The Department of Homeland Security (DHS)

Notice of Funding Opportunity (NOFO)

Fiscal Year 2025 Nonprofit Security Grant Program

Fraud, waste, abuse, mismanagement, and other criminal or noncriminal misconduct related to this program may be reported to the Office of Inspector General (OIG) Hotline. The toll-free numbers to call are 1 (800) 323-8603 and TTY 1 (844) 889-4357.

Contents

1. Basic Information

A. Agency Name	U.S. Department of Homeland Security (DHS), Federal Emergency Management Agency (FEMA)
B. NOFO Title	Fiscal Year 2025 Nonprofit Security Grant Program (NSGP)
C. Announcement Type	Initial
D. Funding Opportunity Number	DHS-25-GPD-008-00-99
E. Assistance Listing Number	97.008
F. Expected Total Funding	$274,500,000 • Subtotal for NSGP-UA: $137,250,000 • Subtotal for NSGP-S: $137,250,000
G. Anticipated Number of Awards	56 awards
H. Expected Award Range	NSGP-UA: $261,630 – $29,938,456 NSGP-S: $0 or $1,050,000 – $4,700,000
I. Projected Application Start Date	07/28/2025 08:00 a.m. Eastern Time (ET)
J. Projected Application End Date	08/11/2025 05:00 p.m. Eastern Time (ET)
K. Anticipated Funding Selection Date	No later than August 23, 2025
L. Anticipated Award Date	No later than 09/30/2025
M. Projected Period of Performance Start Date	09/01/2025
N. Projected Period of Performance End Date	08/31/2028
Executive Summary	The NSGP improves and increases the physical/cybersecurity and facility/target hardening of nonprofit organizations' facilities at risk of a terrorist of other extremist attack, ultimately safeguarding the lives and property of the American people. In FY 2025, there are two funding sources appropriated for nonprofit organizations: 1. **NSGP - Urban Area (NSGP-UA):** NSGP-UA funds nonprofit organizations located **within** FY 2025 designated high-risk

	urban areas. Under NSGP-UA, each urban area will receive an allocation for nonprofit organizations **within** FY 2025 designated high-risk urban areas. 2. **NSGP - State (NSGP-S):** NSGP-S funds nonprofit organizations located **outside** of a FY 2025 Designated high-risk urban area. Under NSGP-S, each state will receive an allocation for nonprofit organizations in the state located **outside** of FY 2025 Designated high-risk urban areas.
O. Agency Contact	**a.** ***Program Office Contact*** FEMA has assigned state-specific Preparedness Officers for the NSGP. If you do not know your Preparedness Officer, please contact FEMA Grants News by e-mail at fema-grants-news@fema.dhs.gov OR by phone at (800) 368-6498, Monday through Friday, 9:00 AM – 5:00 PM ET. **b.** ***FEMA Grants News*** This channel provides general information on all FEMA grant programs and maintains a comprehensive database containing key personnel contact information at the federal, state, and local levels. FEMA Grants News Team is reachable at fema-grants-news@fema.dhs.gov. OR (800) 368-6498, Monday through Friday, 9:00 AM – 5:00 PM ET. **c.** ***Grant Programs Directorate (GPD) Award Administration Division*** GPD's Award Administration Division (AAD) provides support regarding financial matters and budgetary technical assistance. AAD can be contacted at ASK-GMD@fema.dhs.gov. **d.** ***FEMA Regional Offices*** FEMA Regional Offices also may provide fiscal support, including pre- and post-award administration and technical assistance. FEMA Regional Office contact information is available at https://www.fema.gov/fema-regional-contacts. **e.** ***Civil Rights*** Consistent with Executive Order 14173, *Ending Illegal Discrimination & Restoring Merit-Based Opportunity*, the FEMA Office of Civil Rights is responsible for ensuring compliance with and enforcement of federal civil rights obligations in connection with programs and services conducted by FEMA. They are reachable at FEMA-CivilRightsOffice@fema.dhs.gov. **f.** ***Environmental Planning and Historic Preservation*** The FEMA Office of Environmental Planning and Historic Preservation (OEHP) provides guidance and information about the

	EHP review process to FEMA programs and recipients and subrecipients. Send any inquiries regarding compliance for FEMA grant projects under this NOFO to FEMA-OEHP-NOFOQuestions@fema.dhs.gov. **g. *FEMA GO*** For technical assistance with the FEMA GO system, please contact the FEMA GO Helpdesk at femago@fema.dhs.gov or (877) 585-3242, Monday through Friday, 9:00 AM – 6:00 PM ET. **h. *Preparedness Grants Manual*** Recipients seeking guidance on policies and procedures for managing preparedness grants should reference the Preparedness Grants Manual at Preparedness Grants Manual.

2. Eligibility

A. Eligible Entities/Entity Types	Only the following entities or entity types are eligible to apply. **a. *Applicants*** 1. Eligible Applicants ***Note: Throughout this funding notice, the term "applicant" refers to the State Administrative Agency (SAA), and the term "subapplicant" refers to the nonprofit organization.*** Consistent with the commitment to clarity and transparency, most of this NOFO's information identifies actions for the applicant to take, not the subapplicant. Contact FEMA-NSGP@fema.dhs.gov with questions. The SAA is the only eligible applicant to apply for funding to FEMA. Nonprofit organizations are eligible as subapplicants to the SAA. As such, nonprofit organizations must apply for FY 2025 NSGP through their SAA, who then submits application information to FEMA. A list of SAA points of contact is available at: State Administrative Agency (SAA) Contacts | FEMA.gov. Nonprofit organizations may NOT apply directly to DHS/FEMA for FY 2025 NSGP funds. Additional information on the subapplicant process specific to nonprofit organizations is included in Section 4.C. and 4.D. of this funding notice. SAAs, in coordination with the Urban Area Working Groups (UAWG) or other relevant state partners, are encouraged to notify and actively inform eligible nonprofit organizations of the availability of FY 2025 NSGP funding. 2. Applicant Eligibility Criteria

	The SAA is the only eligible applicant. NSGP-UA funds nonprofit organization located within the FY 2025 Designated high-risk urban. Under NSGP-UA, each Urban Area will receive an allocation for nonprofit organizations located within a designated high-risk urban area. See Appendix B for the complete list. NSGP-S funds nonprofit organizations located outside of a FY 2025 Designated high-risk urban area. Under NSGP-S, each state will receive an allocation for nonprofit organizations in the state located outside of FY 2025 Designated high-risk urban areas. See Appendix C for the FY 2025 Allocations. **b. *Subapplicants*** Subapplicants and subawards are allowed. Subapplicants should not have foreign nationals or noncitizens included. If a subapplicant has foreign nationals, they must be properly vetted and must adhere to all government statues, polices, and procedures including "staff American, stay in America" and security requirements. Subawards are allowed under the NSGP. The recipient (the SAA) is awarded, and then all funds to the nonprofit organizations (subrecipients) are considered subawards. 1. Subrecipient Eligibility Nonprofit organizations eligible as **subapplicants to the SAA** are those organizations that are: a) Described under section 501(c)(3) of the Internal Revenue Code of 1986 (IRC) and exempt from tax under section 501(a) of such code. ***This includes entities designated as "private" (e.g., private institutions of higher learning), as private colleges and universities can also be designated as 501c3 entities.*** **Note**: The Internal Revenue Service (IRS) does not require certain organizations such as churches, mosques, and synagogues to apply for and receive a recognition of exemption under section 501(c)(3) of the IRC. Such organizations are automatically exempt if they meet the requirements of section 501(c)(3). These organizations are not required to provide recognition of exemption. For organizations that

	the IRS requires to apply for and receive a recognition of exemption under section 501(c)(3), the state may or may not require recognition of exemption, as long as the method chosen is applied consistently. Refer to links below for additional information: • Exemption Requirements - 501(c)(3) Organizations | Internal Revenue Service (irs.gov) • Publication 557 (01/2022), Tax-Exempt Status for Your Organization | Internal Revenue Service (irs.gov) • Charities and Nonprofits | Internal Revenue Service (irs.gov) b) Able to demonstrate, through the application, that the organization is at high risk of a terrorist or other extremist attack; and c) For NSGP-UA, located within a FY 2025 Designated high-risk urban area; or for NSGP-S, located outside of a FY 2025 Designated high-risk urban area. Examples of eligible subapplicant organizations can include houses of worship, museums, educational facilities, senior centers, community centers, and day camps, among many others. 2. Applying for NSGP-UA versus NSGP-S ***Nonprofit organizations may* NOT *apply to FEMA directly.*** Nonprofit organizations must apply for FY 2025 NSGP through their SAA. A list of SAA points of contact is available at State Administrative Agency (SAA) Contacts | FEMA.gov. ***Nonprofit organizations should contact the respective SAA to:*** • Verify the SAA's application deadline. SAAs establish all requirements and deadlines to manage their nonprofit sub-application process in support of the SAAs' submissions to DHS/FEMA. Deadlines and state requirements may vary from state to state. The deadline published in this funding notice is for the SAA to apply to DHS/FEMA, not for the nonprofit organization to apply to the SAA. • Obtain information on any additional state requirements or processes. Eligible nonprofit subapplicants located within FY 2025 designated high-risk urban areas may apply to the SAA (applicant) to receive funding **only** under NSGP-UA. Eligible nonprofit organization subapplicants located outside of FY 2025 Designated high-risk urban areas may apply to the SAA (applicant) to receive funding **only** under NSGP-S. ***DHS/FEMA will verify that nonprofit subapplicants have***

