



**New Mexico Department of Homeland Security & Emergency Management (DHSEM)
2026 State Homeland Security Grant Program (SHSGP)
Funding Announcement and Allocation Methodology**

Issued By: NM Department of Homeland Security and Emergency Management

Assistance Listings Number: 97.067

Assistance Listings Title: State Homeland Security Grant Program

Funding Opportunity Title: Fiscal Year 2026 State Homeland Security Grant Program (SHSGP)

Funding Opportunity Number: DHS-26-GPD-067-00-98

Authorizing Authority for Program: Section 2002 of the *Homeland Security Act of 2002*, Pub. L. No. 107-296 (codified as amended at 6 U.S.C. §603).

Appropriation Authority for Program: *Homeland Security and Further Additional Continuing Appropriations Act, 2026*, Pub. L. No. 119-86.

Announcement Type: Initial

A. PROGRAM PURPOSE

SHSGP is designed to enhance the capabilities of state, local, tribal, and territorial governments, to prevent, protect against, and respond to terrorist attacks. This program is part of a comprehensive set of measures authorized by Congress and implemented by the Department of Homeland Security (DHS) to strengthen the nation's communities against potential terrorist threats. SHSGP Supports the implementation of risk-driven, capabilities-based State Homeland Security Strategies to address capability targets and aims to strengthen the nation's ability to prevent, prepare for, protect against, and respond to acts of terrorism and other threats.

B. GOALS AND OBJECTIVES,

Goals: The goal of SHSGP is to support statewide and state, local, tribal, and territorial (SLTT) governments in building, enhancing, and sustaining the capabilities needed to prevent, prepare for, protect against, and respond to acts of terrorism. SHSGP funding is intended to help SLTT agencies address capability gaps identified through the THIRA/SPR process, as well as prioritize resources toward high-impact security focus areas, known as NPAs. SHSGP aims to build a cohesive and collaborative approach to homeland security by promoting national preparedness and resilience.

Objectives: SHSGP provides resources that support eligible SLTT governments in meeting the following objectives:

- Build and sustain core capabilities, including LETPA and the NPAs (see priorities below).
- Address capability gaps identified in their THIRA and SPR process.
- Implement a comprehensive and coordinated approach to address enduring security needs of communities that include planning, training and awareness campaigns, equipment and capital projects, and exercises.

C. FUNDING REQUIREMENTS

National Incident Management System (NIMS) Implementation: Prior to allocation of any federal preparedness awards, recipients must ensure and maintain adoption and implementation of NIMS, including implementation of important operational systems defined under NIMS, such as the Incident Command System (ICS).

Emergency Management Assistance Compact (EMAC): SHSGP subrecipients must participate in the Emergency Management Assistance Compact (EMAC). All assets supported in part or entirely with FY 2026 SHSGP funding must be readily deployable and NIMS-typed, when possible, to support emergency or disaster operations per existing EMAC agreements. In addition, funding may be used

for the sustainment of core capabilities that, while they may not be physically deployable, support national response capabilities, such as Geographic/Geospatial Information Systems, interoperable communications systems, and capabilities as defined under the Mitigation Mission Area of the Goal.

Threat Identification and Risk Assessment (THIRA) / Stakeholder Preparedness Review (SPR): Subrecipients are required to complete the THIRA every three years and the SPR annually. These assessments help jurisdictions identify and address capability gaps to enhance overall preparedness. See the [Comprehensive Preparedness Guide \(CPG\) 201, 3rd Edition](#) information on the THIRA/SPR process.

Law Enforcement Terrorism Prevention Activities (LETPA): Funding through SHSGP is aimed at enhancing law enforcement's ability to prevent terrorist attacks. These activities focus on building and sustaining capabilities in areas such as intelligence analysis, information sharing, threat recognition, and terrorist interdiction.

- Allocation Requirement: At least 35% of SHSGP allocations must be allocated to LETPA activities.
- Project Alignment: LETPA funds can be applied to projects across the NPAs or other investments that meet LETPA criteria.
- Additional Guidance: For detailed guidance on allowable LETPA expenditures and requirements, refer to FEMA's [DHS 2026 Homeland Security Grant Program Notice of Funding Opportunity \(NOFO\)](#), [Preparedness Grants Manual](#), [Information Bulletin 485](#) and [Information Bulletin 497](#).

Terrorism Nexus: Allowable investments must have a nexus to terrorism preparedness and fall into the categories of planning, organization, exercises, training, or equipment, aligned to building capability, closing capability gaps, and/or sustaining capabilities, as defined by CPG 201: THIRA/SPR Guide—3rd Edition ([Comprehensive Preparedness Guide \(CPG\) 201, 3rd Edition](#)).

National Priority Areas (NPAs): To ensure strategic focus, DHS has identified five NPAs that reflect the evolving risk landscape and national policy objectives. These priorities serve as a framework for targeting investments that build capability, reduce risk, and promote cross-sector coordination. The following are the required NPAs for FY 2026:

1. Enhancing the protection of soft targets and crowded places,
 - a. This includes faith-based organizations and election sites;
2. Supporting Homeland Security Task Forces (HSTFs) and fusion centers;
3. Enhancing and integrating cybersecurity resiliency;
4. Enhancing election security; and
5. Supporting border crisis response and enforcement.
 - a. Example activities under border crisis response and enforcement support may include:
 - i. Participation in the Department of Homeland Security/Immigration and Customs Enforcement 287(g) training program;
 - ii. Cooperation with Immigration and Customs Enforcement detainees; and
 - iii. Other jurisdictional responsibilities to support the enforcement of United State immigration law.

Allocation Requirement: Subrecipients must allocate at least 30% of their SHSGP funds to the five NPAs. Funds can be applied to projects across the five NPAs and can be used to meet LETPA criteria. By meticulously outlining how each investment and project meets LETPA and NPA requirements within the Investment Justifications (IJ), subaward applicants can enhance the effectiveness and compliance of their funding proposals. Failure to meet NPA spending requirements will result in a hold on affected funds until compliance issues are resolved.

Minimum Spend:

- Enhancing Election Security requires at least 3% of total SHSGP and UASI funds.
- Supporting Border Crisis Response and Enforcement requires at least 10% of total SHSGP funds.
- The remaining 17% can be allocated across all NPAs.

D. REQUIREMENTS FOR PERSONNEL, PARTNERS, AND OTHER PARTIES

An application submitted by an otherwise eligible non-federal entity (i.e., the applicant) may be deemed ineligible when the person that submitted the application is not:

1. A current employee, official, or leader of the recipient organization; and
2. Authorized to apply for the award on behalf of the entity at the time of submission.

Additionally, the Authorized Organization Representative (AOR) must:

1. Be a current authorized employee, official, or leader of the recipient organization.
2. Use a unique email address associated with the recipient organization at the time of application and upon any change in assignment during the period of performance.

