



Office of the Governor, Public Safety Office
Homeland Security Grants Division
Funding Announcement: **2022 State Homeland Security Program – Competitive National Priority Area Projects (SHSP-NPA)**

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. **Funding under this announcement will be awarded on a competitive basis for projects aimed at Combating Domestic Violence Extremism and Enhancing Cybersecurity as described below.**

The purpose of this funding is to support state, tribal and local preparedness activities that address national and state-priority preparedness gaps across selected 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 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). 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 PSO’s eGrants grant management website at <https://eGrants.gov.texas.gov> to register and apply for funding. For more instructions and information, see the OOG’s *eGrants User Guide to Creating an Application*, available [here](#).

Key Dates

Action	Date
Funding Announcement Release	12/13/2021
Online System Opening Date	12/13/2021
Final Date to Submit and Certify an Application	2/10/2021 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.

PSO expects to set-aside at least 15% of available SHSP funding for projects under this funding announcement. This amount is estimated to be \$3 million.

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 required the State to dedicate at least 15% of Texas’ SHSP funds to projects under the NPAs noted below. Applicants are encouraged to submit projects under these NPAs when the primary core capability addressed is consistent with a NPA 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 NPAs:

a. **Combating Domestic Violent Extremism (\$1.5 million estimated available)**

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.

b. **Enhancing Cybersecurity (\$1.5 million estimated available)**

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 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.

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.
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.

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.
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. 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>).
5. 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. weapons accessories to include but not limited to optics/sights, laser aiming devices, ammunition pouches, slings, 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, 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. **Peer/Merit Review:** PSO staff members and a review group selected by the executive director will prioritize applications.
2. Only projects in the Combating Domestic Violent Extremism and the Enhancing Cybersecurity NPAs will be considered under this solicitation. Projects for other NPAs should be submitted for consideration under the SHSP Regular or LETPA solicitations.

Final Decisions – All Projects: The executive director will consider the outcomes of the merit review along with other factors and make all final funding decisions. Other factors may include cost effectiveness, overall funds availability, PSO or state government priorities and strategies, legislative directives, need, geographic distribution, or other relevant factors.

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.

All projects submitted under the FEMA NPAs and selected for award by PSO will undergo an enhanced effectiveness review by FEMA for final approval prior release of any funds.

Contact Information

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