	applied to the correct program and will disqualify the applications of nonprofit subapplicants that apply to the wrong program. For nonprofit organizations that are unsure if they are within a FY 2025 Designated urban area, contact the respective SAA. A list of SAA contacts can be found at State Administrative Agency (SAA) Contacts | FEMA.gov. If a nonprofit organization has a physical location within a defined Metropolitan Statistical Area but the location is NOT within the bounds of how the UAWG defines the high-risk urban area footprint, then that location should apply under NSGP-S. ***Nonprofit organizations that have locations both within and outside of Designated high-risk urban areas can apply under both NSGP-UA and NSGP-S depending on the physical location of the facilities.*** In such cases, the nonprofit subapplicant must submit separate applications for NSGP-UA and NSGP-S to the SAA (applicant) for funding consideration. SAA applicants and nonprofit subapplicants must still adhere to the other restrictions and requirements set forth in this funding notice, including applying for a maximum of six locations total per nonprofit organization with no more than three locations in either NSGP-UA or NSGP-S, and a maximum of $200,000 per location. If a nonprofit organization has a physical location within a defined Metropolitan Statistical Area ***but the location is NOT within the bounds of how the UAWG defines the high-risk urban area then that location should apply under NSGP-S.*** Nonprofit organizations should contact their SAAs to determine if their physical location falls within the UAWG-defined high-risk urban area footprint. Additionally, the final beneficiary of the NSGP grant award must be an eligible nonprofit organization and cannot be a for-profit/fundraising extension of a nonprofit organization. While these for-profit or fundraising extensions may be associated with the eligible nonprofit organization, NSGP funding cannot be used to benefit those extensions and therefore they will be considered ineligible applications. If the funding being sought is for the benefit of a for-profit/fundraising extension, then that would constitute an ineligible subaward since only nonprofit organizations are eligible subrecipients. This is distinct from a contract under an award in which a nonprofit organization could seek the assistance of a for-profit/fundraising extension, but the purpose would be to benefit the *nonprofit organization* and not for the benefit of the for-profit/fundraising extension. For further information on the distinction between a subaward and contract, see 2 C.F.R. § 200.331.

	3. Reducing Subapplicant Burden For FY 2025, each SAA is **strongly encouraged** to re-evaluate its process for collecting and evaluating subaward applications. FEMA encourages each SAA to minimize the type and quantity of information that it collects as part of the subaward application process, in order to decrease the overall financial and time burden associated with applying for subawards under this grant program. Each SAA should review its subaward application and reduce or eliminate the request for any information that is not needed for legal, financial, or oversight purposes.
B. Project Type Eligibility	**a.** ***Unallowable Project Types*** See Section 3.F "Program-Specific Unallowable Costs" for more information on unallowable project types." **b.** ***Allowable Project Types*** Allowable costs generally must fall into the categories of planning, equipment, training, or exercises. Please see Appendix A: Allowable Costs for more information on allowable costs. If there are any questions regarding allowable costs, please contact the appropriate FEMA Headquarters (HQ) Preparedness Officer.
C. Requirements for Personnel, Partners, and Other Parties	An application submitted by an otherwise eligible non-federal entity (which for this program is the SAA) may be deemed ineligible when the person that submitted the application (for the applicant/SAA) is not: 1) a ***current employee, personnel, official, staff, or leadership*** of the non-federal entity; and 2) ***duly authorized to apply*** for an award on behalf of the non-federal entity at the time of application. Further, the Authorized Organization Representative (AOR) must be a duly authorized current employee, personnel, official, staff or leadership of the recipient and ***provide an email address unique to the recipient (SAA) at the time of application and upon any change in assignment during the period of performance. Consultants or contractors of the recipient are not permitted to be the AOR of the recipient.*** Subapplicants should not have foreign nationals or noncitizens included. If a subapplicant has foreign nationals, they must be properly vetted and must adhere to all government statues, polices, and procedures including "staff American, stay in America" and security requirements. Subapplicants/subrecipients must submit short bios and resumes. This should include the type of entity, organizational leadership, and board

	members along with the both the names and addresses of the individuals. Resumes are subject to approval.
D. Maximum Number of Applications	The maximum number of applications that can be submitted is: 1. One per State Nonprofit organizations must apply through their respective SAA. See Section 2.A.1 "Eligible Applicants" for more information about the SAA, nonprofit organization, and applicant/subapplicant roles and responsibilities. For NSGP-UA and NSGP-S, consistent with prior years, each nonprofit organization may only represent one site/location/physical address per application. For example, a nonprofit organization with one site may apply for up to $200,000 for that site. **Maximum Award Amount** Nonprofit organizations must apply through their respective SAA. See Section 2.A. "Eligible Entities/Entity Types" for more information about the SAA, nonprofit organization, and applicant/subapplicant roles and responsibilities. For NSGP-UA and NSGP-S, consistent with prior years, each nonprofit organization may only represent one site/location/physical address per application. For example, a nonprofit organization with one site may apply for up to $200,000 for that site. Nonprofit organizations with multiple sites/locations/physical addresses may choose to apply for additional sites for up to $200,000 per site, for a maximum of three sites per funding stream, *not to exceed $600,000 total per state*. That is, a nonprofit organization with sites in both NSGP-S and NSGP-UA areas in a given state may apply for a total of up to six sites, but the total of their applications cannot exceed $600,000. **A nonprofit organization subapplicant may not exceed a total of six applications (three for NSGP-S and three for NSGP-UA) for a total of $600,000 per state**. A nonprofit organization with locations in multiple states may apply for up to three sites within each state and funding stream (three for NSGP-S and three for NSGP-UA per state). Appendix B provides a table of the eligible Urban Areas for FY 2025 that would apply to the NSGP-UA funding stream. All other nonprofit organizations outside of these Urban Areas apply to the NSGP-S program. If a nonprofit subapplicant applies for projects at multiple sites, regardless of whether the projects are similar in nature, each individual site must include an assessment of the vulnerability and risk unique to each site. That is, one vulnerability assessment per location/physical address. Failure to do so may be cause for rejection of the application.
E. Additional Restrictions	**a.** ***National Incident Management System (NIMS) Implementation***

	Prior to allocation of any federal preparedness awards, recipients (the SAA) must ensure and maintain adoption and implementation of NIMS. The list of objectives used for progress and achievement reporting is on FEMA's website at https://www.fema.gov/emergency-managers/nims/implementation-training. Please see the Preparedness Grants Manual for more information on NIMS. Applicants/subapplicants or recipients/subrecipients are required to certify their compliance with federal statues, DHS directives, polices, and procedures.
F. References for Eligibility Factors within the NOFO	Please see the following references provided below: 1. "Responsiveness Review Criteria" subsection 2. "Financial Integrity Criteria" subsection 3. "Supplemental Financial Integrity Criteria and Review" subsection 4. FEMA may/will request financial information such as Employer Identification Number (EIN) and bank information as part of the potential award selection. This will apply to everyone, including subrecipients.
G. Cost Sharing Requirement	There is no cost share requirement for the FY 2025 NSGP.
H. Cost Share Description, Type and Restrictions	Not applicable.
I. Cost Sharing Calculation Example	Not applicable.
J. Required information for verifying Cost Share	Not applicable.

3. Program Description

A. Background, Program Purpose, and Program History

The Nonprofit Security Grant Program (NSGP) is one of the grant programs that support DHS/FEMA's focus on enhancing the ability of state, local, tribal, and territorial governments, as well as nonprofits, to prevent, protect against, prepare for, and respond to terrorist or other extremist attacks. These grant programs are part of a comprehensive set of measures authorized by Congress and implemented by DHS to help strengthen the nation's communities against potential terrorist or other extremist attacks. The NSGP is a competitive grant program intended to provide federal funding for physical security enhancements and other security-related activities to nonprofit organizations that are at risk of terrorist attack.

DHS is focused on the criticality of information sharing and collaboration in building a national mindset of preparedness and protecting against terrorism and other threats to our national security. DHS and its homeland security mission were born from the "failures among federal agencies and between the federal agencies and state and local authorities to share critical information related to the threat of terrorism" prior to the September 11, 2001, attacks. However, the threat profile has changed in the past two decades. We now face continuous cyberattacks by sophisticated actors, as well as ongoing threats to soft targets and crowded places, such as schools, churches, synagogues, mosques, and other nonprofit entities. The NSGP reflects DHS's commitment to risk-informed investment, collaboration, and resilience. To ensure that priorities reflect the current threat environment, FEMA's Preparedness Grant Programs are guided by annually designated National Priority Areas (NPAs). The FY 2025 NPAs are:

a. Enhancing the protection of soft targets and crowded places,
    i. This includes faith-based organizations and election sites;
b. Supporting Homeland Security Task Forces and fusion centers;
c. Enhancing and integrating cybersecurity resiliency;
d. Enhancing election security; and
e. Border Crisis Response and Enforcement Support.
    i. 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.