Consultants or contractors are not permitted to serve as the AOR of the recipient organization. For more information on the roles and responsibilities of the AOR, refer to FEMA's guidance on [Roles and Permissions](#).

Subaward applicants should not have foreign nationals or noncitizens included. If a subaward applicant has foreign nationals, they must be properly vetted and must adhere to all government statutes, policies, and procedures including “staff American, stay in America” and security requirements.

Subaward applicants/subrecipients must submit short bios and resumes. This should include the type of entity, organizational leadership, and board members along with both the names and addresses of the individuals. Resumes are subject to approval.

E. INELIGIBLE FOR HSGP FUNDING

Ineligible Projects: Ineligible Projects are those that do not align with the purposes of the SHSGP, including those that fail to demonstrate a clear nexus to preventing, preparing for, protecting against, or responding to acts of terrorism. Activities not permitted under SHSGP guidance or that do not meet criteria for allowable costs as outlined in the [DHS 2026 Homeland Security Grant Program Notice of Funding Opportunity \(NOFO\)](#) and [Preparedness Grants Manual](#).

Non-SAA Organization. SAAs are the only applicants eligible to submit SHSGP applications to FEMA.

Unaffiliated or Unauthorized Representatives: Applications submitted by individuals who are not current employees, personnel, or authorized representatives of the subaward applicant organization (e.g., consultants or contractors acting on behalf of an organization) will be deemed ineligible.

Organizations Not Registered in SAM.gov: Applicants that fail to register and maintain an active profile in SAM.gov, or those without a UEI, are not eligible to receive funding.

Direct Applications by Tribal Governments: Tribal governments cannot directly apply for SHSGP funding. However, they may receive funding as subrecipients through their state's SAA.

Non-Compliance with Federal Requirements: Failure to submit a complete and accurate application by the deadline. Applications missing required documentation or information, such as active registration in SAM.gov or compliance with UEI requirements. Entities with a history of non-compliance with federal statutes, regulations, or program requirements that impact eligibility for federal funding.

E. NATIONAL PRIORITY AREAS

Enhancing and Protection of Soft Targets/Crowded Places (no minimum percentage). Soft targets and crowded places, like parks, shopping centers, transportation hubs, and event venues, are increasingly appealing to terrorists because of their accessibility and the large gatherings. These areas often lack strict security measures, making them vulnerable. To address this, public and private sectors must collaborate to strengthen the security of locations such as transportation centers, restaurants, polling places, and similar facilities. Personnel responding to incidents at these sites should also be trained in key operational systems, such as the [Incident Command System \(ICS\)](#), to ensure effective on-scene incident management. DHS/FEMA expects that national priorities will continue to be included in future years, evolving as threats change and capability gaps are addressed. Subrecipients are strongly encouraged to start planning now to sustain existing capabilities using funding sources other than DHS preparedness grants.

The malicious use of unmanned aircraft systems (i.e., drones) poses safety and security risks to soft targets and crowded places. Detecting drones is an allowable use of funds under the SHSGP in accordance with [Executive Order 14305](#), Restoring American Airspace Sovereignty, which allows the purchase of unmanned aircraft systems (UAS) or equipment or services for the detection, tracking, or identification of drones and drone signals, and FEMA [Information Bulletin 530](#).

Before purchasing and deploying these systems, as outlined in the Domestic Counter-UAS National Action Plan, recipients must:

- **Consult DHSEM and Legal Experts:** Work with DHSEM and your jurisdiction's legal experts to ensure your policies and procedures comply with federal and state laws regarding surveillance and communication.
- **Develop Standard Operating Procedures (SOPs):** Establish clear guidelines to ensure operations are conducted in a manner consistent with First and Fourth Amendment protections, and other applicable provisions of federal law.
- **Provide Training and Certification:** Ensure personnel operating UAS systems are properly trained and certified, in accordance with FEMA and Federal Aviation Administration standards.

Additional Resources: Further guidance and resources for securing soft targets and crowded places can be found through the [Cybersecurity and Infrastructure Security Agency](#) (CISA) and the [National Institute of Standards and Technology](#). For comprehensive compliance and operational details, refer to [DHS 2026 Homeland Security Grant Program Notice of Funding Opportunity \(NOFO\)](#) and [Preparedness Grants Manual](#) for more information.

Supporting Homeland Security Task Forces (HSTFs) and Fusion Centers (no minimum percentage). This priority supports the Administration's direction under [Executive Order 14159](#), Protecting the American People Against Invasion, which calls for the establishment of Homeland Security Task Forces (HSTFs) nationwide. These multi-agency teams, composed of federal and local law enforcement partners—are tasked with disrupting and dismantling transnational criminal organizations, targeting cross-border human smuggling and trafficking networks (especially those involving children), and using all appropriate law enforcement tools to support lawful immigration enforcement. Activities under this NPA also enhance broader national efforts in:

- Counterterrorism;
- Cybersecurity;
- Border security;
- Immigration enforcement;
- Transnational organized crime; and
- Protection of economic and critical infrastructure

Allowable HSTFs and Fusion Center Costs: Subrecipients may use grant funds for the following.

- Establishing or enhancing multi-agency HSTFs, including operational coordination centers
- Enhancing capabilities and integration with local fusion centers;
- Procuring technology or equipment to support surveillance, communications, and data analysis;
- Developing 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; and
- Community engagement efforts to foster trust and encourage threat reporting.

Cybersecurity (no minimum percentage). In today's interconnected world, increased connectivity brings greater risks, including the potential for adversaries and terrorists to exploit cyber vulnerabilities and disrupt critical systems. Cybersecurity investments should enhance the security and functioning of critical infrastructure and core capabilities related to preventing, preparing for, protecting against, or responding to acts of terrorism.

Election Security (3% minimum allocation). Securing election infrastructure, ensuring its continued operation in the face of threats and harassment, advancing the safety of election officials, and protecting against foreign interference are national security priorities. Because threats to election systems are constantly evolving, defending these systems requires constant vigilance, innovation, and adaptation. By integrating the directives of [Executive Order 14248](#), Preserving and Protection the Integrity of American Elections, into the Election Security NPA, SHSGP subrecipients can ensure that their efforts contribute to a secure, transparent, and resilient electoral process, thereby reinforcing public trust and the integrity of democratic institutions. To address these priorities, subaward applicant must make at least one investment that supports physical and/or cyber election security. Proposed investments must meet or exceed the FY 2026 national priority percentage for election security (minimum 3%) and will be evaluated by DHS/FEMA for effectiveness and alignment with program goals.

