Office of the Governor, Public Safety Office
Homeland Security Grants Division
Funding Announcement: 2020 State Homeland Security Program – Regular Projects (SHSP-R)

Purpose

The Homeland Security Grants Division (HSGD) 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. HSGD provides funding to implement investments that build, sustain, and deliver the 32 core capabilities essential to achieving a secure and resilient state.

The purpose of this solicitation is to support state, tribal and local preparedness activities that address high-priority preparedness gaps across all core capabilities where a nexus to terrorism exists. All investments must be consistent with capability targets set during the Threat and Hazard Identification and Risk Assessment (THIRA) process, and gaps identified in the Stakeholder Preparedness Review (SPR).

The SHSP is intended to support investments that improve the ability of jurisdictions to:

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

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 SHSP projects must assist grantees in achieving target capabilities related to preventing, preparing for, protecting against, or responding to acts of terrorism.**

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). State Homeland Security Program (SHSP) 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. State agencies;
2. Regional councils of governments;
3. Units of local government;
4. Nonprofit organizations;
5. Universities or Colleges; and
6. Federally recognized Native American tribes.

Application Process

Applicants must access the Office of the Governor's eGrants website at https://eGrants.gov.texas.gov to register and apply for funding.

1. For eligible local and regional projects:

a. Applicants must contact their applicable regional council of governments (COG) regarding their application.

b. Each of Texas' 24 COGs holds its own application planning workshops, workgroups, and/or subcommittees and facilitates application prioritization for certain programs within its region. Failure to comply with regional requirements imposed by the COG may render an application ineligible.

2. State agencies, and other organizations proposing projects to increase preparedness statewide, may submit applications directly to HSGD.

Note for All Applicants: Applicants must upload the required Texas Direct Deposit Authorization Form, Texas Application for Payee Identification Number Form, and IRS W9 Form for each application prior to submission. The eGrants system will not allow an application submission until these forms are attached to the application. These forms are available at https://egrants.gov.texas.gov/updates.aspx under the Financial Management section of "Forms and Guides" or by clicking on the hyperlink above.

Key Dates

Action	Date
Funding Announcement Release	12/13/2019
Online System Opening Date	12/13/2019
Final Date to Submit and Certify an Application	2/27/2020 at 5:00pm CST

Project Period

Projects selected for funding must begin between September 1, 2020 and March 1, 2021, and expire on or before August 31, 2022. 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. HSGD 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. However, HSGD uses a risk-based formula to determine regional allocations. Local agencies should contact their regional COG for amounts historically available to the region and any maximum established by their COG. Additionally, HSGD expects to make available approximately $1.6 million to state agencies in support of 10 – 12 projects under this solicitation and the SHSP-LETPA solicitation.

Match Requirement: None

Standards

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

Eligible Activities and Costs

1. Grant projects must be submitted in support of one of the following approved activity areas:
    a. **Critical Infrastructure**
        i. Implementing target hardening and other measures associated with increased security at critical infrastructure sites including backfill and overtime to staff emergency operations centers and contracted security at critical infrastructure sites.
        ii. Identifying critical infrastructure, collecting and maintaining data, and prioritizing critical infrastructure assets, clusters, and systems.
        iii. Assessing critical infrastructure vulnerabilities and interdependencies, particularly those involving multiple sites and/or sectors.
        iv. Planning, training, exercises, equipment, and modeling enabling responsible jurisdictions to mitigate threats to and vulnerabilities of critical infrastructure facilities, assets, networks, and systems.
        v. Analyzing critical infrastructure threats and information sharing with private sector partners.
        vi. Enhancing public awareness education and communications and increasing reporting of suspicious activities related to critical infrastructure.
    b. **Cybersecurity**
        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.
        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.
    c. **Intelligence and Information Sharing** (Note: Only non-Fusion Center requests may be submitted under the SHSP-Regular solicitation. Fusion Center projects should refer to the SHSP-Law Enforcement Terrorism Prevention Activities (LETPA) solicitation.)
        i. Identifying, developing, providing, and sharing timely, accurate, and actionable information, data, or knowledge among government or private sector entities.
        ii. 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.

iii. 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.

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

v. Implementing and maintaining suspicious activity reporting initiatives.