For FY 2025, the Administration encourages applicants to propose innovative solutions that support the broader homeland security mission reflected in the NPAs, as applicable. Applicants must clearly demonstrate how their proposed projects address an NPA and how they align with the stated purpose and objectives of this NOFO.

The NSGP has significantly contributed to the improvement and increase in the physical/cyber security and facility/target hardening of nonprofit organizations' facilities, ultimately safeguarding the lives and property of the American people. Nonprofit organizations tend to be high-profile and/or visible targets of group- or identity-based attacks because the populations affiliated with these organizations are usually members of a group with a shared identity (religious, ideological, mission-based, etc.). The frequency and severity of attacks – whether they are hate-based, group-based, opportunistic, or random – are increasing. The Federal Bureau of Investigation (FBI) reported more than 11,862 hate or bias-based attacks in 2023, an increase from previous years.

Nonprofit organizations tend to not have the resources, capital, or experience to secure facilities and implement costly and effective (i.e., state-of-the-art) security measures to protect the individuals who use their services or facilities from the increasing acts of violence perpetrated against populations who affiliate with these, often identity-based, nonprofits. In FY 2024, the types of equipment nonprofit organizations requested and received the most NSGP funding for

included: 1) video assessment and security systems; 2) impact resistant doors and gates; 3) physical access control systems; 4) jersey walls, fences, and other barriers; and 5) fixed area lighting. By providing crucial funding to high-risk non-profit organizations, the NSGP supports the ability of non-profit organizations to protect themselves and the individuals targeted by affiliation.

In the history of the program, over $1.8 billion has been allocated to nonprofit organizations and over 14,000 applications have been awarded. In recent years:

- NSGP emphasized the integration of preparedness activities of nonprofit organizations with broader state and local preparedness efforts.
- Funding priorities evolved to include spending Planning, Organizational, Equipment, Training, and Exercises (POETE) towards addressing the NPAs.

B. Goals, Objectives, and Priorities

Goals: The NSGP will improve and increase the physical/cybersecurity and facility/target hardening of nonprofit organizations' facilities at risk of a terrorist of other extremist attack, ultimately safeguarding the lives and property of the American people. Concurrently, the NSGP will integrate the preparedness activities of nonprofit organizations that are at high risk of a terrorist or other extremist attack with broader state and local preparedness efforts.

Objectives: The NGSP, via State Administrative Agencies (SAA), provides funds to nonprofit organizations that are at high risk of terrorist or other extremist attack to meet the following three objectives throughout the period of performance:

1) **Enhance equipment and conduct security-related activities to improve the security posture of nonprofit organizations that are at high risk of a terrorist or other extremist attack.**
   a) With this funding, build and sustain core capabilities, as identified in individual nonprofit organization Vulnerability Assessments, of high-risk nonprofit organizations in the annual national priority areas. See the table "FY 2025 NSGP Funding Priorities" in Section 3B.
2) **Address and close capability gaps that are identified in individual nonprofit organization Vulnerability Assessments via funding spent on Planning, Equipment, and Training and Exercises that aim to enhance the protection of soft targets and crowded places.**
   a) Planning – carrying out risk management for the protection of programs and activities, risk and disaster resilience assessment, threats, and hazard identification, as well as operational coordination.
   b) Equipment– Strengthening security infrastructure, technology, and protective measures.
   c) Training & Exercises – long-term vulnerability reduction via preparedness training, public information and warning enhancement, and threat response exercises.
3) **Strengthen relationships across non-profit organization, state, local, and territorial homeland security agencies for a whole community approach to preparedness.**
   a) Implementing a comprehensive and coordinated (whole of community) approach to preparedness can address enduring security needs, including effective planning, training and awareness campaigns, and exercises. See the table "FY 2025 NSGP Funding Priorities" in Section 3B.

Priorities: Given the evolving threat landscape, it is incumbent upon DHS/FEMA to continuously evaluate the national risk profile and set priorities that help ensure appropriate allocation of scarce security dollars. The FY 2025 NPAs reflect FEMA's broader mission across all preparedness efforts. Applicants should be familiar with these NPAs, as they represent DHS's current focus areas and may shape future guidance:

- Enhancing Protection of Soft Targets/Crowded Places
- Supporting Homeland Security Task Forces and Fusion Centers
- Enhancing Cybersecurity
- Enhancing Election Security
- Supporting Border Crisis Response and Enforcement

Enduring needs include:

- Effective planning
- Training and awareness campaigns
- Equipment and capital projects
- Exercises

The table below provides a breakdown of the NPAs and core capabilities impacted, as well as examples of eligible project types for each area. More information on allowable investments can be found in the Funding Restrictions and Allowable Costs section below.

FY 2025 NSGP Funding Priorities

All priorities in this table concern the Safety and Security Lifelines.

Priority Areas	Core Capabilities Enhanced	Example Project Types
National Priorities		

Enhancing the Protection of Soft Targets/Crowded Places	• Planning
	• 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
	• Long-term vulnerability reduction
	• Situational assessment
	• Infrastructure systems
		• Private contracted security guards
		• Physical security enhancements
		  ○ Closed circuit television (CCTV) security cameras
		  ○ Security screening equipment for people and baggage
		  ○ Access controls
		  ▪ Fencing, gates, barriers, etc.
		  ▪ Card readers, associated hardware/software

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 • Procurement of technology or equipment to support surveillance, communications, and data analysis

Priority Areas	Core Capabilities Enhanced	Example Project Types
		• 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 Cybersecurity	• Cybersecurity
	• Intelligence and Information Sharing
	• Interdiction and disruption
	• Long-term vulnerability reduction
		• Cybersecurity enhancements
		  ○ Risk-based cybersecurity planning and training
		  ○ Improving cybersecurity of access control and identify verification systems
		  ○ Improving cybersecurity of security technologies (e.g., CCTV systems)
		• Adoption of cybersecurity performance goals (CISA's Cross-Sector Cybersecurity Performance Goals)

Priority Areas	Core Capabilities Enhanced	Example Project Types
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 • 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

Priority Areas	Core Capabilities Enhanced	Example Project Types
		• 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	• Conduct or enhancement of security risk assessments • Development of: ○ Security plans and protocols ○ Emergency/contingency plans ○ Evacuation/shelter in place plans
Training & Awareness	• Long-term vulnerability reduction • Public information and warning	• Active shooter training, including integrating the needs of persons with disabilities • Security training for employees • Public awareness/preparedness campaigns
Exercises	• Long-term vulnerability reduction	• Response exercises

C. Program Rationale

The stated goals, objectives, and priorities of NSGP support Section 2002 of the Homeland Security Act of 2002 (Pub. L. No. 107-296, as amended) (6 U.S.C. § 609a) by supporting eligible nonprofit organizations at risk of terrorist or extremist attack with funding to enhance facility hardening, improve cybersecurity, and cover costs related to security training, facility security personnel, grant administration, and other appropriate activities as determined by the Administrator.

D. Federal Assistance Type

Grant

E. Performance Measures and Targets

Performance metric for this program is:

- Performance Measure 1: Percentage of funding allocated by the recipient to core capabilities to build or sustain the national priorities identified in Section B above. (80%)

FEMA will calculate and analyze the above metrics through a review of recipient Biannual Strategy Implementation Report (BSIR) updates and award monitoring to ensure that the funds are expended for their intended purpose and achieve the stated outcomes in the grant application.

F. Program-Specific Unallowable Costs
The following projects and costs are considered **ineligible** for award consideration:

- Organization costs, and operational overtime costs;
- Hiring of public safety personnel (excluding off duty law enforcement personnel in the capacity of contract security);
- General use expenditures;
- Overtime and backfill;
- Initiatives that do not address the implementation of programs/initiatives to build prevention and protection-focused capabilities directed at identified facilities and/or the surrounding communities;
- The development of risk/vulnerability assessment models;
- Initiatives that fund risk or vulnerability security assessments or the development of the Investment Justification (IJ);
- Initiatives in which federal agencies are the beneficiary or that enhance federal property;
- Initiatives which study technology development;
- Proof-of-concept initiatives; and
- Direct or indirect pass-through of benefits to non-eligible entities.

G. General Funding Requirements
Costs charged to federal awards (including federal and non-federal cost share funds) must comply with applicable statutes, rules and regulations, policies, this NOFO, the Preparedness Grants Manual, and the terms and conditions of the federal award. This includes, among other requirements, that costs must be incurred, and products and services must be delivered within the budget period. See 2 C.F.R. § 200.403(h).