To strengthen the integrity of U.S. elections, each state and high-risk urban area election jurisdiction must:

- Submit a transition plan: Submit a plan for transitioning from electronic voting systems that utilize bar codes or QR codes to count votes to equipment that accepts hand-marked paper ballots. The plan for all jurisdictions currently using such systems, must include a timeline and, if necessary, a funding request to eliminate ballot marking devices and utilize hand-marked paper ballots.
- Post-election manual audit: Demonstrate proof of compliance with a post-election 5% manual audit, conducted according to the guidelines established by the Secretary, to ensure that electronic voting systems accurately count votes.
- Voter/ballot reconciliation: Ensure that each election jurisdiction reconciles the number of voters who voted in each federal election to the number of ballots cast, using the methodology established by the Secretary.
- Voter roll citizenship verification: Utilize the U.S. Citizenship and Immigration Services' Systematic Alien Verification for Entitlements (SAVE) system to verify the citizenship of all individuals in the state voter registration database within 120 days of accepting the grant award*. To mitigate operational vulnerabilities exploitable by terrorist or foreign actors and advance HSGP counterterrorism objectives, the State's chief election official must take timely corrective action, consistent with applicable law, to remove verified non-U.S. citizens from the database.

Utilize the SAVE system, or another authorized government system, to verify U.S. citizenship for any person working at a polling place in any capacity, or operating any election system in the jurisdiction, including temporary agency workers and vendors who work on or with election systems. To prevent sabotage, infiltration, or foreign interference, the State's chief election official must ensure verified non-U.S. citizens are prohibited from operating election systems or working at polling places, consistent with applicable law, thereby hardening critical infrastructure under HSGP. Additional resources and information regarding election security are available through the [Cybersecurity and Infrastructure Security Agency](#).

Supporting Border Crisis Response and Enforcement (10% minimum allocation). State and local law enforcement agencies are essential partners in safeguarding national security and public safety. Pursuant to [Executive Order 14159, Protecting the American People Against Invasion](#), it is the policy of the United States to enforce immigration laws against all inadmissible and removable aliens—particularly those who threaten the safety or security of the American people. This includes the efficient execution of these laws through lawful incentives and enhanced detention capabilities. This NPA supports efforts that align with this policy and promote cooperation between local and federal partners. Projects may include, but are not limited to:

- Participation in the [DHS/ICE 287\(g\) program](#), allowing trained local officers to support ICE with immigration enforcement.
 - Cooperation with ICE detainers and other jurisdictional responsibilities related to immigration enforcement; and
 - Supportive activities such as officer training, technology and information sharing, operational support, and community engagement.

At least one investment must support efforts under this NPA. Subaward applicants must allocate at least 10% of total SHSGP funds to this area. All investments will be reviewed by DHS/FEMA to ensure they are effective, lawful, and aligned with program goals. The SAA must coordinate with ICE on all projects and related matters. Additional guidance and information on the 287(g) program are available through the [ICE 287\(g\) program website](#).

Enduring Needs: There are several enduring security needs that crosscut the homeland security enterprise to which recipients should consider allocating funding across core capability gaps and national priorities. The following are enduring needs that help recipients implement a comprehensive approach to securing communities:

- Effective planning (Including assessment of critical infrastructure system vulnerabilities and plans to reduce consequences of disruptions, using the Infrastructure Resilience Planning Framework and Regional Resiliency Assessment Methodology produced by the Cybersecurity and Infrastructure Security Agency);
- Training and awareness campaigns;
- Equipment and capital projects; and
- Exercises.

F. ALLOWABLE COSTS

Subrecipients must comply with all the requirements in [2 C.F.R. Part 200 Uniform Administrative Requirements; Cost Principles; and Audit Requirements for Federal Awards](#). In general, recipients should consult with DHSEM before making any investment that does not clearly meet the allowable expense criteria. Funding guidelines established within this section support four of the five mission areas—Prevention, Protection, Mitigation, and Response—and associated core capabilities within the National Preparedness Goal (Goal). While Recovery is part of the Goal, it is not explicitly part of SHSGP.

Planning: SHSGP funds may be used for a range of emergency preparedness and management planning activities, such as those associated with the development, review, and revision of the THIRA, SPR, continuity plans, and other planning activities that support the Goal and placing an emphasis on updating and maintaining a current Emergency Operations Plan (EOP) that conforms to the guidelines outlined in [Comprehensive Preparedness Guide \(CPG\) 101 v3](#). Planning efforts can also include conducting risk and resilience assessments on increasingly connected cyber and physical systems, on which security depends, using the [Infrastructure Resilience Planning Framework](#) and related CISA resources. Additionally, SHSP funds may be used for planning efforts related to state court cybersecurity, 911 call capabilities, alert and warning capabilities, and implementation of the REAL ID Act (Pub. L. No. 109-13).

Organization: Organization costs are allowed under this program only as described in the [DHS 2026 Homeland Security Grant Program Notice of Funding Opportunity \(NOFO\)](#) and [Preparedness Grants Manual](#). Subaward applications must justify proposed expenditures of SHSP funds to support organization activities within their IJ submission. Organizational activities include:

1. Program management.
2. Development of whole community partnerships, through groups such as Citizen Corp Councils.
3. Structures and mechanisms for information-sharing between the public and private sector.
4. Implementing models, programs, and workforce enhancement initiatives to address ideologically inspired radicalization to violence in the homeland.
5. Tools, resources, and activities that facilitate shared situational awareness between the public and private sectors.
6. Operational Support.
7. Utilizing standardized resource management concepts such as typing, inventorying, organizing, and tracking to facilitate the dispatch, deployment, and recovery of resources before, during, and after an incident.
8. Responding to an increase in the threat level under the NTAS or needs resulting from a National Special Security Event.
9. Paying salaries and benefits for personnel to serve as qualified Intelligence Analysts. Per the Personnel Reimbursement for Intelligence Cooperation and Enhancement of Homeland Security Act (PRICE Act), Pub. L. No. 110-412, § 2, codified in relevant part, as amended, at 6 U.S.C. § 609(a), SHSGP funds may be used to hire new staff and/or contractor positions to serve as intelligence analysts to enable information/intelligence sharing capabilities, as well as support existing intelligence analysts previously covered by SHSGP funding. See 6 U.S.C. § 609(a). To be hired as an intelligence analyst, staff and/or contractor personnel must meet at least one of the following criteria:
 - a. Complete training to ensure baseline proficiency in intelligence analysis and production within six months of being hired; and/or,
 - b. Previously served as an intelligence analyst for a minimum of two years either in a federal intelligence agency, the military, or state and/or local law enforcement intelligence unit.
10. All fusion center analytical personnel must demonstrate qualifications that meet or exceed competencies identified in the [Common Competencies for state, local, and tribal intelligence analysts](#), which outlines the minimum categories of training needed for intelligence analysts. A certificate of completion of such training must be on file with DHSEM and must be made available to the recipient's respective FEMA HQ Preparedness Officer upon request; and
11. Migrating online services to the ".gov" internet domain.

