active detection of CBRNE. • Operate in a hazardous environment. • Conduct technical search/detection operations. • Conduct nontechnical search/detection operations. • Conduct bio-surveillance. • Search databases and other information and intelligence sources. • Employ wide-area search and detection assets in targeted regions in concert with state, local, and tribal personnel or other Federal agencies (depending on the threat). 	1
Suspicious Activity Reporting	
<p>Implementation and maintenance of the Nationwide Suspicious Activity Reporting (SAR) Initiative, including regional training with the goal of enhanced reporting of suspicious activities and efforts to increase SAR reporting for small, medium, and large law enforcement agencies.</p>	2

Eligible Activity - LETPA Descriptions

(HSGD Compilation of References - September 2016)

Training/Exercises	
Full Scale Training Exercises - Support for coordination of regional full-scale training exercises (federal, state, and local law enforcement participation) focused on responding to terrorism-related events and increasing participation with community and business organizations.	2
Regional Counterterrorism Training Programs for small, medium, and large jurisdictions to exchange information and discuss the current threat environment, lessons learned, and best practices to help prevent, protect against, and mitigate acts of terrorism.	2
<p>Exercises - LETPP funds may be used to design, develop, conduct, and evaluate terrorism prevention-related exercises, including the following:</p> <ul style="list-style-type: none"> • Exercises to evaluate the effectiveness of information sharing plans, policies, procedures, and protocols • Exercises to evaluate NIMS implementation • Exercises to evaluate facility and/or vessel security protection • Exercises to evaluate area maritime security protection • Exercises to evaluate threat recognition capabilities • Exercises to evaluate cyber security capabilities • Exercises to evaluate agricultural/food security capabilities • Exercises to evaluate prevention readiness and techniques • “Red Team” (force on force) exercises • Interoperable communications exercises • Critical infrastructure vulnerability, protection, and/or attack exercises 	4
<p>Terrorism Prevention Training - LETPP funds may be used for a range of law enforcement terrorism prevention related training activities to enhance the capabilities of State and local personnel including:</p> <ul style="list-style-type: none"> • Training intelligence analysts • Building information sharing capacity • Methods of target hardening • Facility law enforcement security personnel • CBRNE, agriculture, and cyber threats • History of terrorism and social environments contributing to threats • Surveillance and counter-surveillance techniques • Critical Infrastructure Protection training • Cyber/agriculture/food security threats recognition and protective measures • Multi-cultural training for undercover operations related to terrorist organizations • Languages, such as Arabic, Urdu, or Farsi • Joint training with other HS entities (CBP, Secret Service) • Use of interoperable communications equipment • Collection, analysis, mapping, integration, and dissemination of geospatial data and imagery • Geospatial database use, design, development, and management training • Citizens in terrorism awareness and for volunteer participation to support law enforcement activities, to include the Volunteers in Police Service and Neighborhood Watch programs 	4

Source Key	FEMA Reference
1	National Prevention Framework
2	IB 412 - DHS Identified Priorities
3	Homeland Security Act of 2002, Section 2006 (6 U.S.C. § 607)
4	FY 2007 Homeland Security Grant Program Guidance