Recipients may not use federal funds or any cost share funds for the following activities:

1. Matching or cost sharing requirements for other federal grants and cooperative agreements (see 2 C.F.R. § 200.306).
2. Lobbying or other prohibited activities under 18 U.S.C. § 1913 or 2 C.F.R. § 200.450.
3. Prosecuting claims against the federal government or any other government entity (see 2 C.F.R. § 200.435).

See the Preparedness Grants Manual for more information on funding restrictions and allowable costs.

H. Indirect Costs (Facilities and Administrative Costs)
Indirect costs are allowed for recipients and subrecipients.

Indirect costs (IDC) are costs incurred for a common or joint purpose benefitting more than one cost objective and not readily assignable to specific cost objectives without disproportionate effort. Applicants with a current negotiated IDC rate agreement who desire to charge indirect costs to a federal award must provide a copy of their IDC rate agreement with their applications. Not all applicants are required to have a current negotiated IDC rate agreement. Applicants that are not required to have a negotiated IDC rate agreement, but are required to develop an IDC rate proposal, must provide a copy of their proposal with their applications. Applicants without a

current negotiated IDC rate agreement (including a provisional rate) and wish to charge the de minimis rate must reach out to FEMA for further instructions. Applicants who wish to use a cost allocation plan in lieu of an IDC rate proposal must reach out to FEMA for further instructions. As it relates to the IDC for subrecipients, a recipient must follow the requirements of 2 C.F.R. §§ 200.332 and 200.414 in approving the IDC rate for subawards. See the Preparedness Grants Manual for information on establishing indirect cost rates.

I. Management and Administration (M&A) Costs
M&A costs are allowed.

M&A costs are not operational costs but are necessary costs incurred in direct support of the federal award or as a consequence of it, such as travel, meeting-related expenses, and salaries of full/part-time staff in direct support of the program. As such, M&A costs can be itemized in financial reports. Other M&A costs examples include preparing and submitting required programmatic and financial reports, establishing and/or maintaining equipment inventory, documenting operational and equipment expenditures for financial accounting purposes, and responding to official informational requests from state and federal oversight authorities.

Note: SAAs must be able to separately account for M&A costs associated with the NSGP-UA award from those associated with the NSGP-S award.

M&A costs are allowed under this program as described below:

1. **SAA (Recipient) for NSGP-S and NSGP-UA M&A**
   The SAA may use and expend up to 5% of their total FY 2025 NSGP-S and NSGP-UA awards for M&A purposes associated with administering the NSGP-S and NSGP-UA awards. SAAs must include the amount they are requesting for NSGP-S and NSGP-UA M&A in the SF-424A form. The amount should be in addition to the total requested by the subapplicant nonprofit organizations, but not exceed 5% of the total requested by the subapplicant nonprofit organizations. SAAs must be able to separately account for M&A costs associated with the NSGP-UA award from those associated with the NSGP-S.

2. **Nonprofit Organization (subrecipient) for NSGP-S and NSGP-UA M&A**
   Nonprofit organizations that receive a subaward under the NSGP may use and expend up to 5% of each subaward for M&A purposes associated with that subaward. If an organization is receiving more than one subaward, they must be able to separately account for M&A costs for each subaward.

J. Pre-Award Costs
Recipient (SAA) pre-award costs are allowable only with the prior written approval of DHS/FEMA and as included in the award agreement. To request pre-award costs, a written request must be included with the application, signed by the SAA. The letter must outline what the pre-award costs are for, including a detailed budget break-out of pre-award costs from the post-award costs, and a justification for approval. Subrecipients cannot claim pre-award costs. Please contact your SAA should exigent circumstances exist.

K. Beneficiary Eligibility

There are no program requirements. See Section 2 for additional information on eligibility. This NOFO and any subsequent federal awards create no rights or causes of action for any beneficiary.

L. Participant Eligibility
There are no program requirements. This NOFO and any subsequent federal awards create no rights or causes of action for any participant.

M. Authorizing Authority
Section 2009 of the *Homeland Security Act of 2002* (Pub. L. No. 107-296, as amended) (6 U.S.C. § 609a).

N. Appropriation Authority
Full-Year Continuing Appropriations and Extensions Act, 2025, Pub. L. No. 119-4, § 1101.

O. Budget Period
There will be only a single budget period with the same start and end dates as the period of performance.

P. Prohibition on Covered Equipment or Services
See the Preparedness Grants Manual for information on prohibitions on expending funds on covered telecommunications and surveillance equipment and services.

4. Application Contents and Format

A. Pre-Application, Letter of Intent, and Whitepapers
Not applicable.

B. Application Content and Format
Applications are required to be submitted in FEMA GO **by the SAA ONLY**. To begin, visit Grants.gov and search for the NSGP posting. Once you find the posting, go to the **Related Documents** tab to download the necessary documents. Fill out these forms carefully, ensuring all information is accurate and clearly labeled. Save the completed forms. Finally, log in to FEMA GO and upload the required documents as part of your application submission.

C. Application Components
The following forms or information are required to be submitted via FEMA GO. Applicants can complete these forms directly in FEMA GO without needing to upload PDF versions of the forms. The Standard Forms (SF) are also available at Forms | Grants.gov:

- SF-424, Application for Federal Assistance
- Grants.gov Lobbying Form, Certification Regarding Lobbying
- SF-424A, Budget Information (Non-Construction)
    - For construction under an award, submit SF-424C, Budget Information (Construction), in addition to or instead of SF-424A
    - To comply with 2 C.F.R. § 200.402 - 2 C.F.R. § 200.405, NSGP applicants must complete and submit an SF-424A or SF-424C, as appropriate, reflecting cost breakdown per budget cost categories per sub-programs (NSGP-S and NSGP-UA) and **Management and Administration costs** as applicable to align with the FY 2025 NSGP funding notice. The SF-424A or SF-424C with the pre-filled requirements can be found with the NSGP funding notice and associated attachments on grants.gov. Adjustments to the SF-424A or SF-424C maybe required after the FY 2025 NSGP final allocation announcements are made. GPD Grants Management Specialists will contact applicants for any necessary revisions.
- SF-424B, Standard Assurances (Non-Construction)
    - For construction under an award, submit SF-424D, Standard Assurances (Construction), in addition to or instead of SF-424B
- SF-LLL, Disclosure of Lobbying Activities

D. Program-Specific Required Documents and Information
The following program-specific forms or information are required to be submitted in FEMA GO ***following award to the applicable SAA and before any subawards are approved/issued***:

- Investment Justifications (IJ) from ALL nonprofit subapplicants, regardless of if the SAA recommends them for funding in the provided FY 2025 IJ Template (OMB Control Number: 1660-0110/FEMA Form FF-207-FY-21-115).
- SAA Prioritization of IJs in the DHS/FEMA-provided template (OMB Control Number: 1660-0110/FEMA Form FF 207-21-114) located in the Related Documents tab of the Grants.gov posting:
    - SAAs **must** include nonprofit organization application details (e.g., nonprofit organization name, IJ title(s), requested amount(s)) for each nonprofit organization that applied to the SAA for funding on the State Prioritization of IJs even if not being recommended by the SAA for funding.
    - IJs for applications not being recommended for funding **must still be submitted to FEMA.**

- Each nonprofit organization being recommended for funding must be scored and must have a **unique rank** (#1 [one] being the highest ranked through the total number of applications the SAA scored).
- States with multiple FY 2025 Designated high-risk urban areas must ensure that nonprofits are ranked by high-risk urban area. For example, if a state has three high-risk urban areas, there should be three groups of rankings.

As part of the FY 2025 NSGP application, each eligible nonprofit subapplicant must submit the following three documents to the SAA by the deadline established by the SAA:

a. ***NSGP IJ***
Nonprofit subapplicants with one site may apply for up to $200,000 for that site. Nonprofit subapplicants with multiple sites may apply for up to $200,000 per site, for up to three sites per funding stream for a maximum of $600,000 per state. See Section 2.D. for more information about this maximum. If a nonprofit subapplicant applies for multiple sites, it must submit one complete IJ per each site. [1] IJs cannot include more than one physical site.

A fillable IJ form (DHS/FEMA Form FF-207-FY-21-115, OMB Control Number: 1660-0110) is available in the Related Documents tab of the Grants.gov NSGP posting. This year, for the first time, FEMA is also offering a web version of the IJ, available at Grants.gov. The IJ must describe each investment proposed for funding. The investments or projects described in the IJ must:

- Be for the location(s)/physical address(es) (NOT P.O. Boxes) that the nonprofit occupies at the time of application;
- Address an identified risk, including threat and vulnerability, regardless of whether it is submitting for similar projects at multiple sites;
- Demonstrate the ability to provide enhancements consistent with the purpose of the program and guidance provided by DHS/FEMA;
- Be both feasible and effective at reducing the risks for which the project was designed;
- Be able to be fully completed within the three-year period of performance; and
- Be consistent with all applicable requirements outlined in this NOFO and the Preparedness Grants Manual.

More information about the IJ's content and scoring is listed in Appendix D.