Personnel: Subrecipients are allowed to use up to 50% of their SHSGP funding, for personnel costs per 6 U.S.C. § 609(b)(2)(A). Personnel hiring, overtime, and backfill expenses are permitted under this grant only to the extent that such expenses are for the allowable activities within the scope of the grant. Personnel expenses may include, but are not limited to training and exercise coordinators, program managers and planners, and intelligence analysts. At the request of a subrecipient, through DHSEM, the FEMA Administrator (or their designee) may grant a waiver of this 50% limitation under 6 U.S.C. § 609(b)(2)(B). Requests for waivers to the personnel cap must be submitted by the authorized representative of the jurisdiction in writing on official letterhead, with the following information:

1. Documentation explaining why the cap should be waived.
2. Conditions under which the request is submitted; and
3. The budget and method of calculation of personnel costs both in percentages of the grant award and in total dollar amount.

SHSGP funds may not be used to support the hiring of any personnel to fulfill traditional public health and safety duties nor to supplant traditional public health and safety positions and responsibilities.

The following definitions apply to personnel costs:

- **Hiring.** Local entities may use grant funding to cover the salary of newly hired personnel who are exclusively undertaking allowable FEMA grant activities as specified in the [Preparedness Grants Manual](#) and the [DHS 2026 Homeland Security](#)

[Grant Program Notice of Funding Opportunity \(NOFO\)](#). This may not include new personnel who are hired to fulfill any non-FEMA HSGP program activities under any circumstances. Hiring will always result in a net increase of Full Time Equivalent (FTE) employees.

- **Overtime.** These expenses are limited to the additional costs that result from personnel working over and above 40 hours of weekly work time as the direct result of their performance of FEMA-approved activities specified in this guidance. Overtime associated with any other activity is not eligible.
- **Backfill-Related Overtime.** Also called “Overtime as Backfill,” these expenses are limited to overtime costs that result from personnel who are working overtime (as identified above) to perform the duties of other personnel who are temporarily assigned to FEMA-approved activities outside their core responsibilities.
- **Supplanting.** Grant funds will be used to supplement existing funds and will not replace (supplant) funds that have been appropriated for the same purpose. Subrecipients may be required to supply documentation certifying that a reduction in non-federal resources occurred for reasons other than the receipt or expected receipt of federal funds.

Operational Overtime Costs: Supporting efforts to enhance capabilities for detecting, deterring, disrupting, and preventing acts of terrorism and other catastrophic events, operational overtime costs are allowable for increased protective security measures at critical infrastructure sites or other high-risk locations and to enhance public safety during mass gatherings and high-profile events. In that regard, HSGP recipients are urged to consider using grant funding to support soft target preparedness activities. SHSP or UASI funds may be used to support select operational expenses associated with increased security measures in the authorized categories below. FEMA retains the discretion to approve other types of requests that do not fit within one of the categories of the table. Refer to the [Preparedness Grants Manual](#) and [DHS 2026 Homeland Security Grant Program Notice of Funding Opportunity \(NOFO\)](#) for more information on authorized operational overtime costs.

Equipment: Equipment costs are allowed under this program only as described in the [Preparedness Grants Manual](#) and [DHS 2026 Homeland Security Grant Program Notice of Funding Opportunity \(NOFO\)](#). The 21 allowable prevention, protection, mitigation, and response equipment categories for SHSGP are listed on the [Authorized Equipment List](#) (AEL). Some equipment items require prior approval from FEMA before obligation or purchase of the items. Please reference the grant notes for each equipment item to ensure prior approval is not required or to ensure prior approval is obtained if necessary. Subrecipients may purchase equipment not listed on the AEL, but only if they first seek and obtain prior approval from FEMA, through DHSEM.

Unless otherwise stated, all equipment must meet all mandatory regulatory and/or FEMA-adopted standards to be eligible for purchase using these funds. In addition, subrecipients will be responsible for obtaining and maintaining all necessary certifications and licenses for the requested equipment. Investments in emergency communications systems and equipment must meet applicable SAFECOM Guidance on Emergency Communications Grants ([SAFECOM Guidance](#)) recommendations. Such investments must be coordinated with DHSEM’s Statewide Interoperability Coordinator (SWIC) and the State Interoperability Governing Body to ensure interoperability and long-term compatibility. For personal protective equipment (PPE), recipients are encouraged to give procurement preference to domestic manufacturers of PPE or PPE raw materials to the maximum practicable and allowed by law.

Grant funds may be used for the procurement of medical countermeasures. Procurement of medical countermeasures must be conducted in collaboration with state, city, or local health departments that administer federal funds from the Department of Health and Human Services for this purpose and with existing Metropolitan Medical Response System committees where available, to sustain their long-term planning for appropriate, rapid, and local medical countermeasures, including antibiotics and antidotes for nerve agents, cyanide, and other toxins. Procurement must have a sound threat-based justification with an aim to reduce the consequences of mass casualty incidents during the first crucial hours of a response. Prior to procuring pharmaceuticals, recipients must have in place an inventory management plan to avoid large periodic variations in supplies due to coinciding purchase and expiration dates. Subrecipients are encouraged to enter into rotational procurement agreements with vendors and distributors. Purchases of pharmaceuticals must include a budget for the disposal of expired drugs within each fiscal year’s Period of Performance (POP) for HSGP. The cost of disposal **cannot be carried over to another FEMA grant or grant period**. EMS electronic patient care data systems should comply with the most current data standard of the [National Emergency Medical Services Information System](#).

School hardening is an eligible activity under SHSGP. School hardening measures include but are not limited to:

1. Bullet resistant doors and glass.
2. Hinge-locking mechanisms.
3. Immediate notification to emergency 911 systems.

4. Mechanisms that provide real time actionable intelligence directly to law enforcement and first responders.
5. Installation of distraction devices or other countermeasures administered by law enforcement; and
6. Other measures are determined to provide significant improvements to schools' physical security.

SHSP funds may be used for equipment purchases related to court cybersecurity, 911 call capabilities, alert and warning capabilities, and implementation of the REAL ID Act (Pub. L. No. 109-13).

General Purpose Equipment: SHSGP allows expenditures on general purpose equipment if it aligns to and supports one or more core capabilities identified in the Goal and has a nexus to terrorism preparedness. General purpose equipment, like all equipment funded under the HSGP, must be sharable through the EMAC and allowable under 6 U.S.C. § 609, and any other applicable provision of the *Homeland Security Act of 2002*, as amended. Examples of such general-purpose equipment may include:

1. Emergency medical services, equipment and vehicles;
2. Fire service equipment and vehicles, to include hose, pump accessories, and foam
3. concentrate for specialized chemical/biological/radiological/nuclear/explosive (CBRNE) response;
4. Interoperability of data systems, such as CAD and RMS; and
5. Office equipment for staff engaged in homeland security program activity. This applies to all homeland security personnel and is not limited to M&A staff, and costs are to be captured outside the cap on M&A costs.

