Name:

State Homeland Security Program – Regular Projects (SHSP-R), Federal Fiscal Year 2025

Available
12/16/2024

Due Date
02/13/2025

Purpose:

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

This funding supports 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 State Homeland Security Program (SHSP) is intended to support investments that improve the ability of jurisdictions to:

- **Prevent** a threatened or 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.**

Note for Cybersecurity Applicants: Projects seeking to design and implement efforts to address imminent cybersecurity threats to local information systems should refer to the State and Local Cybersecurity Grant Program (SLCGP) Announcements available on the *Funding Opportunities* page in eGrants.

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 PSO's eGrants grant management website at https://eGrants.gov.texas.gov to register and apply for funding.

1. For eligible local and regional projects:

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

Key Dates:

Action	Date
Funding Anouncemtent Release	12/16/2024
Online System Opening Date	12/16/2024
Final Date to Submit and Certify an Application	02/13/2025 at 5:00PM CST
Earliest Project Start Date	09/01/2025

Project Period:

Projects selected for funding must begin between September 1, 2025 and March 1, 2026, and expire on or before August 31, 2027. 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: $10,000

Maximum: None. However, PSO 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, PSO expects to make available approximately $1.5 - $2 million to state agencies in support of 10 – 15 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 Texas Grant Management Standards (TxGMS), Federal Uniform Grant Guidance, and all statutes, requirements, and guidelines applicable to this funding.

Eligible Activities and Costs

1. The Federal Emergency Management Agency (FEMA) has established National Priority Areas (NPA) for the Homeland Security Grant Program and requires the State to dedicate at least 30% of Texas' SHSP funds to projects under the NPAs. The NPAs and prescribed amounts for each NPA are noted below. PSO anticipates these priorities will remain in place for the 2024 SHSP grant cycle. Applicants are encouraged to submit projects under these National Priority Areas when the primary core capability addressed is consistent with a National Priority Area description below. Note: The National Priority Areas are subject to change without notice upon release of the federal Notice of Funding Opportunity (NOFO).

2. Grant projects must be submitted in support of one of the following approved activity areas:

a. Community Preparedness and Resilience (NPA)

- **Core Capabilities:** Planning; Public Information and Warning; Community Resilience; Mass Care Services; Risk and Disaster Resilience Assessment; Long Term Vulnerability Reduction.
  - Projects supporting training and equipping regional and local Citizen Corps Programs (CCP) including Community Emergency Response Teams (CERT).
  - Provide continuity training, such as FEMA's Organizations Preparing for Emergency Needs training to faith-based organizations, local businesses, and community-based organizations including homeless shelters, food pantries, nonprofit medical providers, and senior care facilities to bolster their resilience to all hazards.
  - Community Mapping: identify community resources and characteristics in order to identify gaps in resources, identify hazards and vulnerabilities, and inform action to promote resilience.

b. Emergency Operations Centers and Technology

- 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.
- Implementing WebEOC and other situational awareness and decision support tools.
- Enhancing emergency operations centers.
- Conducting or participating in incident management training and/or exercises.

c. Information and Intelligence Sharing/Cooperation (NPA)

(Note: Applicants should submit Fusion Center projects under the Law Enforcement Terrorism Prevention Activities (LETPA) solicitation.)

- **Core Capability:** Intelligence and Information Sharing

- 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.
- Cooperation with DHS officials and other entities designated by DHS in intelligence, threat recognition and analysis.
- Joint training and planning with DHS officials and other entities designated by DHS.
- 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.
- 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.
- Assessing threat information to inform continued prevention operations and ongoing response activities.
- Implementing and maintaining suspicious activity reporting initiatives.
- Implementing or sustaining public information and warning systems to relay information regarding terrorism threats.

d. Interoperable Emergency Communications

- Building capabilities to meet P-25 standards.
- Sustaining existing capabilities (e.g. life cycle replacement of equipment).
- 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.*
- 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. Planning

- Developing state and regional risk and preparedness assessments, including those related to special events.
- Core capability development planning, to include typing and tracking of equipment and special response teams.