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

d. **Interoperable Emergency Communications**

i. Building capabilities to meet P-25 standards.

ii. Sustaining existing capabilities (e.g. life cycle replacement of equipment).

iii. 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. ***Note:*** *Projects to increase voice communications interoperability for counties with the lowest interoperability levels are preferred over other types of communications projects.*

iv. 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. ***Note:*** *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.*

e. **Operational Coordination**

i. Establishing and maintaining a unified and coordinated operational structure and process that integrates critical stakeholders across and among all levels of government and with critical private and nonprofit sectors to protect against potential threats, conduct law enforcement investigations, or engage in enforcement, protective, and response activities.

ii. Implementing WebEOC and other situational awareness and decision support tools.

iii. Enhancing emergency operations centers.

iv. Conducting or participating in incident management training and/or exercises.

f. **State, Regional and Local Planning**

i. Developing state and regional risk and preparedness assessments, including those related to special events.

ii. Core capability development planning, to include typing and tracking of equipment and special response teams.

iii. Planning and execution of training and exercises focused on terrorism prevention, protection and response.

iv. Multi-jurisdictional operational planning to include plans for regional operational coordination of terrorism prevention, protection, and response capabilities.

v. Maintaining or updating Emergency Operations Plans, consistent with guidance in CPG 101.v2 and the whole community approach to security and emergency management.

vi. Planning and implementation of initiatives to enhance the Citizen Corps Program and other community resilience initiatives.

vii. Planning for continuity of operations.

g. **Sustaining Special Response Teams and First Responder Capabilities**

i. Sustaining and enhancing capacity to detect and resolve threats involving chemical, biological, radiological, nuclear and explosive (CBRNE) devices or weapons of mass destruction (WMD).

ii. Sustaining and enhancing tactical teams including HAZMAT response and decontamination, Urban Search and Rescue, and SWAT.

iii. Sustaining equipment needs, including personal protective equipment, WMD pharmaceuticals, calibration and maintenance for WMD-related detection and identification systems, and closely related investments to update or sustain current equipment.

iv. Sustaining and enhancing efforts to delay, divert, intercept, halt, apprehend, or secure threats or hazards (includes capabilities related to Border Security).

v. Coordinating regional training exercises with federal, state and local law enforcement participation focused on responding to terrorism-related events and increasing participation with community and business organizations.

vi. Identifying or locating terrorists through active and passive surveillance and search procedures including systematic examinations and assessments, bio-surveillance, sensor technologies, or physical investigation and intelligence.

Program-Specific Requirements

1. All capabilities being built or sustained must have a clear link to one or more Core Capabilities in the National Preparedness Goal.
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 SHSP must support terrorism preparedness by building or sustaining capabilities that relate to the prevention of, protection from, mitigation of, response to, and/or recovery from 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 and must be at least at the Intermediate Level. 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 2020 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. Entities receiving funds from HSGD 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.
2. Beginning January 1, 2020, counties applying for grant awards from the Office of the Governor must commit that the county will report at least 90 percent of convictions within seven business days to the Criminal Justice Information System at the Department of Public Safety. By January 1, 2021, such reporting must take place within five business days.
3. Eligible applicants operating a law enforcement agency must be current on reporting Part I violent crime data to the Texas Department of Public Safety (DPS) for inclusion in the annual Uniform Crime Report (UCR). 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.
4. The Texas Department of Public Safety (DPS) has established a goal set by the Texas Legislature for all local law enforcement agencies to implement and report crime statistics data by using the requirements of the National Incident-Based Reporting System (NIBRS). Additionally, the Federal Bureau of Investigations (FBI) will collect required crime statistics solely through the NIBRS starting January 1, 2021. Due to the upcoming federal deadline, grantees are advised that eligibility for future grant funding may be tied to compliance with NIBRS. Financial grant assistance for transitioning to NIBRS may be available for your jurisdiction from the Public Safety Office.
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/.

Failure to comply with program or eligibility requirements may cause funds to be withheld and/or suspension or termination of grant funds.

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. admission fees or tickets to any amusement park, recreational activity or sporting event;
7. promotional gifts;
8. food, meals, beverages, or other refreshments, except for eligible per diem associated with grant-related travel or where pre-approved for working events;
9. membership dues for individuals;
10. any expense or service that is readily available at no cost to the grant project;
11. any use of grant funds to replace (supplant) funds that have been budgeted for the same purpose through non-grant sources;
12. fundraising;
13. legal services for adult offenders;
14. amateur radios and equipment, FMS radios, GMRS radios, or other radio equipment that is not P25 compliant;
15. riot equipment including but not limited to shields, batons, less-lethal ammunition, and grenades designed or intended for dispersing crowds;
16. 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; 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.

1. **Peer/Merit Review:** For eligible local and regional projects:
    a. Each COG's homeland security advisory committee will prioritize all eligible applications using the region's risk-informed methodology.
    b. HSGD will accept priority listings that are approved by the COG's executive committee.
    c. HSGD will make all final funding decisions based on eligibility, COG priorities, reasonableness, availability of funding, and cost-effectiveness.
2. For statewide discretionary projects, applications will be reviewed by HSGD staff members or a review group selected by the executive director. The qualitative scores from the review team will be one factor used during HSGD's prioritization of the statewide projects.

Final Decisions – All Projects: The executive director will consider rankings along with other factors and make all final funding decisions. Other factors may include cost effectiveness, overall funds availability, HSGD or state government priorities and strategies, legislative directives, need, geographic distribution, balance of focuses and approaches, 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, HSGD 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.