Construction and Renovation: Construction and renovation costs to achieve capability targets related to preventing, preparing for, protecting against, or responding to acts of terrorism are allowed under this program. For construction and renovation costs to be allowed, they must be specifically approved by DHS/FEMA, through DHSEM, in writing prior to the use of any program funds. Limits on the total amount of grant funding that may be used for construction or renovation may apply. All proposed construction and renovation activities must undergo an Environmental and Historic Preservation (EHP) review, including approval of the review from FEMA, prior to undertaking any action related to the project. Failure of a grant subrecipient to meet these requirements may jeopardize Federal funding. Please see the [Preparedness Grants Manual](#) and [DHS 2026 Homeland Security Grant Program Notice of Funding Opportunity \(NOFO\)](#) for more information.

Training and Exercises: Training and exercise costs are allowed under this program only as described in the [Preparedness Grants Manual](#) and [DHS 2026 Homeland Security Grant Program Notice of Funding Opportunity \(NOFO\)](#). Recipients are encouraged to consider tuition-free courses offered by FEMA first, before investing in training. For more information and a catalog of courses please refer to the [National Preparedness Course Catalog at the National Training and Education Division \(NTED\)](#).

Allowable Training-Related Costs: The establishment, support, conduct, and attendance of training specifically identified under the SHSGP program and/or in conjunction with emergency preparedness training by other federal agencies (e.g., HHS and Department of Transportation [DOT]) is allowable. Training conducted using SHSGP funds should address a performance gap identified through an Integrated Preparedness Plan (IPP) or other assessments (e.g., National Emergency Communications Plan Goal Assessments) and contribute to building a capability that will be evaluated through a formal exercise. When developing new courses, recipients are encouraged to apply the Analysis, Design, Development, Implementation, and Evaluation model of instructional design.

Maintenance and Sustainment: Maintenance and sustainment related costs are allowed under this program only as described in the [Preparedness Grants Manual](#) and [DHS 2026 Homeland Security Grant Program Notice of Funding Opportunity \(NOFO\)](#).

More information on allowable investments is included in Appendix 2: Allowable Costs, the [Preparedness Grants Manual](#) and [DHS 2026 Homeland Security Grant Program Notice of Funding Opportunity \(NOFO\)](#).

Management and Administration Costs (M&A): Subrecipients may also use up to 5% of the funding passed through by the state specifically for M&A related to the SHSGP award. Subrecipients can apply M&A costs toward meeting the NPA spending requirements. For example, if a recipient spent \$5,000 on administering election security projects, it could count toward the mandatory 3% allocation for the election security NPA.

G. PROGRAM-SPECIFIC UNALLOWABLE COSTS

Per FEMA policy, the purchase of weapons and weapons accessories, including ammunition, is not allowed with SHSGP funds. Grant funds may not be used for the purchase of the following equipment: firearms; ammunition; grenade launchers; bayonets; or weaponized aircraft, vessels, or vehicles of any kind with weapons installed.

Unauthorized exercise-related costs include:

- Reimbursing for the maintenance or wear-and-tear costs of general use vehicles (e.g., construction vehicles), medical supplies, and emergency response apparatus (e.g., fire trucks, ambulances); and
- Equipment that is purchased for permanent installation and/or use, beyond the scope of the conclusion of the training or exercise (e.g., electronic messaging sign).

SHSGP funds may not be used to support the hiring of sworn public safety officers for purposes of fulfilling traditional public safety duties or to supplant traditional public safety positions and responsibilities (6 U.S.C. § 609(b)(1)(A)).

H. PROHIBITION OF COVERED EQUIPMENT OR SERVICES

FEMA provides additional resources regarding the prohibition on covered telecommunications equipment and services in its policy titled [Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services](#) (FEMA Policy #405-143-1). This policy outlines specific requirements related to the prohibition. Additionally, FEMA's [Contract Provisions Guide](#) offers sample language for the required contract provisions.

Recipients, subrecipients, and their contractors or subcontractors must comply with the prohibitions set forth in [Section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019](#), which restrict the purchase of covered telecommunications and surveillance equipment and services. See [2 C.F.R. §§ 200.216, 200.327, 200.471](#), and [Appendix II to 2 C.F.R. Part 200](#) for more information.

Subrecipients, and their contractors or subcontractors must also comply with Section 1825 of the American Security Drone Act of 2023, enacted as part of the [National Defense Authorization Act for Fiscal Year 2024](#) (Pub. L. No. 118-31 §§ 1821-33, 41 U.S.C. 3901 note prec.). This provision mandates that, beginning December 22, 2025, no federal funds awarded through a contract, grant, or cooperative agreement, or otherwise made available may be used to procure a covered unmanned aircraft system (UAS) that is manufactured or assembled by a covered foreign entity. Significantly, no funds may be used in connection with the operation of such a drone or UAS. For more information, refer to the [Preparedness Grants Manual](#) and [DHS 2026 Homeland Security Grant Program Notice of Funding Opportunity \(NOFO\)](#).

J. DHS STANDARD TERMS AND CONDITIONS

A subrecipient under this funding opportunity must comply with the [DHS Standard Terms and Conditions](#) in effect as of the federal award, unless a term and condition specifically indicates otherwise. For continuation awards, the terms and conditions for the initial federal award will apply unless otherwise specified in the terms and conditions of the continuation award. The specific version of the DHS Standard Terms and Conditions applicable to the federal award will be in the federal award package.

A subrecipient under this funding opportunity must comply with the FY 2026 Department of Homeland Security Standard Terms and Conditions, with the following exceptions. The term titled "Communication and Cooperation with the Department of Homeland Security and Immigration Officials" and paragraph (2)(a)(ii) of the term titled "Federal Anti-Discrimination Laws Material to the Government's Payment Decisions Under the False Claims Act" do not apply to any federal award under this funding opportunity.

Pursuant to the preliminary injunction order issued on November 21, 2025, in *County of Santa Clara et al. v. Noem, et al.*, No. 25-cv-08330-WHO (N.D. Cal.), the following terms and conditions do not apply to awards or subawards issued to any of the plaintiffs subject to the preliminary injunction order while the order remains in effect: (1) The DHS Standard Term and Condition titled "Federal Anti-Discrimination Laws Material to the Government's Payment Decisions Under the False Claims Act"; and (2) the DHS Standard Term and Condition titled "All Executive Orders Related to Grants". If the preliminary injunction is extended to cover additional plaintiffs, this provision will also not apply to any awards or subawards issued to those plaintiffs. If the preliminary injunction is stayed, vacated, or extinguished, both terms will immediately become effective. As stated above, Paragraph (2)(a)(ii) of the DHS Standard Term and Condition titled "Federal Anti-Discrimination Laws Material to the Government's Payment Decisions Under the False Claims Act" will not apply even if the preliminary injunction is stayed, vacated, or extinguished.

