2. National Priority Areas (NPAs)

- Description: FY 2025 HSGP aligns with the Administration's priorities by directing resources toward the most urgent threats facing the Nation. Through the State Homeland Security Program (SHSP), HSGP supports the development and sustainment of core capabilities essential to achieving the National Preparedness Goal (NPG): "A secure and resilient Nation."

  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 FY 2025 NPAs are:

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

  These NPAs are rooted in the core mission areas of the NPG—prevention, protection, mitigation, and response—, and reflect a whole-of-government approach to homeland security. Applicants should use these priorities to guide planning, investment, and implementation to drive measurable outcomes and long-term resilience.

- Allocation Requirement:
  Recipients must allocate at least 30% of their SHSP 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), applicants can enhance the effectiveness and compliance of their funding proposals.

- Minimum Spend:
  - Enhancing Election Security requires at least 3% of total SHSP funds.
  - Supporting Border Crisis Response and Enforcement requires at least 10% of total SHSP funds.

- The remaining 17% can be allocated across the other NPAs.

Failure to meet NPA spending requirements will result in a hold on affected funds until compliance issues are resolved.

Priority Areas	Description	Minimum Allocation Requirement
Enhancing the Protection of Soft Targets/Crowded Places	Improving security at locations accessible to the public and vulnerable to attacks.	No minimum allocation
Supporting Homeland Security Task Forces and Fusion Centers	Promoting coordination of activities and critical information sharing and analysis to prevent and respond to threats.	No minimum allocation
Enhancing Cybersecurity	Strengthening the protection of computer systems and networks against cyber threats.	No minimum allocation
Enhancing Election Security	Ensuring the integrity and security of voting systems.	At least 3% of the total SHSP allocation must be dedicated to this area
Supporting Border Crisis Response and Enforcement	Supporting collaboration between state and local law enforcement and U.S. Immigration and Customs Enforcement (ICE) through the 287(g) program to identify and remove individuals who pose a threat to public safety and national security.	At least 10% of the total SHSP allocation must be dedicated to this area

States are encouraged to review the Strategic Framework for Countering Terrorism and Targeted Violence when developing investments.

- **NPA Investments: SHSP**
  - **Soft Targets/Crowded Places (no minimum percent)**
    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.

    In addition, 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 HSGP 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 EO 14305, recipients must:

- **Consult FEMA and Legal Experts:** Work with FEMA's Preparedness Officer and 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.

Applicants are encouraged to submit an investment related to protecting soft targets/crowded places. The proposed investment will be subject to DHS/FEMA's evaluation of the effectiveness of the proposed investments. States are encouraged to engage DHS' Protective Security Advisors for security assessments of soft targets to ensure that recommendations from those assessments are taken into consideration when allocating grant funding.

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 FEMA's Preparedness Grants Manual and related program documents.

- **Supporting Homeland Security Task Forces and Fusion Centers (no minimum percent)**
  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
  - Protection of economic and critical infrastructure

  Allowable Costs:

Applicants may use grant funds for:

- Establishing or enhancing multi-agency 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

Fusion Center Requirements: While there is no minimum spending requirement for this NPA, applicants must include at least one dedicated fusion center project under this priority. Applicants must clearly justify how their project will enhance information sharing, collaboration, and a culture of national preparedness. DHS/FEMA will evaluate these investments based on their effectiveness and alignment with program objectives. Please see the Preparedness Grants Manual for more information on fusion center performance measures.

Additional resources and information regarding collaboration and information sharing are also available through the Department's Office of Intelligence and Analysis.

- **Cybersecurity (no minimum percent)**
  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. While not mandatory, applicants are encouraged to submit proposals for ongoing or high-priority cybersecurity projects. DHS/FEMA will evaluate these investments based on their effectiveness.

  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.

  Additional resources and information regarding cybersecurity and cybersecurity performance goals are available through the Cybersecurity and Infrastructure Security Agency, Cross-Sector Cybersecurity Performance Goals | CISA, and the National Institute of Standards and Technology.

- **Election Security (3% minimum allocation)**
  In January 2017, DHS designated the infrastructure used to administer the Nation's elections as critical infrastructure. This designation recognizes that the United States'

election infrastructure is of such vital importance to the American way of life that its incapacitation or destruction would have a devastating effect on the country. Additionally, the Homeland Threat Assessment 2024 indicates that electoral processes remain an attractive target for many adversaries.

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, HSGP recipients 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, each state must make at least one (1) investment that supports physical and/or cyber election security. Proposed investments must meet or exceed the FY 2025 national priority percentage for election security (minimum 3%) and will be evaluated by DHS/FEMA for effectiveness and alignment with program goals.

