Office of the Governor, Public Safety Office
Homeland Security Grants Division
Funding Announcement: ***2022 Urban Area Security Initiative – LETPA Projects (UASI-L)***

Purpose

The Public Safety Office (PSO) is soliciting applications for projects that support state and local efforts to prevent terrorism and other catastrophic events and prepare for the threats and hazards that pose the greatest risk to the security of Texas citizens. PSO provides funding to implement investments that build, sustain, and deliver the 32 core capabilities essential to achieving a secure and resilient state.

Per Congressional mandate (911 Act), twenty-five percent (25%) of the combined Homeland Security Grant Program funding must be spent on Law Enforcement Terrorism Prevention Activities (LETPA). The purpose of this solicitation is to assist high-threat, high-density Urban Areas in efforts to build and sustain the capabilities necessary to prevent terrorist attacks and support critical prevention and protection activities. All LETPA investments must be consistent with capability targets set during the Threat and Hazard Identification and Risk Assessment (THIRA) process, and gaps identified in the State Preparedness Report (SPR).

The Urban Area Security Initiative (UASI) is intended to support investments that improve the ability of jurisdictions to:

- **Prevent** a threatened or an actual act of terrorism; and/or
- **Protect** its citizens, residents, visitors, and assets against the greatest threats and hazards.

Prevention is defined as the capabilities necessary to avoid, prevent, or stop a threatened or actual act of terrorism.

Many activities which support the achievement of target capabilities related to terrorism preparedness may simultaneously support enhanced preparedness for other hazards unrelated to acts of terrorism. However, **all UASI-LETPA projects must assist grantees in achieving target capabilities related to preventing or thwarting an initial or follow-on terrorist attack.**

Available Funding

Federal funds are authorized under Section 2002 of the Homeland Security Act of 2002, as amended (Pub. L. No. 107-296), (6 U.S.C. 603). Urban Area Security Initiative (UASI) funds are made available through a Congressional appropriation to the United States Department of Homeland Security (DHS). All awards are subject to the availability of appropriated federal funds and any modifications or additional requirements that may be imposed by law.

Eligible Organizations

1. Eligible applicants must be located within a designated high-risk Urban Area receiving a FY 2022 federal allocation based upon an analysis of the relative risk of terrorism faced by the 100 most populous metropolitan statistical areas in the United States. Most recently, these areas in Texas include the Dallas/Fort Worth/Arlington Area, the Houston Area, and the San Antonio Area.
2. Applications from the following entities will be considered*:
    a. State agencies;
    b. Regional councils of governments;
    c. Units of local government;
    d. Nonprofit organizations; and

e. Universities or Colleges.

*Note: All applicant entities must have a mission to serve in an Urban Area operational role or be partnering on plans, training, and exercises within the Urban Area.

Application Process

1. Applicants must contact the applicable Urban Area Working Group (UAWG) regarding their application.
2. Each UAWG holds its own application planning workshops, workgroups, and/or subcommittees and facilitates application prioritization for certain programs within its area. Failure to comply with requirements imposed by the UAWG will render an application ineligible.
3. Upon approval of the UAWG, eligible applicants must access the Office of the Governor's eGrants website at https://eGrants.gov.texas.gov to register and continue the application process. For more instructions and information, see *eGrants User Guide to Creating an Application*, available here.

Key Dates

Action	Date
Funding Announcement Release	03/04/2022
Online System Opening Date	03/04/2022
Final Date to Submit and Certify an Application	04/08/2022 at 5:00pm CST
Earliest Project Start Date	09/01/2022

Project Period

Projects selected for funding must begin between September 1, 2022 and March 1, 2023, and expire on or before August 31, 2024. Additional guidelines are below:

1. Project periods should be structured so that projects that include grant-funded salaries and/or annual recurring costs do not overlap with the project periods of previous or future grant awards with the same costs.
2. Project periods should be structured so that projects that include grant-funded salaries and/or annual recurring costs are on a 12 **or** 24-month grant cycle/performance period.
3. Project periods for equipment only projects are generally awarded for a 6 to 12-month grant period.
4. PSO will consider proposed start or end dates falling outside of these guidelines on a case-by-case basis.

Funding Levels

Minimum: $2,500

Maximum: None.

Match Requirement: None

Standards

Grantees must comply with standards applicable to this fund source cited in the Texas Grant Management Standards (TxGMS), Federal Uniform Grant Guidance, and all statutes, requirements, and guidelines applicable to this funding.