Nonprofit subapplicants are required to self-identify with one of the following categories in the IJ as part of the application process:

- Ideology-based/Spiritual/Religious (Houses of Worship, Educational Institutions, Medical Facilities, etc.)
- Educational (secular)
- Medical (secular)
- Other

[1] A nonprofit organization may procure resources covering similar purposes across multiple sites, but the quantities and costs must be broken down by site in each IJ.

b. ***Vulnerability/Risk Assessment***
Each nonprofit subapplicant must include a vulnerability/risk assessment **unique to the site** the IJ is being submitted for.

c. ***Mission Statement***
Each nonprofit subapplicant must include its Mission Statement and any mission implementation policies or practices that may elevate the organization's risk. SAAs will use the Mission Statement along with the nonprofit subapplicant's self-identification in the IJ to validate that the organization is one of the following types: 1) Ideology-based/Spiritual/Religious; 2) Educational; 3) Medical; or 4) Other. The organization type is a factor when calculating the final score of the application; see Section 7 "Application Review Information," subsection "Final Score."

The Vulnerability/Risk Assessment and Mission Statement are not to be submitted in FEMA GO but should be maintained by the SAA and must be made available to DHS/FEMA upon request.

The Vulnerability/Risk Assessment and Mission Statement are not to be submitted in FEMA GO but should be maintained by the SAA and must be made available to DHS/FEMA upon request.

E. Post-Application Requirements for Successful Applicants
a. ***Grant Agreement and Acceptance***
Recipients must review, sign, and return the grant agreement to formalize acceptance of the award and its terms.

b. ***Additional Application Material***
With FEMA's approval, applicants may submit certain required information post award. For detailed guidance, please refer to the award letter or contact your assigned FEMA HQ Preparedness Officer.

c. ***General Information About Post-Federal Award Reporting Requirements***
Award recipients must submit the following reports: quarterly financial reports, semi-annual performance reports and BSIR submissions, final financial and performance reports, and an annual audit report (if required). These must follow the Part 200 Uniform Requirements or specific conditions of the award. If reports are late, future funding or fund access may be delayed, and additional reports may be requested in some cases.

5. Submission Requirements and Deadlines

A. Address to Request Application Package
Applications are processed through the FEMA GO system. To access the system, go to https://go.fema.gov/.

Steps Required to Apply for An Award Under This Program and Submit an Application:

To apply for an award under this program, all applicants must:

a. Apply for, update, or verify their Unique Entity Identifier (UEI) number and EIN from the Internal Revenue Service;

b. In the application, provide an UEI number;
c. Have an account with login.gov;
d. Register for, update, or verify their SAM account and ensure the account is active before submitting the application;
e. Register in FEMA GO, add the organization to the system, and establish the Authorized Organizational Representative (AOR). The organization's electronic business point of contact (eBiz POC) from the SAM registration may need to be involved in this step. For step-by-step instructions, see https://www.fema.gov/media-library/assets/documents/181607;
f. Submit the complete application in FEMA GO; and
g. Continue to maintain an active SAM registration with current information at all times during which it has an active federal award or an application or plan under consideration by a federal awarding agency. As part of this, applicants must also provide information on an applicant's immediate and highest-level owner and subsidiaries, as well as on all predecessors that have been awarded federal contracts or federal financial assistance within the last three years, if applicable.

Per 2 C.F.R. § 25.110(a)(2)(iv), if an applicant is experiencing exigent circumstances that prevents it from obtaining an UEI number and completing SAM registration prior to receiving a federal award, the applicant must notify FEMA as soon as possible. Contact fema-grants-news@fema.dhs.gov and provide the details of the exigent circumstances.

How to Register to Apply:

General Instructions:

Registering and applying for an award under this program is a multi-step process and requires time to complete. Below are instructions for registering to apply for FEMA funds. Read the instructions carefully and prepare the requested information before beginning the registration process. Gathering the required information before starting the process will alleviate last-minute searches for required information.

The registration process can take up to four weeks to complete. To ensure an application meets the deadline, applicants are advised to start the required steps well in advance of their submission.

Organizations must have a Unique Entity Identifier (UEI) number, Employer Identification Number (EIN), and an active System for Award Management (SAM) registration.

Obtain a UEI Number:

All entities applying for funding, including renewal funding, must have a UEI number. Applicants must enter the UEI number in the applicable data entry field on the SF-424 form. For more detailed instructions for obtaining a UEI number, refer to SAM.gov.

Obtain Employer Identification Number:

In addition to having a UEI number, all entities applying for funding must provide an Employer Identification Number (EIN). The EIN can be obtained from the IRS by visiting

https://www.irs.gov/businesses/small-businesses-self-employed/apply-for-an-employer-identification-number-ein-online.

Create a login.gov account:

Applicants must have a login.gov account in order to register with SAM or update their SAM registration. Applicants can create a login.gov account at: https://secure.login.gov/sign_up/enter_email?request_id=34f19fa8-14a2-438c-8323-a62b99571fd.

Applicants only have to create a login.gov account once. For existing SAM users, use the same email address for both login.gov and SAM.gov so that the two accounts can be linked.

For more information on the login.gov requirements for SAM registration, refer to https://www.sam.gov/SAM/pages/public/loginFAQ.jsf.

Register with SAM:

In addition to having a UEI number, all organizations must register with SAM. Failure to register with SAM will prevent your organization from applying through FEMA GO. SAM registration must be renewed annually and must remain active throughout the entire grant life cycle.

For more detailed instructions for registering with SAM, refer to: Register with SAM

Note: per 2 C.F.R. § 25.200, applicants must also provide the applicant's immediate and highest-level owner, subsidiaries, and predecessors that have been awarded federal contracts or federal financial assistance within the past three years, if applicable.

Register in FEMA GO, Add the Organization to the System, and Establish the AOR:

Applicants must register in FEMA GO and add their organization to the system. The organization's electronic business point of contact (eBiz POC) from the SAM registration may need to be involved in this step. For step-by-step instructions, see FEMA GO Startup Guide.

Note: FEMA GO will support only the most recent major release of the following browsers:

- Google Chrome;
- Mozilla Firefox;
- Apple Safari; and
- Microsoft Edge.

Applicants using tablet type devices or other browsers may encounter issues with using FEMA GO.

Submitting the Final Application:

Applicants will be prompted to submit the standard application information and any program-specific information required. Standard Forms (SF) may be accessed in the Forms tab under the

SF-424 family on Grants.gov. Applicants should review these forms before applying to ensure they are providing all required information.

After submitting the final application, FEMA GO will provide either an error message, or an email to the submitting AOR confirming the transmission was successfully received.

B. Application Deadline
08/11/25 05:00:00 PM Eastern Time

C. Pre-Application Requirements Deadline
Not applicable.

D. Post-Application Requirements Deadline
Not applicable.

E. Effects of Missing the Deadline
All applications must be completed in FEMA GO by the application deadline. FEMA GO automatically records proof of submission and generates an electronic date/time stamp when FEMA GO successfully receives an application. The submitting AOR will receive via email the official date/time stamp and a FEMA GO tracking number to serve as proof of timely submission prior to the application deadline.

Applicants experiencing system-related issues have until 3:00 PM ET on the date applications are due to notify FEMA. No new system-related issues will be addressed after this deadline. Applications not received by the application submission deadline will not be accepted.

6. Intergovernmental Review

A. Requirement Description and State Single Point of Contact
An intergovernmental review may be required. Applicants must contact their state's Single Point of Contact (SPOC) to comply with the state's process under Executive Order 12372.

7. Application Review Information

A. Threshold Criteria
Subapplicants will be disqualified if they: submit incomplete subapplication packages; are administratively noncompliant (e.g., scanned IJs, incorrect or previous year forms); have a history of poor performance in grant administration; apply for the wrong funding stream; and/or are deemed an ineligible organization.

B. Application Criteria
a. ***Programmatic Criteria***
Nonprofit organizations must submit their FY 2025 NSGP applications to their respective SAA by the deadline established by the SAA. If an SAA has established deadline that is prior to release of the FY 2025 NSGP funding notice, the SAA is responsible for working with any nonprofits that may need to amend their submissions to account for changes in the FY 2025 NSGP program prior to the start of the SAA application evaluation process. FY 2025 NSGP-S and NSGP-UA applications will be reviewed through a two-phase state and federal review process for completeness, adherence to programmatic guidelines, feasibility, and how well the IJ (project description and justification) addresses the identified risk(s). For FY 2025 NSGP-S and

NSGP-UA SAAs will make recommendations to DHS/FEMA based on their allocation and according to the chart listed in the respective process subsection below.