Pursuant to the preliminary injunction order issued on November 21, 2025, in *City of Chicago et al. v. Noem, et al.*, No. 25-CV-12765 (N.D. Ill.), the following terms and conditions do not apply to awards or subawards issued to any of the plaintiffs subject to the preliminary injunction order while the order remains in effect: (1) the DHS Standard Term and Condition titled "Federal Anti-Discrimination Laws Material to the Government's Payment Decisions Under the False Claims Act"; and (2) the DHS Standard Term and Condition titled "All Executive Orders Related to Grants". If the preliminary injunction is extended to cover additional plaintiffs, this provision will also not apply to any awards or subawards issued to those plaintiffs. If the preliminary injunction is stayed, vacated, or

extinguished, both terms will immediately become effective. As stated above, paragraph (2)(a)(ii) of the DHS Standard Term and Condition titled "Federal Anti-Discrimination Laws Material to the Government's Payment Decisions Under the False Claims Act" will not apply even if the preliminary injunction is stayed, vacated, or extinguished.

Pursuant to the preliminary injunction order issued on October 31, 2025, in *City of Seattle v. Trump, et al.*, No. 2:25-cv-01435-BJR (W.D. Wa.), the following terms and conditions do not apply to awards or subawards issued to any of the plaintiffs subject to the preliminary injunction order while the order remains in effect: the DHS Standard Term and Condition titled "Federal Anti-Discrimination Laws Material to the Government's Payment Decisions Under the False Claims Act". If the preliminary injunction is extended to cover additional plaintiffs, this provision will also not apply to any awards or subawards issued to those plaintiffs. If the preliminary injunction is stayed, vacated, or extinguished, the term will immediately become effective. As stated above, paragraph (2)(a)(ii) the DHS Standard Term and Condition titled "Federal Anti-Discrimination Laws Material to the Government's Payment Decisions Under the False Claims Act" will not apply even if the preliminary injunction is stayed, vacated, or extinguished.

Note: While not a requirement in the DHS Standard Terms and Conditions, as a best practice, entities receiving funds through this program should ensure that cybersecurity is integrated into the design, development, operation, and maintenance of investments that impact information technology (IT) and/ or operational technology (OT) systems.

Additionally, the recipient and subrecipient must take reasonable cybersecurity and other measures to safeguard information including protected personally identifiable information (PII) and other types of information per [2 C.F.R. § 200.303\(e\)](#).

K. IMMIGRATION CONDITIONS

Materiality of Pending Immigration Condition: An immigration term and condition, including those in the DHS Standard Terms and Conditions, may be material to the Department of Homeland Security's decision to make this grant award, and the Department of Homeland Security may take any remedy for noncompliance, including termination, if the state or territorial recipient or any local government subrecipient fails to comply with this term and condition. No final agency determination has been made as of the date of this publication.

L. FUNDING METHODOLOGY

This Methodology describes the steps taken by DHSEM to allocate SHSGP funding to stakeholders. It also serves as one way to increase transparency by sharing the decision-making approach with all stakeholders. The Subgrant period of performance will be determined based on the actual award date from FEMA.

DHSEM Review and Recommendation to Cabinet Secretary

1. The DHSEM's Grants Management Bureau reviews all applications for eligibility, completeness and to validate compliance with both the Federal NOFO and State Funding Announcement.
2. Applicant eligibility is determined based on supporting documentation showing:
 - NIMS compliance
 - Acknowledgement of intent to work towards achieving NQS compliance
 - Approved THIRA
 - Approved SPR
 - IPP Multi-year Schedule

For jurisdictions applying for the first time, eligibility is determined by:

- Demonstrable efforts made toward achieving NIMS compliance
 - Demonstrable efforts made toward achieving NQS compliance
 - Participation in developing the IPP Multi-year Schedule
 - Working with a Local Preparedness Coordinator to document and seek technical support to become funding eligible.
3. An electronic certified signature is acceptable on the application packet. Scan of hard copy wet ink signatures is also acceptable.
 4. The successful completion of projects and milestones in previous awards are considered when funding requests are reviewed. Consideration is given to extenuating circumstances such as disaster declaration, and/or large-scale crisis that prevented the completion of milestones.
 5. DHSEM Grants Management Bureau will contact each applicant that needs to submit additional 'proof' or 'back-up'.
 6. DHSEM State Exercise Coordinator will determine if the applicant's IPP Multi-year Schedule is current and if the exercise activities being requested are HSEEP complaint.

7. DHSEM may determine that it will not make an award to a subaward application that is considered high risk or that poses a risk of non-compliance. One example of 'high-risk' is unresolved findings from an A144 Audit and an example of 'risk of non-compliance' may be based on previous incomplete project deliverables. DHSEM may determine that it will make an award to an at-risk applicant, subject to additional terms and conditions as described in [2 C.F.R. 200.206](#).
8. The SHSGP Application Review Committee convenes to determine allocation recommendations and submits these to the Cabinet Secretary or designee for final approval.
9. The Cabinet Secretary or designee reviews the allocation recommendations and approves or denies the final allocations.
10. Award letters are sent to applicants that are allocated funding. Letters will also be sent to applicants that do not receive funding. It is anticipated that these letters will be sent within 45 – 60 days of DHSEM's receipt of the SHSGP award.
11. For those communities that are allocated funding, a Sub-grant Agreement will be sent. As the Sub-grant Agreement can be sent only after FEMA awards funding to the State, the distribution date will be within 45 – 60 days of DHSEM's receipt of the SHSGP award.

Submitting the Application

1. Read the DHSEM Funding Announcement and Allocation Methodology (this document), the DHSEM Application packet, [DHS 2026 Homeland Security Grant Program Notice of Funding Opportunity \(NOFO\)](#) and the [Preparedness Grants Manual](#).
2. **Question & Answers:** Submit your questions or requests for technical assistance from the DHSEM Grants Management Bureau at DHSEM-GrantsManagement@state.nm.us. Be sure to include URGENT 2026 SHSGP Grant Program in the subject line of your email.
3. **Identification Numbers:**
 - Organizations must have a State SHARE Vendor number.
 - Active SAM registration. Register at [SAM.gov](#). SAM.gov registration must be renewed annually and must remain active throughout the entire grant life cycle. Failure to register with SAM.gov will prevent your organization from applying for SHSGP funding.
 - Unique Entity Identifier number (UEI). Obtain a UEI number at [SAM.gov](#)
 - Employer Identification Number (EIN). Obtain an EIN at [Get an employer identification number](#).
4. **Application Deadline:** Prepare and submit the application and all required supporting documentation to DHSEM-GrantsManagement@state.nm.us. **no later than 5:00 p.m. July 15, 2026**. This short timeframe is due to FEMA's shortened application period for the 2026 SHSGP. Include **URGENT 2026 SHSGP APPLICATION** and your Jurisdiction's name in the subject line of your email.
5. **New Program:** Prepare and submit an acknowledgement, on your organization's letterhead, that your jurisdiction will be working towards implementation of NQS. Justification and a timeline for completion of required eligibility materials.
6. **Signature:** An electronic certified signature is acceptable for the application. Scan of hard copy wet ink signatures is also acceptable.