To further strengthen election integrity, jurisdictions must:

- Prioritize compliance with the Voluntary Voting System Guidelines (VVSG) 2.0 established by the U.S. Election Assistance Commission;
- Complete testing through a Voting System Test Laboratory (VSTL) accredited by the Commission;[1]
- Utilize the U.S. Citizenship and Immigration Services' Systematic Alien Verification Entitlements (SAVE) system to verify that anyone working at a polling place in any capacity is a U.S. citizen.
- Demonstrate proof of compliance before accessing the full HSGP award—3% of the award will be withheld from drawdown until compliance is confirmed.

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

[1] Exec. Order No. 14,248, Preserving and Protecting the Integrity of American Elections, 90 Fed. Reg. 14,005 (Mar. 25, 2025).

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 (1) investment must support efforts under this NPA. Applicants must allocate at least 10% of total SHSP 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 is available through the ICE 287(g) program website.

d. *Other FY 2025 SHSP Funding Priorities*

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;[2]
- Training and awareness campaigns;
- Equipment and capital projects; and
- Exercises.

The table below provides a breakdown of the FY 2025 SHSP priorities showing the core capabilities enhanced and lifelines supported, as well as examples of eligible project types for each area. More information on allowable investments can be found in Appendix 12.B and in the Preparedness Grants Manual (FM-207-23-001).

DHS/FEMA expects that national priorities will continue to be included in future years, evolving as threats change and capability gaps are addressed. Applicants are strongly encouraged to start planning now to sustain existing capabilities using funding sources other than DHS preparedness grants.

[2] 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.

Projects listed in the table below may be useful in preparing for disasters unrelated to terrorism, as long as they also support the primary goals of preventing, preparing for, protecting against, or responding to acts of terrorism.

Example Project Types

All priorities in this table concern the 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 12.B 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	• Establishing or enhancing multi-agency Homeland Security Task Forces (HSTFs), including operational coordination centers • Enhancing capabilities and integration with local fusion centers

Priority Areas	Core Capabilities	Example Project Types
	• Operational coordination • Risk management for protection programs and activities	• 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)
Enhancing Election Security	• Cybersecurity • Intelligence and information sharing • Planning • Long-term vulnerability reduction • Situational assessment • Infrastructure systems • Operational coordination • Community resilience	• Prioritize compliance with the VVSG 2.0 established by the U.S. Election Assistance Commission • Complete testing through a VSTL accredited by the U.S. Election Assistance Commission • Physical security planning and exercise support • Physical/site security measures – e.g., locks, shatter proof glass, alarms, access controls, etc. • 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, 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

Priority Areas	Core Capabilities	Example Project Types
		• Public awareness/preparedness campaigns discussing election security and integrity measures • Long-term vulnerability reduction and community resilience
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 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 communication 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
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	• Protection of high-risk, high-consequence areas or systems that have been identified through risk assessments • Physical security enhancements ○ Security cameras (CCTV)

Priority Areas	Core Capabilities	Example Project Types
	• Interdiction and disruption • Screening, search and detection • Access control and identity verification • Physical protective measures	○ 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 communications • Community resilience	• Response exercises, including exercise planning with community-based organizations

For FY 2025, each SHSP recipient is required to submit an Investment Justification (IJ) for the NPAs with minimum spend requirements (i.e., Enhancing Election Security and Supporting Border Crisis Response and Enforcement). The investments must also account for at least the relevant minimum percentage of the applicant's SHSP allocations. SAAs may submit complete project-level information at the time of application, including the NPA IJs, but are not required to do so. ***As a reminder, all SHSP-funded projects must have a demonstrated nexus to achieving target capabilities related to preventing, preparing for, protecting against, and responding to acts of terrorism***. At the same time, these projects can also help improve preparedness for other types of disasters.

e. *Goals and Objectives for OPSG*

Operation Stonegarden (OPSG) supports enhanced cooperation and coordination among Customs and Border Protection (CBP)/United States Border Patrol (USBP), and federal, state, local, tribal, and territorial law enforcement agencies to strengthen border security.

The program's objectives are to:

- Enhance collaboration and coordination among federal, state, local, tribal, and territorial law enforcement agencies to strengthen border security;
- Support joint efforts to secure borders, including land and water routes, and critical travel corridors; and
- Improve information and intelligence sharing to address border-related threats effectively.

f. *OPSG Funding Priorities*

FY 2025 Emphasis:

- Jurisdictions are encouraged to participate in the 287(g) program as part of their OPSG efforts when coordinated with and endorsed by USBP.