Eligible Activities and Costs

1. Grant projects must be consistent with the Federal Emergency Management Agency (FEMA) Information Bulletin (IB) 412 which discusses eligible activities outlined in:
    a. The National Prevention Framework;
    b. The National Protection Framework where capabilities are shared with the prevention mission area;
    c. Section 2006 of the Homeland Security Act of 2002, as amended; and
    d. The FY 2007 Homeland Security Grant Program Guidance and Application Kit.
2. Grant projects must be consistent with the program purpose stated above and must be submitted in support of one of the approved urban area investment categories. Contact the applicable Urban Area Working Group for an updated list of investment categories.
3. DHS/FEMA has outlined the following five (5) required National Priorities. Urban Areas must allocate specific percentages of UASI funds toward each priority for a total of 30% of the award. The National Priority areas and examples of projects include:
    a. **Addressing Emerging Threats (FEMA National Priority, 5%)**

    Core Capabilities: Interdiction & Disruption; Screening, Search and Detection; Physical Protective Measures; Intelligence and Information Sharing; Planning; Public Information and Warning; Operational Coordination

        i. Enhancing weapons of mass destruction (WMD) and/or improvised explosive device (IED) prevention, detection, response and recovery capabilities.
        ii. Enhancing Chemical Biological Radiological Nuclear and Explosive (CBRNE) detection, prevention, response, and recovery capabilities.
        iii. Building and enhancing UAS detection capabilities
        iv. Enhancing public awareness education and communications and increasing reporting of suspicious activities related to critical infrastructure.

    b. **Combating Domestic Violent Extremism (FEMA National Priority, 7.5%)**

    Core Capabilities: Interdiction & 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

        i. Open source analysis of misinformation campaigns, targeted violence and threats to life, including tips/leads, and online/social media-based threats.
        ii. Execution and management of threat assessment programs to identify, evaluate, and analyze indicators and behaviors indicative of domestic violent extremists.
        iii. Establishing and maintaining suspicious activity reporting programs.
        iv. 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.

    c. **Enhancing Cybersecurity (FEMA National Priority, 7.5%)**

    Core Capabilities: Cybersecurity; Intelligence and Information Sharing

        i. Assessing organizational cybersecurity risk and potential risk.
        ii. Creating or updating strategic cybersecurity plans and related response and recovery plans and exercises.

iii. Developing approaches for identifying, authenticating and authorizing individuals to access an organization's assets and systems.

iv. Purchasing software such as anti-virus, anti-malware, continuous monitoring, encryption, enhanced remote authentication, patch management or distributed denial of service protection.

v. Purchasing hardware such as intrusion detection systems, firewalls, additional servers, routers or switches for the purpose of reducing cybersecurity vulnerabilities.

vi. Implementing awareness and training measures.

vii. Establishing anomalous activity detection and system/asset monitoring.

viii. Developing or sustaining response activities, including information sharing or other mitigation efforts.

ix. Conducting other cyber-related activities derived from a prioritized, risk management plan and consistent with objectives of the Texas Cybersecurity Framework (TXCSF) or other comparable framework.

d. **Information and Intelligence Sharing/Cooperation (FEMA National Priority, 5%)**
(Note: Applicants should submit Fusion Center projects under this UASI-Law Enforcement Terrorism Prevention Activities (LETPA) solicitation.)

Core Capability: Intelligence and Information Sharing

i. Identifying, developing, providing, and sharing timely, accurate, and actionable information, data, or knowledge among government or private sector entities to include information sharing with all DHS components, fusion centers, and other entities designated by DHS.

ii. Cooperation with DHS officials and other entities designated by DHS in intelligence, threat recognition and analysis.

iii. Joint training and planning with DHS officials and other entities designated by DHS

iv. Enabling interdiction and disruption of terrorist activity through enhanced understanding and recognition of pre-operational activity and other crimes that may be precursors or indicators of terrorist activity.

v. Paying for personnel or contractors to serve as qualified intelligence analysts and/or to participate in information, investigative, and intelligence sharing activities specifically related to homeland security.

vi. Assessing threat information to inform continued prevention operations and ongoing response activities.

vii. Implementing and maintaining suspicious activity reporting initiatives.

viii. Implementing or sustaining public information and warning systems to relay information regarding terrorism threats.

e. **Protection of Soft Targets/Crowded Places (FEMA National Priority, 5%)**

Core Capabilities: Operational Coordination; Public Information and Warning; Intelligence and Information Sharing; Interdiction and Disruption; Screening, Search, and Detection; Access Control/Identity Verification; Physical Protective Measures: Risk Management for Protection Programs

i. Implementing target hardening and other measures associated with increased security to mitigate risks at places where people gather, such as schools, workplaces, entertainment venues, transportation nodes, and houses of worship.

ii. Assessing critical infrastructure vulnerabilities and interdependencies, particularly those involving multiple sites and/or sectors.

iii. Planning, training, exercises, equipment, and modeling enabling responsible jurisdictions to mitigate threats to and vulnerabilities of critical infrastructure facilities, assets, networks, and systems.

iv. Analyzing critical infrastructure threats and information sharing with private sector partners.

v. Enhancing public awareness education and communications and increasing reporting of suspicious activities related to critical infrastructure.