The following are the FY 2025 NSGP-S and NSGP-UA evaluation process and criteria:

- For NSGP-UA, state and federal verification that the nonprofit organization is located within one of the FY 2025 Designated high-risk urban areas (contact the appropriate SAA for the UAWG-defined high-risk urban area footprints); and for NSPG-S, verification that the nonprofit is located outside of one of the FY 2025 Designated high-risk urban areas;
- Identification and substantiation of current or persistent threats or attacks (from within or outside the United States) by a terrorist or other extremist organization, network, or cell against the subapplicant based on their ideology, beliefs, and/or mission as: 1) an ideology-based/spiritual/religious; 2) educational; 3) medical; or 4) other nonprofit entity;
- Symbolic value of the site(s) as a highly recognized regional and/or national or historical institution(s) that renders the site a possible target of terrorist or other extremist attack;
- Role of the nonprofit organization in responding to or recovering from terrorist or other extremist attacks;
- Alignment between the project activities requested within the physical or cyber vulnerabilities identified in the organization's vulnerability assessment;
- Integration of nonprofit preparedness with broader state and local preparedness efforts;
- Completed IJ **for each site** that addresses an identified risk **unique to that site**, including the assessed threat, vulnerability, and consequence of the risk; and
- History of prior funding under NSGP. Not having received prior year NSGP funding is a positive factor when calculating the state score of the application; see Section 7, Application Review Information – Review and Selection Process, for additional information.

Grant projects must be: 1) both feasible and effective at mitigating the identified vulnerability and thus reducing the risks for which the project was designed; and 2) able to be fully completed within the three-year period of performance. DHS/FEMA will use the information provided in the application, as well as any supporting documentation, to determine the feasibility and effectiveness of the grant project. Information that would assist in the feasibility and effectiveness determination includes the following:

- Scope of work (purpose and objectives of the project, identification of what is being protected);
- Desired outcomes, including expected long-term impact where applicable;
- Summary of status of planning and design accomplished to date (e.g., included in a capital improvement plan); and
- Project schedule.

Recipients and subrecipients are expected to conform, as applicable, with accepted engineering practices, established codes, standards, modeling techniques, and best practices.

b. *Review and Selection Process*

Because of the timing of the FY 2025 NSGP Program, the NSGP-S and NSGP-UA funding will be issued as risk-based allocations to each state and territory. Subawards will still be governed by the competitive process described below; ***however, this will occur after award of the state- and territory-based allocations to ensure that all funds can be obligated prior to the end of the fiscal year.***

1. NSGP-UA Process

State Review

Application packages are submitted by the nonprofit organization to the SAA based on the established criteria. As part of the review for NSGP-UA, the SAAs must:

- Conduct an eligibility review, in coordination with the UAWG;
- Verify that the nonprofit is located within a FY 2025 Designated high-risk urban area;
- Review and score only **complete** application packages (including mission statements and vulnerability assessments) using the NSGP Scoring Criteria provided by DHS/FEMA;
- Validate the **self-certified organization type listed in the IJ** by assessing the central purpose of the organization described in the mission statement;
- Prioritize all NSGP IJs by ranking each IJ. Each IJ will receive a **unique rank** (#1 [one] being the highest ranked through the total number of applications the SAA scored);
- For states with multiple FY 2025 Designated high-risk urban areas, each high-risk urban area must be ranked separately;
- Submit the results of the SAA review of **complete applications from eligible subapplicants** to DHS/FEMA using the SAA Prioritization Tracker;
- Submit nonprofit organization application details for ***applications received but not recommended for funding (including incomplete applications and ineligible subapplicants), as well as justification as to why they are not being recommended for funding*** to DHS/FEMA using the SAA Prioritization Tracker;
- Submit IJs that are recommended for funding; SAAs should submit IJs that collectively represent 150% of the state's NSGP-UA allocation; this will allow DHS/FEMA to award the next prioritized IJ in instances when a subapplicant is found to be ineligible or when a significant portion of an IJ includes proposed projects that are unallowable, for example:

NSGP-UA Allocation	Submit IJs That Total This Amount to DHS/FEMA
$1.4 million	$2.1 million
$2 million	$3 million
$2.5 million	$3.75 million

- Submit IJs received and *not* recommended for funding, including incomplete IJs and IJs from subapplicants deemed ineligible; and
- Retain the mission statements and vulnerability assessments submitted by each nonprofit organization.

The SAA will base the ranking on the final scores from the Prioritization Tracker as determined by the SAA's subject-matter expertise and discretion with consideration of the following factors:

- **Need**: the relative need for the nonprofit organization compared to the other subapplicants; and
- **Impact**: the feasibility of the proposed project and how effectively the proposed project addresses the identified need.

The SAA reviewers will score each question in the IJ according to the scoring matrix in Appendix D.

Federal Review

The highest-ranking IJs from each submitting high-risk urban area are reviewed by a panel made up of DHS/FEMA federal staff. As a part of this review, federal staff will also verify that the nonprofit is located within a FY 2025 Designated high-risk urban area.

Federal reviewers will review each IJ to check for the following:

- Eligibility (e.g., that a potential subrecipient meets all the criteria for the program);
- Allowability of the proposed project(s); and
- Any derogatory information on the organization applying per Section 7.B.3. "Security Review."

Final Score

To calculate an application's final score, the subapplicant's SAA score will be multiplied:

- By a factor of three for ideology-based/spiritual/religious entities (Houses of Worship, Educational Institutions, Medical Facilities, etc.);
- By a factor of two for secular medical and educational institutions; and
- By a factor of one for all other nonprofit organizations.

Subapplicants that have never received an NSGP award will have 15 points added to their score.

Subapplicants will be selected from highest to lowest scored within their respective urban area until the available urban area allocation has been exhausted. In the event of a tie during the funding determination process, priority will be given to nonprofit organizations that have not received prior year funding, and then those prioritized highest by their SAA. Should an Urban Area fail to meet their published allocation, the remaining balance will not be reallocated.

DHS/FEMA will use the final results to make subaward funding recommendations to the Secretary of Homeland Security. All final subaward funding determinations will be made by the Secretary of Homeland Security, who retains the discretion to consider other factors and information in addition to DHS/FEMA's funding recommendations.

2. NSGP-S Process

State Review

Application packages are submitted by the nonprofit organization to the SAA based on the established criteria. The SAA will review applications and recommend to DHS/FEMA which nonprofit organizations should be selected for funding. As part of the state review, the SAAs must:

- Conduct an eligibility review;
- Verify that the nonprofit is located outside a FY 2025 Designated high-risk urban area;
- Review and score all **complete** application packages (including vulnerability assessments and mission statement) using the NSGP Scoring Criteria provided by DHS/FEMA;
- Validate the **self-certified organization type listed in the IJ** by assessing the central purpose of the organization described in the mission statement;
- Prioritize all NSGP IJs by ranking each IJ. Each IJ will receive a **unique rank** (#1 [one] being the highest ranked through the total number of applications the SAA scored);
- Submit the results of the state review along with **complete IJs from eligible subapplicants** to DHS/FEMA using the SAA Prioritization Tracker;
- Submit nonprofit organization application details for ***applications received but not recommended for funding (including incomplete and ineligible subapplicants), as well as justification as to why they are not being recommended for funding*** to DHS/FEMA using the SAA Prioritization Tracker;
- Submit IJs that are recommended for funding; SAAs should submit IJs that collectively represent 150% of the state's NSGP-S allocation; this will allow DHS/FEMA to award the next prioritized IJ in instances when a subapplicant is found to be ineligible or when a significant portion of an IJ includes proposed projects that are unallowable, for example:

NSGP-S Allocation	Submit IJs That Total This Amount to DHS/FEMA
$1.4 million	$2.1 million
$2 million	$3 million
$2.5 million	$3.75 million

- Submit IJs received and *not* recommended for funding, including incomplete IJs and IJs from subapplicants deemed ineligible.
- Retain the mission statements and vulnerability assessments submitted by each nonprofit organization.

The SAA will base the ranking on the final scores from the Prioritization Tracker as determined by the SAA's subject-matter expertise and discretion with consideration of the following factors:

- **Need**: The relative need for the nonprofit organization compared to the other subapplicants; and
- **Impact**: The feasibility of the proposed project and how effectively the proposed project addresses the identified need.

The SAA reviewers will score each question in the IJ according to the scoring matrix in Appendix D.

Federal Review

The IJs submitted by each SAA will be reviewed by DHS/FEMA federal staff. Federal staff will also verify that the nonprofit organization is located outside of a FY 2025 Designated high-risk urban area. Federal reviewers will review each IJ to check for the following:

- Eligibility (e.g., that a potential subrecipient meets all the criteria for the program);
- Allowability of the proposed project(s); and
- Any derogatory information on the organization applying per Section 7.B.3. "Security Review."

Final Score

To calculate an application's final score, the subapplicant's SAA score will be multiplied:

- By a factor of three for ideology-based/spiritual/religious entities (Houses of Worship, Educational Institutions, Medical Facilities, etc.);
- By a factor of two for secular medical and educational institutions; and
- By a factor of one for all other nonprofit organizations.

Subapplicants who have never received a NSGP award will have 15 points added to their score.

Subapplicants will be selected from highest to lowest scored within their respective state/territory until the available state allocation has been exhausted. In the event of a tie during the funding determination process, priority will be given to nonprofit organizations that have not received prior year funding, and then those prioritized highest by their SAA. Should a state/territory fail to meet their published allocation, the remaining balance will not be reallocated.

