Name:

Urban Area Security Initiative Federal Fiscal Year 2026 – Regular Projects (UASI-R) - AMENDED

Available
03/02/2026

Due Date
04/30/2026

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.

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, protect against, mitigate, respond to, and recover from acts of terrorism. 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 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;
- **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 UASI 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). 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 2026 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, the Austin Area and the San Antonio Area.

2. Applications from the following entities will be considered*:State agencies;

- Regional councils of governments;
- Units of local government;
- Nonprofit organizations; and
- 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 their 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 region. Failure to comply with requirements imposed by the UAWG may render an application ineligible.

Upon approval of the UAWG, eligible applicants must access PSO's eGrants grant management website at https://eGrants.gov.texas.gov to register and continue the application process.

*****NEW APPLICATION SUBMISSION REQUIREMENT*****

The following documents must be submitted with the application for the application to be considered complete and eligible for funding. See the Eligibility Requirements and/or Program-Specific Requirements Sections of this Funding Announcement for more details on the requirements for each attachment/certification:

- **Resolution from Governing Body** - Applications from nonprofit corporations, local units of governments, and other political subdivisions must submit a fully executed resolution.
- **CEO/Law Enforcement Certifications and Assurances Form** - Each local unit of government, and institution of higher education that operates a law enforcement agency, must certify compliance with federal and state immigration enforcement requirements.
- **CEO/NGO Certification and Assurances Form –** Each non-profit organization must certify compliance with federal and state immigration enforcement requirements.

Key Dates:

Action	Date
Funding Anouncemtent Release	03/02/2026
Online System Opening Date	03/02/2026
Final Date to Submit and Certify an Application	04/30/2026 at 5:00PM CST
Earliest Project Start Date	09/01/2026

Project Period:

Projects selected for funding must begin between September 1, 2026 and March 1, 2027, and expire on or before August 31, 2028. Additional guidelines are below:

1. PSO prefers project periods 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. PSO prefers project periods 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. PSO prefers project periods for equipment only projects are generally be awarded 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.

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 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 (UAWG) for an updated list of investment categories.

2. The Federal Emergency Management Agency (FEMA) has established National Priority Areas (NPA) for the Homeland Security Grant Program and requires designated Urban Areas to dedicate at least

30% of allocated 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 2026 UASI 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). The required National Priority Areas and examples of projects include:

a. 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.

b. Enhancing Elections Security (NPA, Required to fund at least 3%)

- **Core Capabilities:** Cybersecurity; Intelligence and Information Sharing; Planning; Long-term Vulnerability Reduction; Situational Assessment; Infrastructure Systems
  - Physical security planning support.
  - Physical/site security measures – e.g., locks, shatter proof glass, alarms, etc. for elections infrastructure.
  - General election security navigator support.
  - Cyber navigator support
  - Cybersecurity risk assessments, training, and planning for elections systems.
  - Projects that address vulnerabilities identified in cybersecurity risk assessments of elections systems.
  - Iterative backups, encrypted backups, network segmentation, software to monitor/scan, and endpoint protection.
  - Distributed Denial of Service protection.
  - Migrating online services to the ".gov" internet domain.
  - Online harassment and targeting prevention services.
  - Public awareness/preparedness campaigns discussing election security and integrity measures

c. Enhancing Cybersecurity (NPA)

- **Core Capabilities:** Cybersecurity; Intelligence and Information Sharing

- Assessing organizational cybersecurity risk and potential risk.
- Creating or updating strategic cybersecurity plans and related response and recovery plans and exercises.
- Developing approaches for identifying, authenticating, and authorizing individuals to access an organization's assets and systems.
- Purchasing software such as anti-virus, anti-malware, continuous monitoring, encryption, enhanced remote authentication, patch management or distributed denial of service protection.
- Purchasing hardware such as intrusion detection systems, firewalls, additional servers, routers or switches for the purpose of reducing cybersecurity vulnerabilities.
- Implementing awareness and training measures.
- Establishing anomalous activity detection and system/asset monitoring.
- Developing or sustaining response activities, including information sharing or other mitigation efforts.
- 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. Supporting Homeland Security Task Forces and Fusion Centers (NPA)

- **Core Capabilities:** Intelligence and Information Sharing, Interdiction and Disruption, Public information and Warning, Operational Coordination, Risk Management for Protection Programs and Activities
  - Establishing or enhancing multi-agency Homeland Security Task Forces (HSTFs), including operational coordination centers
  - Enhancing capabilities and integration with local fusion centers
  - Procurement of technology or equipment to support surveillance, communications, and data analysis
  - Development of standard operating procedures for information sharing, joint operations, and immigration enforcement coordination
  - Personnel training, credentialing, and certification to improve interoperability and mission alignment
  - Intelligence analysis, reporting, and suspicious activity monitoring
  - Exercises and simulations focused on joint operations, intelligence sharing, or interdiction/disruption of criminal or smuggling networks
  - Community engagement efforts to foster trust and encourage threat reporting
  - Information sharing with all DHS components; fusion centers; other operational, investigative, and analytic entities; and other federal law enforcement and intelligence entities
  - Cooperation with DHS and other entities in intelligence, threat recognition, assessment, analysis, and mitigation
  - Identification, assessment, and reporting of threats of violence
  - Intelligence analysis training, planning, and exercises
  - Coordinating the intake, triage, analysis, and reporting of tips/ leads and suspicious activity, to include coordination with the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI).