- Planning and execution of training and exercises focused on terrorism prevention, protection and response.
- Multi-jurisdictional operational planning to include plans for regional operational coordination of terrorism prevention, protection, and response capabilities.
- Maintaining or updating Emergency Operations Plans, consistent with guidance in CPG 101.v2 and the whole community approach to security and emergency management.
- Planning and implementation of initiatives to enhance the Citizen Corps Program and other community resilience initiatives.
- Planning for continuity of operations.

f. Protection of Soft Targets/Crowded Places (NPA)

- **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
  - 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.
  - Assessing critical infrastructure vulnerabilities and interdependencies, particularly those involving multiple sites and/or sectors.
  - Planning, training, exercises, equipment, and modeling enabling responsible jurisdictions to mitigate threats to and vulnerabilities of critical infrastructure facilities, assets, networks, and systems.
  - Analyzing critical infrastructure threats and information sharing with private sector partners.
  - Enhancing public awareness, education and communications, and increasing reporting of suspicious activities related to critical infrastructure.

g. Support of First Responder Capabilities

Note: Because there is the potential for significant overlap between this activity area and the FEMA National Priorities, applicants should first check whether their proposed project is consistent with the description and core capabilities outlined for the National Priority Areas.

- Sustaining and enhancing capacity to detect and resolve threats involving chemical, biological, radiological, nuclear and explosive (CBRNE) devices or weapons of mass destruction (WMD).
- Sustaining and enhancing tactical teams including HAZMAT response and decontamination, Urban Search and Rescue, and SWAT.
- 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.
- Sustaining and enhancing efforts to delay, divert, intercept, halt, apprehend, or secure threats or hazards (includes capabilities related to Border Security).
- 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.
- 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.

h. Combating Domestic Violent Extremism (NPA)

- **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
  - 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, SAR indicators and behaviors) to educate the public on misinformation and disinformation campaigns and resources to help them identify and report potential instances of domestic violent extremism.

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 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.

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. The 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.

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 five business days to the Criminal Justice Information System at the Department of Public Safety.

3. 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.

4. In accordance with Texas Government Code, Section 420.034, any facility or entity that collects evidence for sexual assault or other sex offenses or investigates or prosecutes a sexual assault or other sex offense for which evidence has been collected, must participate in the statewide electronic tracking system developed and implemented by the Texas Department of Public Safety. Visit DPS's Sexual Assault Evidence Tracking Program website for more information or to set up an account to begin participating. Additionally, per Section 420.042 "A law enforcement agency that receives evidence of a sexual assault or other sex offense...shall submit that evidence to a public accredited crime laboratory for analysis no later than the 30th day after the date on which that evidence was received." A law enforcement agency in possession of a significant number of Sexual Assault Evidence Kits (SAEK) where the 30-day window has passed may be considered noncompliant.

5. Eligible applicants must be registered in the federal System for Award Management (SAM) database and have an UEI (Unique Entity ID) number assigned to its agency (to get registered in the SAM database and request an UEI number, go to https://sam.gov/)

Failure to comply with program 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. weapons accessories to include but not limited to optics/sights, laser aiming devices, ammunition pouches, slings, firearm silencers, bayonets, rifle bags 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 items 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, Mobile ad hoc networks (MANETs), 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: PSO will screen all applications to ensure that they meet the requirements included in the funding announcement.

1. For eligible local and regional projects:

- Each COG's homeland security advisory committee will prioritize all eligible applications using the region's risk-informed methodology.
- PSO will accept priority listings that are approved by the COG's executive committee.
- PSO will make all final funding decisions based on eligibility, FEMA National Priorities, COG priorities, reasonableness, availability of funding, and cost-effectiveness.

2. For statewide discretionary projects, applications will be reviewed by PSO staff members or a review group selected by the executive director. PSO will make all final funding decisions based on eligibility, reasonableness, availability of funding, and cost-effectiveness.

3. The State must designate at least 30% of available SHSP funding to projects supporting the FEMA NPAs listed above as outlined in the FY 2024 HSGP guidance. PSO encourages the COG regions to solicit projects to support each of the NPAs listed in this solicitation.

PSO 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.

Total Funds

$TBD