DHS/FEMA will use the final results to make funding recommendations for subawards to the Secretary of Homeland Security. All final funding determinations for subawards will be made by the Secretary of Homeland Security, who retains the discretion to consider other factors and information in addition to DHS/FEMA's funding recommendations.

3. Security Review

DHS Office of Intelligence and Analysis receives a list of potential NSGP subrecipient organizations, which it reviews against U.S. intelligence community reporting. The security review occurs after the competitive scoring and selection process is complete. The information provided for the security review is limited to the nonprofit organization's name and physical address, as submitted by the nonprofit organization. Any potentially derogatory information, as well as any potentially mitigating information, that could assist in determining whether a security risk exists is sent to FEMA and is used in making final award decisions.

C. Financial Integrity Criteria
Before making an award, FEMA is required to review OMB-designated databases for applicants' eligibility and financial integrity information. This is required by the Payment Integrity Information Act of 2019 (Pub. L. No. 116-117, § 2 (2020)), 41 U.S.C. § 2313, and the "Do Not Pay Initiative" (31 U.S.C. 3354). For more details, please see 2 C.F.R. § 200.206.

Thus, the Financial Integrity Criteria may include the following risk-based considerations of the applicant:

1. Financial stability.
2. Quality of management systems and ability to meet management standards.
3. History of performance in managing federal award.
4. Reports and findings from audits.
5. Ability to effectively implement statutory, regulatory, or other requirements.

D. Supplemental Financial Integrity Criteria and Review
Before making an award expected to exceed the simplified acquisition threshold (currently a total federal share of $250,000) over the period of performance:
1. FEMA is required by 41 U.S.C. § 2313 to review or consider certain information found in SAM.gov. For details, please see 2 C.F.R. § 200.206(a)(2).
2. An applicant may review and comment on any information in the responsibility/qualification records available in SAM.gov.
3. Before making decisions in the risk review required by 2 C.F.R. § 200.206, FEMA will consider any comments by the applicant.

E. Reviewers and Reviewer Selection
NSGP subapplications undergo a two-tiered review process. The SAAs review, score, and rank all submitted subapplications. FEMA then reviews all subapplications recommended by the SAA for Federal Review. FEMA's review is conducted by the GPD Homeland Security Programs Division's Branch Chiefs, Section Chiefs, and Preparedness Officers, who receive comprehensive training on evaluation criteria to ensure consistency and fairness. To uphold impartiality, FEMA enforces strict conflict of interest policies, requiring reviewers to disclose any potential conflicts prior to participation. This rigorous process ensures that funding decisions are thorough and unbiased.

F. Merit Review Process
In the NSGP Federal Review, the SAAs' score is multiplied by the applicable multiplier and bonus points are added based on first-time status (see Section 7.B.b.1 or 7.B.b.2 of this NOFO). The scoring matrix the SAAs use is found in Appendix D of this NOFO. IJs are also reviewed to identify any unallowable expenses or projects/activities, with costs disallowed or placed on hold as necessary. Subapplications are selected for funding in descending order, starting with the highest-scored subapplications, until the available funds are allocated. Additional information on this process can be found in section 7.G of this NOFO. This merit-based selection process ensures that funding is directed to the most promising and highest risk subapplications.

G. Final Selection
For NSGP, the determination is made using Final Score (SAA Score * Multiplier + Bonus Points). In both NSGP-S and NSGP-UA, subapplications are compared to those within the same

State or Territory. The highest scored subapplication in a State and UA is selected for funding first and selection proceeds in descending order until the state reaches its allocation. In the event of ties, preference is given to first-time recipients, then SAA rank.

Final selections of NSGP subawards are at the discretion of the Secretary of Homeland Security.

8. Award Notices

A. Notice of Award
The Authorized Organization Representative should carefully read the federal award package before accepting the federal award. The federal award package includes instructions on administering the federal award as well as terms and conditions for the award.

By submitting an application, applicants agree to comply with the prerequisites stated in this NOFO, the Preparedness Grants Manual, and the material terms and conditions of the federal award, should they receive an award.

FEMA will provide the federal award package to the applicant electronically via FEMA GO. Award packages include an Award Letter, Summary Award Memo, Agreement Articles, and Obligating Document. An award package notification email is sent via the grant application system to the submitting AOR.

Recipients must accept their awards no later than 60 days from the award date. Recipients shall notify FEMA of their intent to accept the award and proceed with work via the FEMA GO system.

Funds will remain on hold until the recipient accepts the award via FEMA GO and all other conditions of the award have been satisfied, or until the award is otherwise rescinded. Failure to accept a grant award within the specified timeframe may result in a loss of funds.

B. Pass-Through Requirements
Pass-through funding is required under this program. For more information, please see the Preparedness Grants Manual.

C. Note Regarding Pre-Award Costs
Even if pre-award costs are allowed, beginning performance is at the applicant and/or sub-applicant's own risk.

D. Obligation of Funds
The funds are obligated only when and once the agency's signatory authority approves and signs the award package.

E. Notification to Unsuccessful Applicants
SAAs are required to inform nonprofit organization subapplicants of their non-selection. FEMA will provide an optional template that SAAs can use; however, SAAs can modify this template as needed. SAAs are required to inform subapplicants of their non-selection no later than 90 days from the date they accept their NSGP award.

9. Post-Award Requirements and Administration

A. Administrative and National Policy Requirements

Presidential Executive Orders

Recipients must comply with the requirements of Presidential Executive Orders related to grants (also known as federal assistance and financial assistance), the full text of which are incorporated by reference.

In accordance with *Executive Order 14305, Restoring American Airspace Sovereignty (June 6, 2025),* and to the extent allowed by law, eligible state, local, tribal, and territorial grant recipients under this NOFO are permitted to purchase unmanned aircraft systems, otherwise known as drones, or equipment or services for the detection, tracking, or identification of drones and drone signals, consistent with the legal authorities of state, local, tribal, and territorial agencies. Recipients must comply with all applicable federal, state, and local laws and regulations, and adhere to any statutory requirements on the use of federal funds for such unmanned aircraft systems, equipment, or services.

Subrecipient Monitoring and Management

Pass-through entities must comply with the requirements for subrecipient monitoring and management as set forth in 2 C.F.R. §§ 200.331-333.

B. DHS Standard Terms and Conditions
A recipient under this funding opportunity must comply with the DHS Standard Terms and Conditions in effect as of the date of the federal award. The DHS Standard Terms and Conditions are available online: DHS Standard Terms and Conditions | Homeland Security. 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 recipient under this funding opportunity must comply with the FY 2025 Department of Homeland Security Standard Terms and Conditions, v. 3 (Apr. 18, 2025), with the exception Paragraph C.IX (Communication and Cooperation with the Department of Homeland Security and Immigration Officials) and paragraph C.XVII(2)(a)(iii) (Anti-Discrimination Grant Award Certification regarding immigration). Paragraphs C.IX and C.XVII(2)(a)(iii) do not apply to any federal award under this funding opportunity. The FY 2025 Department of Homeland Security Standard Terms and Conditions, v. 3 (Apr. 18, 2025) are available at www.dhs.gov/publication/dhs-standard-terms-and-conditions.

C. Financial Reporting Requirements
See the Preparedness Grants Manual for information on financial reporting requirements.

D. Programmatic Performance Reporting Requirements
See the Preparedness Grants Manual for information on performance reporting requirements.

E. Closeout Reporting Requirements
See the Preparedness Grants Manual for information on closeout reporting requirements and administrative closeout.

Anytime there is a chance in personnel for any of the awardees and/or subrecipients, their information needs to be submitted for approval (all the previous personal information identified).

F. Disclosing Information
See the Preparedness Grants Manual for information on disclosing information per 2 C.F.R. § 180.335.

G. Reporting of Matters Related to Recipient Integrity and Performance
See the Preparedness Grants Manual for information on reporting of matters related to recipient integrity and performance.

H. Single Audit Report
See the Preparedness Grants Manual for information on single audit reports.

I. Monitoring and Oversight
Per 2 C.F.R. § 200.337, DHS and its authorized representatives have the right of access to any records of the recipient or subrecipient pertinent to a Federal award to perform audits, site visits, and any other official use. The right also includes timely and reasonable access to the recipient's or subrecipient's personnel for the purpose of interview and discussion related to such documents or the Federal award in general.

Pursuant to this right and per 2 C.F.R. § 200.329, DHS may conduct desk reviews and make site visits to review and evaluate project accomplishments and management control systems as well as provide any required technical assistance. Recipients and subrecipients must respond in a timely and accurate manner to DHS requests for information relating to a federal award.