4. Interoperable communications projects must enhance current capabilities or address capability gaps identified by the Texas Department of Public Safety (DPS) or Texas Interoperable Communications Coalition (TxICC) in either the Texas Statewide Communications Interoperability Plan (SCIP) or DPS Report on Interoperable Communications to the Texas Legislature.

   Notes: *Projects to increase voice communications interoperability for counties with the lowest interoperability levels are preferred over other types of communications projects. If a project is funded (after an agency receives the grant award from the PSO), the planned expenditures must be submitted to and receive validation from the Statewide Interoperability Coordinator (SWIC) prior to purchase.* ***Projects for the purchase of radios and similar equipment are only permitted under LETPA when the equipment is for members of special teams and the project narrative outlines how the teams will use the equipment for terrorism prevention/protection activities.*** *Radios purchased must: a) follow the Statewide Radio ID Management Plan; b) be programmed following the Statewide Interoperability Channel Plan, and c) include encryption options capable of Advanced Encryption Standard (AES) encryption, IF encryption is being purchased.*

5. Cybersecurity projects must enhance current cyber-related activities or address cyber-related capability gaps derived from a prioritized, risk management decision that is consistent with the objectives of the Texas Cyber Security Framework (TXCSF) or other cybersecurity guidance and priorities established by your UAWG.

6. Fusion Center projects must directly align to any capability gaps identified (if applicable) and leverage the data the fusion center used to complete DHS's annual Fusion Center Assessment of the national network. Additionally, each project must align to and reference specific performance areas of the Fusion Center Assessment that the funding is intended to support.

   Recognized fusion centers must meet fusion center operational standards as established by the Texas Department of Public Safety, including but not limited to: sharing information within the Texas Suspicious Activity Reporting Network; contributing to and supporting activities of the School Safety Working Group; participating in groups established by the Texas Fusion Center Policy Council (TxFCPC); and implementing activities to assist in achieving the objectives of the Texas Homeland Security Strategic Plan.

   Examples of eligible grant-funded fusion center activities include: Facilitating the implementation of plans and procedures, in conjunction with the Texas' primary fusion center, to support the maturation of the Information Sharing Environment (ISE); strengthening capabilities to address emerging threats, sustain analytic capability, integrate technology and/or support other priorities identified by DHS/FEMA or Texas Executive Orders; implementing Suspicious Activity Reporting (SAR) guidance and tools for fusion centers; and attending approved training classes for intelligence analysts (please refer to https://www.dhs.gov/fema-approved-intelligence-analyst-training-courses).

Program-Specific Requirements

1. All capabilities being built or sustained must have a clear link to one or more of the following Core Capabilities in the National Preparedness Goal: **Planning; Public Information and Warning;**

Operational Coordination; Intelligence and Information Sharing; Interdiction and Disruption; Screening, Search and Detection; and Forensics and Attribution.

2. Many capabilities which support terrorism preparedness simultaneously support preparedness for other hazards. Grantees must demonstrate this dual-use quality for any activities implemented under this program that are not explicitly focused on terrorism preparedness. Activities implemented under UASI must support terrorism preparedness by building or sustaining capabilities that relate to the prevention of terrorism.
3. Grantees are required to maintain adoption and implementation of the National Incident Management System (NIMS). The NIMS uses a systematic approach to integrate the best existing processes and methods into a unified national framework for incident management across all homeland security activities including prevention, protection, response, mitigation, and recovery. Grantees must use standardized resource management concepts for resource typing, credentialing, and an inventory to facilitate the effective identification, dispatch, deployment, tracking and recovery of resources.
4. Cities and counties must have a current emergency management plan or be a legally established member of an inter-jurisdictional emergency management program with a plan on file with the Texas Department of Public Safety, Texas Division of Emergency Management (TDEM). Plans must be maintained throughout the entire grant performance period. If you have questions concerning your Emergency Management Plan (preparedness) level, contact your Emergency Management Coordinator (EMC) or your regional Council of Governments (COG). For questions concerning plan deficiencies, contact TDEM at tdem.plans@tdem.texas.gov.
5. Grantees will be required to complete the 2022 Nationwide Cybersecurity Review (NCSR), enabling agencies to benchmark and measure progress of improving their cybersecurity posture. The Chief Information Officer (CIO), Chief Information Security Officer (CISO), or equivalent for each recipient agency should complete the NCSR. If there is no CIO or CISO, the most senior cybersecurity professional should complete the assessment. The NCSR is available at no cost to the user and takes approximately 2-3 hours to complete. For more information about the NCSR, visit: https://www.cisecurity.org/ms-isac/services/ncsr/.