M. IMPORTANT KEY DATES

DATE	GRANT ACTIVITY
July 8, 2026	Release of DHSEM's 2026 State Homeland Security Grant Program (SHSGP) Funding Announcement and Allocation Methodology
July 15, 2026	Local/Tribal Jurisdictions Applications due to DHSEM no later than 5:00 p.m.
July 16 – July 20, 2026	DHSEM Review of applications and Request for Information (RFI) process
July 21, 2026	SHSGP Application Review Committee
July 23, 2026	SHSGP Application Review Committee's Recommendation for Allocations submitted to the Cabinet Secretary or designee
July 24, 2026	DHSEM Application Due to FEMA
45 days after FEMA releases the State Award	Subgrants to be awarded will be sent only after FEMA awards the grant to State

APPENDIX 1

Example Project Types: All priorities in this table concern Safety and Security Lifelines.

Priority Areas	Core Capabilities	Example Project Types
National Priorities		
Enhancing the Protection of Soft Targets/Crowded Places (Securing Public Gathering Locations)	- Operational coordination - Public information and warning - Intelligence and information sharing - Interdiction and disruption - Screening, search, and detection - Access control and identity verification - Physical protective measures - Risk management for protection programs and activities	- Operational overtime. For more information on operational overtime, see Appendix 2 of this NOFO. - Physical security enhancements - Security cameras (closed-circuit television [CCTV]) - Security screening equipment for people and baggage - Lighting - Access controls - Fencing, gates, barriers, etc. - UAS and detection technologies
Enhancing Cybersecurity	- Cybersecurity - Intelligence and information sharing - Planning - Public information and warning - Operational coordination - Screening, search, and detection - Access control and identity verification - Supply chain integrity and security - Risk management for protection programs and activities - Long-term vulnerability reduction - Situational assessment - Infrastructure systems - Operational communications	- Cybersecurity risk assessments - Migrating online services to the “.gov” internet domain - Projects that address vulnerabilities identified in cybersecurity risk assessments - Improving cybersecurity of critical infrastructure to meet minimum levels identified by the Cybersecurity and Infrastructure Security Agency and the National Institute of Standards and Technology Cybersecurity Framework (Version 1.1) - Adoption of cybersecurity performance goals (CISA's Cross-Sector Cybersecurity Performance Goals) - Cybersecurity training, planning, and exercises
Supporting Homeland Security Task Forces and Fusion Centers	- 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 - Procuring technology or equipment to support surveillance, communications, and data analysis - Developing 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

Priority Areas	Core Capabilities	Example Project Types
		• Information sharing with all DHS components; fusion centers; other operational, investigative, and analytic entities; and other federal law enforcement and intelligence entities • Cooperating with DHS and other entities in intelligence, threat recognition, assessment, analysis, and mitigation • Identifying, assessing, 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)
Enhancing Election Security	• Cybersecurity • Intelligence and information sharing • Planning • Long-term vulnerability reduction • Situational assessment • Infrastructure systems • Operational coordination • Community resilience	• Physical security planning and exercise support • Physical/site security measures (e.g., locks, shatter-proof glass, alarms, access controls) • General election security navigator support • Cyber and general election security navigator support • Cybersecurity risk assessments, training, and planning • Projects that address vulnerabilities identified in cybersecurity risk assessments • Iterative backups, encrypted backups, network segmentation, monitoring/scanning software, and endpoint protection • Distributed Denial of Service (DDoS) protection • Migrating online services to the “.gov” internet domain • Public awareness and preparedness campaigns addressing election security and integrity measures • Long-term vulnerability reduction and community resilience initiatives
Supporting Border Crisis Response and Enforcement	• Training and awareness • Community resilience • Operational coordination • Risk management for protection programs and activities	• Staffing support to expand 287(g) screening operations within correctional 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 and civil liberties protections, and 287(g) procedures • Developing or enhancing information-sharing platforms between ICE and local agencies • Procuring screening, detection, and communications technology to support immigration enforcement activities

Priority Areas	Core Capabilities	Example Project Types
		- Establishing secure and dedicated communication networks with ICE Field Offices - Conducting joint training exercises with ICE and local law enforcement to test operational coordination - Supporting 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
Enduring Needs		
Planning	- Planning - Risk management for protection programs and activities - Risk and disaster resilience assessment - Threats and hazards identification - Operational coordination - Community resilience	- Development of: - Security Risk Management Plans - Threat Mitigation Plans - Continuity of Operations Plans - Response Plans - Vulnerability Assessments - Efforts to strengthen governance integration between/among regional partners - Joint training and planning with DHS officials and other entities designated by DHS - Cybersecurity training and planning
Training and Awareness	- Long-term vulnerability reduction - Public information and warning - Operational coordination - Situational assessment - Community resilience	- Active shooter training - Intelligence analyst training - SAR and terrorism indicators/behaviors training - Security training for employees - Public awareness/preparedness campaigns - Cybersecurity training and planning - Sharing and leveraging intelligence and information
Equipment and Capital Projects	- Long-term vulnerability reduction - Infrastructure systems - Operational communications - Interdiction and disruption - Screening, search and detection - Access control and identity verification - Physical protective measures	- Protecting high-risk, high-consequence areas or systems that have been identified through risk assessments - Physical security enhancements - Security cameras (CCTV) - Security screening equipment for people and baggage - Lighting - Access Controls - Fencing, gates, barriers, etc. - Enhancing Weapons of Mass Destruction and/or improvised explosive device prevention, detection, and response capabilities - Chemical/Biological/Radiological/Nuclear/Explosive detection, prevention, and response equipment
Exercises	- Long-term vulnerability reduction - Operational coordination - Operational	Response exercises, including exercise planning with community-based organizations

Priority Areas	Core Capabilities	Example Project Types
	communications • Community resilience	

APPENDIX 2
Allowable Projects Costs

The following matrix lists allowable cost for projects. The [Preparedness Grants Manual](#) includes additional information on allowable costs. Subrecipients must follow all applicable requirements in [2 C.F.R. Part 200 Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards](#). SHSGP funds may be used to cover the costs for evaluating the impact of this grant on core capabilities and capability gaps. This list is not exhaustive, therefore, if there are any questions regarding allowable costs, please contact DHSEM.