e. Supporting Border Crisis Response and Enforcement (NPA - Required to fund at least 10%)

- **Core Capabilities:** Risk management for protection programs and activities; Operational coordination; Community resilience
  - Staffing support to expand 287(g) screening operations within corrections facilities
  - Operational overtime costs directly tied to 287(g) screening, processing, and enforcement activities.
  - Training programs for state and local law enforcement officers in immigration law, civil rights protections, and 287(g) procedures.
  - Development or enhancement of information-sharing platforms between ICE and local agencies.
  - Procurement of screening, detection, and communications technology to support immigration enforcement activities.
  - Establishing secure and dedicated communications networks with ICE Field Offices.
  - Conducting joint training exercises with ICE and local law enforcement to test operational coordination.
  - Support for facilities upgrades, such as creating dedicated interview rooms and secure processing spaces.
  - Community engagement and public briefings to promote transparency and understanding of 287(g) operations and protections.
  - Other jurisdictional responsibilities to support the enforcement of United States immigration law.

3. 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. 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.*

4. 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.

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**.**
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. Law Enforcement

Terrorism Prevention Activities implemented under SHSP 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 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. Applications from nonprofit corporations, local units of governments, and other political subdivisions must submit a fully executed resolution with the application to be considered eligible for funding. The resolution must contain the following elements (see Sample Resolution):

- Authorization by your governing body for the submission of the application to the Public Safety Office (PSO) that clearly identifies the name of the project for which funding is requested;
- A commitment to provide all applicable matching funds;
- A designation of the name and/or title of an authorized official who is given the authority to apply for, accept, reject, alter, or terminate a grant;
- A designation of the name and/or title of a financial officer who is given the authority to submit financial and/or performance reports or alter a grant; and
- A written assurance that, in the event of loss or misuse of grant funds, the governing body will return all funds to PSO

2. 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.

3. 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% 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. 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.

6. Local units of government, including cities, counties and other general purpose political subdivisions, as appropriate, and institutions of higher education that operate a law enforcement agency, must comply with all aspects of the programs and procedures utilized by the U.S. Department of Homeland Security ("DHS") to: (1) notify DHS of all information requested by DHS related to illegal aliens in Agency's custody; and (2) detain such illegal aliens in accordance with requests by DHS. Additionally, counties and municipalities may NOT have in effect, purport to have in effect, or make themselves subject to or bound by, any law, rule, policy, or practice (written or unwritten) that would: (1) require or authorize the public disclosure of federal law enforcement information in order to conceal, harbor, or shield from detection fugitives from justice or aliens illegally in the United States, 8 U.S.C. § 1324(a)(1)(A)(iii); (2) impede federal officers from exercising authority under 8 U.S.C. § 1226(a), § 1226(c), § 1231(a), § 1357(a), § 1366(1), or § 1366(3); (3) encourage or induce an alien to come to, enter, or reside in the United States in violation of law, 8 U.S.C. § 1324(a)(1)(A)(iv); (4) result in the illegal transport or movement of aliens within the United States, 8 U.S.C. § 1324(a)(1)(A)(ii) . Lastly, eligible applicants must comply with all provisions, policies, and penalties found in Chapter 752, Subchapter C of the Texas Government Code.

Each local unit of government, and institution of higher education that operates a law enforcement agency, must download, complete and then upload into eGrants the CEO/Law Enforcement Certifications and Assurances Form certifying compliance with federal and state immigration

enforcement requirements. This Form is required for each application submitted to OOG and is active until August 31, 2027 or the end of the grant period, whichever is later.

7. Each non-profit 501(c)(3) organization must certify that it does not have, and will continue not to have any policy, procedure, or agreement (written or unwritten) that in any way encourages, induces, entices, or aids any violations of immigration laws. Additionally, the organization certifies that it does not have in effect, purport to have in effect, and is not subject to or bound by any rule, policy, or practice (written or unwritten) that would: (1) encourage the concealment, harboring, or shielding from detection of fugitives from justice or aliens who illegally came to, entered, or remained in the United States, 8 U.S.C. § 1324(a)(1)(A)(iii), or (2) impede federal officers from exercising authority under 8 U.S.C. § 1226(a), § 1226(c), § 1231(a), § 1357(a), § 1366(1), or § 1366(3); (3) encourage or induce an alien to come to, enter, or reside in the United States in violation of law, 8 U.S.C. § 1324(a)(1)(A)(iv); (4) result in the illegal transport or movement of aliens within the United States, 8 U.S.C. § 1324(a)(1)(A)(ii). Lastly, the organization certifies that it will not adopt, enforce, or endorse a policy which prohibits or materially limits the enforcement of immigration laws, and will not, as demonstrated by pattern or practice, prohibit or materially limit the enforcement of immigration laws.

Each non-profit organization must download, complete and then upload into eGrants the CEO/NGO Certifications and Assurances Form Certifying compliance with federal and state immigration enforcement requirements.

8. 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, 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 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.

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.

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