Eligibility Requirements

1. Local units of governments must comply with the Cybersecurity Training requirements described in Section 772.012 and Section 2054.5191 of the Texas Government Code. Local governments determined to not be in compliance with the cybersecurity requirements required by Section 2054.5191 of the Texas Government Code are ineligible for OOG grant funds until the second anniversary of the date the local government is determined ineligible. Government entities must annually certify their compliance with the training requirements using the Cybersecurity Training Certification for State and Local Governments. A copy of the Training Certification must be uploaded to your eGrants application. For more information or to access available training programs, visit the Texas Department of Information Resources Statewide Cybersecurity Awareness Training page.
2. Entities receiving funds from PSO must be located in a county that has an average of 90% or above on both adult and juvenile dispositions entered into the computerized criminal history database maintained by the Texas Department of Public Safety (DPS) as directed in the Texas Code of Criminal Procedure, Chapter 66. This disposition completeness percentage is defined as the percentage of arrest charges a county reports to DPS for which a disposition has been subsequently reported and entered into the computerized criminal history system.

3. Counties applying for grant awards from the Office of the Governor must commit that the county will report at least 90% of convictions within five business days to the Criminal Justice Information System at the Department of Public Safety.
4. Eligible applicants operating a law enforcement agency must be current on reporting complete UCR data and the Texas specific reporting mandated by 411.042 TGC, to the Texas Department of Public Safety (DPS) for inclusion in the annual Crime in Texas (CIT) publication. To be considered eligible for funding, applicants must have submitted a full twelve months of accurate data to DPS for the most recent calendar year by the deadline(s) established by DPS. Due to the importance of timely reporting, applicants are required to submit complete and accurate UCR data, as well as the Texas-mandated reporting, on a no less than monthly basis and respond promptly to requests from DPS related to the data submitted.
5. Eligible applicants must have a DUNS (Data Universal Numbering System) number assigned to its agency (to request a DUNS number, go to https://fedgov.dnb.com/webform).
6. Eligible applicants must be registered in the federal System for Award Management (SAM) database located at https://www.sam.gov/.

Prohibitions

Grant funds may not be used to support the unallowable costs listed in the Guide to Grants or any of the following unallowable costs:

1. inherently religious activities such as prayer, worship, religious instruction, or proselytization;
2. lobbying;
3. any portion of the salary of, or any other compensation for, an elected or appointed government official;
4. vehicles or equipment for government agencies that are for general agency use and/or do not have a clear nexus to terrorism prevention, interdiction, and disruption (i.e. mobile data terminals, body cameras, in-car video systems, or radar units, etc. for officers assigned to routine patrol; general firefighting equipment or uniforms);
5. weapons, ammunition, tasers, weaponized vehicles or explosives (exceptions may be granted when explosives are used for bomb squad training);
6. weapons or weapons accessories to include but not limited to optics/sights, ammunition pouches, slings, or other accessories designed for use with any firearms/weapon;
7. admission fees or tickets to any amusement park, recreational activity or sporting event;
8. promotional item or gifts;
9. food, meals, beverages, or other refreshments, except for eligible per diem associated with grant-related travel or where pre-approved for working events;
10. membership dues for individuals;
11. any expense or service that is readily available at no cost to the grant project;
12. any use of grant funds to replace (supplant) funds that have been budgeted for the same purpose through non-grant sources;
13. fundraising;
14. legal services for adult offenders;
15. amateur radios and equipment, FMS radios, GMRS radios, or other radio equipment that is not P25 compliant;
16. riot equipment including but not limited to shields, batons, less-lethal ammunition, and grenades designed or intended for dispersing crowds; and

17. any other prohibition imposed by federal, state, or local law.

Selection Process

Application Screening: HSGD will screen all applications to ensure that they meet the requirements included in the funding announcement.

Peer/Merit Review:

1. The UAWG's sub-committee(s) will prioritize all eligible applications based on state and UAWG priorities, the UAWG risk-informed methodology, cost, and program effectiveness.
2. PSO will accept priority listings that are approved by the UAWG's executive committee.

Final Decisions – All Projects: The executive director will consider UAWG rankings along with other factors and make all final funding decisions. Other factors may include cost effectiveness, overall funds availability, reasonableness, or other relevant factors.

HSGD may not fund all applications or may only award part of the amount requested. In the event that funding requests exceed available funds, PSO may revise projects to address a more limited focus.

Contact Information

For more information, contact the eGrants help desk at eGrants@gov.texas.gov or (512) 463-1919.