Allowable Program Activities	SHSGP
Allowable Planning Costs	
Developing hazard/threat-specific annexes	Yes
Developing and implementing homeland security support programs and adopting ongoing DHS/FEMA national initiatives	Yes
Developing related terrorism and other catastrophic event prevention activities	Yes
Developing and enhancing plans and protocols	Yes
Developing or conducting assessments	Yes
Hiring full- or part-time staff or contract/consultants to assist with planning, engagement, and volunteer management activities	Yes
Materials required to conduct planning, engagement, and volunteer management activities	Yes
Travel/per diem related to planning, engagement, and volunteer management activities	Yes
Overtime and backfill costs (in accordance with operational Cost Guidance)	Yes
Issuance of Western Hemisphere Travel Initiative-compliant Tribal identification cards	Yes
Activities to achieve planning inclusive of people with disabilities and others with access and functional needs and limited English proficiency	Yes
Coordinating with Citizen Corps Councils for public information/education and development of volunteer programs	Yes
Coordinating with and material support to Citizen Corps Councils and local firehouses for the establishment, training and maintenance of CERTs	Yes
Updating governance structures and processes and plans for emergency communications	Yes
Developing and reviewing and revising of continuity of operations plans	Yes
Developing and reviewing and revising of the THIRA/SPR and continuity of operations plans	Yes
Allowable Organizational Activities: Note: Personnel hiring, overtime, and backfill expenses are permitted under this grant only to the extent that such expenses are for the allowable activities within the scope of the grant.	
Program management	Yes
Developing whole community partnerships	Yes
Structures and mechanisms for sharing information between the public and private sector	Yes
Implementing models, programs, and workforce enhancement initiatives	Yes
Tools, resources, and activities that facilitate shared situational awareness between the public and private sectors	Yes
Operational support	Yes
Utilizing standardized resource management concepts	Yes
Responding to an increase in the threat level under the National Terrorism Advisory System (NTAS), or needs	Yes

Allowable Program Activities		SHSGP
resulting from a National Special Security Event		
Reimbursement for select operational expenses associated with increased security measures at critical infrastructure sites incurred (up to 50% of the allocation)		Yes
Overtime for information, investigative, and intelligence sharing activities (up to 50% of the allocation)		Yes
Hiring new staff positions/contractors/consultants for participation in information/intelligence analysis and sharing groups or fusion center activities (up to 50% of the allocation).		Yes
Hiring or maintaining staff positions/contractors/consultants at SLTT levels to deliver community preparedness training, resources and material to schools, community-based organizations, faith-based institutions and local businesses.		Yes
Hiring or maintaining staff positions/contractors/consultants to create, support and maintain CERT or Teen CERT		Yes
Cost of migrating online services to the “.gov” domain		Yes
Allowable Equipment Categories		
Personal Protective Equipment		Yes
Explosive Device Mitigation and Remediation Equipment		Yes
CBRNE Operational Search and Rescue Equipment		Yes
Information Technology		Yes
Cybersecurity Enhancement Equipment		Yes
Interoperable Communications Equipment		Yes
Detection		Yes
Decontamination		Yes
Medical countermeasures		Yes
Power (e.g., generators, batteries, power cells)		Yes
CBRNE Reference Materials		Yes
CBRNE Incident Response Vehicles		Yes
Terrorism Incident Prevention Equipment		Yes
Physical Security Enhancement Equipment		Yes
Inspection and Screening Systems		Yes
Animal Care and Foreign Animal Disease		Yes
CBRNE Prevention and Response Watercraft		Yes
CBRNE Prevention and Response Unmanned Aircraft		Yes
CBRNE Aviation Equipment		Yes
CBRNE Logistical Support Equipment		Yes
Intervention Equipment (e.g., tactical entry, crime scene processing)		Yes
Critical emergency supplies		Yes
General use vehicle acquisition, lease, and rental		No
Specialized vehicle acquisition, lease, and rental		Yes
Other Authorized Equipment		Yes

Allowable Program Activities	SHSGP
Allowable Training Costs	
Overtime and backfill for emergency preparedness and response personnel attending DHS/FEMA-sponsored and approved training classes	Yes
Overtime and backfill expenses for part-time and volunteer emergency response personnel participating in DHS/FEMA training	Yes
Training workshops and conferences	Yes
Activities to achieve training inclusive of people with disabilities and others with access and functional needs and limited English proficiency	Yes
Full- or part-time staff or contractors/consultants	Yes
Travel	Yes
Supplies	Yes
Instructor certification/re-certification	Yes
Coordination with Citizen Corps Councils and CERT in conducting training exercises	Yes
Preparedness training for community preparedness initiatives and programs	Yes
Interoperable communications training	Yes
Activities to achieve planning inclusive of people with limited English proficiency	Yes
Immigration enforcement training	Yes
Allowable Exercise Related Costs	
Design, Develop, Conduct, and Evaluate an Exercise	Yes
Full- or part-time staff or contractors/consultants	Yes
Overtime and backfill costs, including expenses for part-time and volunteer emergency response personnel participating in DHS/FEMA exercises	Yes
Implementation of Homeland Security Exercise and Evaluation Program (HSEEP)	Yes
Activities to achieve exercises inclusive of people with disabilities and others with access and functional needs	Yes
Travel	Yes
Supplies	Yes
Interoperable communications exercises	Yes
Activities to achieve planning inclusive of people with limited English proficiency	Yes
Allowable M&A Costs	
Hiring full- or part-time staff or contractors/consultants to assist with the management of the respective grant program, application requirements, and compliance with reporting and data collection requirements	Yes
Development of operating plans for information collection and processing necessary to respond to DHS/FEMA/DHSEM data calls	Yes
Overtime and backfill costs	Yes
Travel	Yes
Meeting related expenses	Yes
Authorized office equipment	Yes
Recurring expenses such as those associated with cell phones and faxes during the period of performance of the grant program	Yes

Allowable Program Activities		SHSGP
Leasing or renting space for newly hired personnel during the period of performance of the grant program		Yes
Conducting activities related to evaluating project effectiveness for HSGP-funded projects		Yes
LETPA Costs		
Integration and interoperability of systems and data, such as computer aided dispatch (CAD) and record management systems (RMS), to facilitate the collection		Yes
Maturation, enhancement, and sustainment of designated state and major Urban Area fusion centers, including information sharing and analysis, threat recognition, terrorist interdiction, and intelligence analyst training and salaries (subject to certain conditions)		Yes
Regional counterterrorism training programs for small, medium, and large jurisdictions to exchange information and discuss the current threat environment, lessons learned, and best practices to help prevent, protect against, and mitigate acts of terrorism		Yes
Coordination of regional full-scale training exercises (federal, state, and local law enforcement participation) focused on terrorism-related events		Yes
Law enforcement Chemical, Biological, Radiological, Nuclear, and high yield Explosives detection and response capabilities, such as bomb detection/disposal capability development, sustainment, or enhancement, including canine teams, robotics platforms, and x-ray technology		Yes
Coordination between fusion centers and other operational analytic and investigative efforts		Yes
Implementation, maintenance, and sustainment of the Nationwide Suspicious Activity Reporting Initiative		Yes
Implementation of the "If You See Something, Say Something®" campaign		Yes
Increase physical security, through law enforcement personnel and other protective measures, by implementing preventive and protective measures at critical infrastructure locations		Yes