J. Program Evaluation
Title I of the Foundations for Evidence-Based Policymaking Act of 2018, Pub. L. No. 115-435 (2019) (Evidence Act), PUBL435.PS urges federal agencies to use program evaluation as a critical tool to learn, improve delivery, and elevate program service and delivery across the program lifecycle. Evaluation means "an assessment using systematic data collection and analysis of one or more programs, policies, and organizations intended to assess their effectiveness and efficiency." Evidence Act, § 101 (codified at 5 U.S.C. § 311). OMB A-11, Section 290 (Evaluation and Evidence-Building Activities) further outlines the standards and practices for evaluation activities. Federal agencies are required to specify any requirements for recipient participation in program evaluation activities (2 C.F.R. § 200.301). Program evaluation activities incorporated from the outset in the NOFO and program design and implementation allow recipients and agencies to meaningfully document and measure progress and achievement towards program goals and objectives, and identify program outcomes and lessons learned, as part of demonstrating recipient performance (2 C.F.R. § 200.301).

As such, recipients and subrecipients are required to participate in a Program Office (PO) or a DHS Component-led evaluation, if selected. This may be carried out by a third-party on behalf of the PO or the DHS Component. Such an evaluation may involve information collections including but not limited to, records of the recipients; surveys, interviews, or discussions with individuals who benefit from the federal award, program operating personnel, and award recipients; and site visits or other observation of recipient activities, as specified in a DHS Component or PO-approved evaluation plan. More details about evaluation requirements may be provided in the federal award, if available at that time, or following the award as evaluation requirements are finalized. Evaluation costs incurred during the period of performance are allowable costs (either as direct or indirect) in accordance with 2 C.F.R.§ 200.413.

Recipients and subrecipients are also encouraged, but not required, to participate in any additional evaluations after the period of performance ends, although any costs incurred to participate in such evaluations are not allowable and may not be charged to the federal award.

K. Additional Performance Reporting Requirements
Not Applicable.

L. Termination of the Federal Award

1. Paragraph C.XL of the FY 2025 DHS Standard Terms and Conditions, v.3 sets forth a term and condition entitled "Termination of a Federal Award." The termination provision condition listed below applies to the grant award and the term and condition in Paragraph C.XL of the FY 2025 DHS Standard Terms and Conditions, v.3 does not.

2. Termination of the Federal Award by FEMA

   FEMA may terminate the federal award in whole or in part for one of the following reasons identified in 2 C.F.R. § 200.340:

   a. If the recipient or subrecipient fails to comply with the terms and conditions of the federal award.
   b. With the consent of the recipient, in which case FEMA and the recipient must agree upon the termination conditions. These conditions include the effective date and, in the case of partial termination, the portion to be terminated.
   c. If the federal award no longer effectuates the program goals or agency priorities. Under this provision, FEMA may terminate the award for these purposes if any of the following reasons apply:
      i. If DHS/FEMA, in its sole discretion, determines that a specific award objective is ineffective at achieving program goals as described in this NOFO;
      ii. If DHS/FEMA, in its sole discretion, determines that an objective of the award as described in this NOFO will be ineffective at achieving program goals or agency priorities;
      iii. If DHS/FEMA, in its sole discretion, determines that the design of the grant program is flawed relative to program goals or agency priorities;
      iv. If DHS/FEMA, in its sole discretion, determines that the grant program is not aligned to either the DHS Strategic Plan, the FEMA Strategic Plan, or successor policies or documents;

v. If DHS/FEMA, in its sole discretion, changes or re-evaluates the goals or priorities of the grant program and determines that the award will be ineffective at achieving the updated program goals or agency priorities; or
vi. For other reasons based on program goals or agency priorities described in the termination notice provided to the recipient pursuant to 2 C.F.R. § 200.341.
vii. If the awardee falls out of compliance with the Agency's statutory or regulatory authority, award terms and conditions, or other applicable laws.

3. Termination of a Subaward by the Pass-Through Entity

The pass-through entity may terminate a subaward in whole or in part for one of the following reasons identified in 2 C.F.R. § 200.340:

a. If the subrecipient fails to comply with the terms and conditions of the federal award.
b. With the consent of the subrecipient, in which case the pass-through entity and the subrecipient must agree upon the termination conditions. These conditions include the effective date and, in the case of partial termination, the portion to be terminated.
c. If the pass-through entity's award has been terminated the pass-through recipient will terminate its subawards.

4. Termination by the Recipient or Subrecipient

The recipient or subrecipient may terminate the federal award in whole or in part for the following reason identified in 2 C.F.R. § 200.340: Upon sending FEMA or pass-through entity a written notification of the reasons for such termination, the effective date, and, in the case of partial termination, the portion to be terminated. However, if FEMA or pass-through entity determines that the remaining portion of the federal award will not accomplish the purposes for which the federal award was made, FEMA or pass-through entity may terminate the federal award in its entirety.

5. Impacts of Termination

a. When FEMA terminates the federal award prior to the end of the period of performance due to the recipient's material failure to comply with the terms and conditions of the federal award, FEMA will report the termination in SAM.gov in the manner described at 2 C.F.R. § 200.340(c).
b. When the federal award is terminated in part or its entirety, FEMA or pass-through entity and recipient or subrecipient remain responsible for compliance with the requirements in 2 C.F.R. §§ 200.344 and 200.345.

6. Notification requirements

FEMA or the pass-through entity must provide written notice of the termination in a manner consistent with 2 C.F.R. § 200.341. The federal award will be terminated on the date of the notification unless stated otherwise in the notification.

7. Opportunities to Object and Appeals

   Where applicable, when FEMA terminates the federal award, the written notification of termination will provide the opportunity and describe the process to object and provide information challenging the action, pursuant to 2 C.F.R. § 200.342.

8. Effects of Suspension and Termination

   The allowability of costs to the recipient or subrecipient resulting from financial obligations incurred by the recipient or subrecipient during a suspension or after the termination of a federal award are subject to 2 C.F.R. 200.343.

M. Best Practices

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." 2 C.F.R. § 200.303(e).

N. Payment Information

Recipients will submit payment requests in FEMA GO for FY25 awards under this program.

Instructions to Grant Recipients Pursuing Payments

FEMA reviews all grant payments and obligations to ensure allowability in accordance with 2 C.F.R. § 200.305. These measures ensure funds are disbursed appropriately while continuing to support and prioritize communities who rely on FEMA for assistance. Once a recipient submits a payment request, FEMA will review the request. If FEMA approves a payment, recipients will be notified by FEMA GO and the payment will be delivered pursuant to the recipients SAM.gov financial information. If FEMA disapproves a payment, FEMA will inform the recipient.

Processing and Payment Timeline

FEMA must comply with regulations governing payments to grant recipients. See 2 C.F.R. § 200.305. For grant recipients other than States, 2 C.F.R. § 200.305(b)(3) stipulates that FEMA is to make payments on a reimbursement basis within 30 days after receipt of the payment request, unless FEMA reasonably believes the request to be improper. For state recipients, 2 C.F.R. § 200.305(a) instructs that federal grant payments are governed by Treasury-State Cash Management Improvement Act (CMIA) agreements ("Treasury-State agreement") and default procedures codified at 31 C.F.R. part 205 and Treasury Financial Manual (TFM) 4A-2000, "Overall Disbursing Rules for All Federal Agencies." *See* 2 C.F.R. § 200.305(a).

Treasury-State agreements generally apply to "major federal assistance programs" that are governed by 31 C.F.R. part 205, subpart A and are identified in the Treasury-State agreement. 31 C.F.R. §§ 205.2, 205.6. Where a federal assistance (grant) program is not governed by subpart A, payment and funds transfers from FEMA to the state are subject to 31 C.F.R. part 205, subpart B. Subpart B requires FEMA to "limit a funds transfer to a state to the minimum amounts needed by the state and must time the disbursement to be in accord with the actual, immediate cash requirements of the state in carrying out a federal assistance program or project. The timing and amount of funds transfers must be as close as is administratively feasible to a state's actual cash outlay for direct program costs and the proportionate share of any allowable indirect costs." 31 C.F.R. § 205.33(a). Nearly all FEMA grants are not "major federal assistance programs." As a result, payments to states for those grants are subject to the "default" rules of 31 C.F.R. part 205, subpart B.

If additional information is needed, a request for information will be issued by FEMA to the recipient; recipients are strongly encouraged to respond to any additional FEMA request for information inquiries within three business days. If an adequate response is not received, the request may be denied, and the entity may need to submit a new reimbursement request; this will re-start the 30-day timeline.

Submission Process

All non-disaster grant program reimbursement requests must be reviewed and approved by FEMA prior to drawdowns.

For all non-disaster reimbursement requests (regardless of system), please ensure submittal of the following information:

1. Grant ID / Award Number
2. Total amount requested for drawdown
3. Purpose of drawdown and timeframe covered (must be within the award performance period)
4. Subrecipient Funding Details (if applicable).
    - Is funding provided directly or indirectly to a subrecipient?
        - If **no,** include statement "This grant funding is not being directed to a subrecipient."
    - If **yes**, provide the following details:
        - The name, mission statement, and purpose of each subrecipient receiving funds, along with the amount allocated and the specific role or activity being reimbursed.
        - Whether the subrecipient's work or mission involves supporting aliens, regardless of whether FEMA funds support such activities.
        - Whether the payment request includes an activity involving support to aliens.
        - Whether the subrecipient has any DEI practices.
5. Supporting documentation to demonstrate that expenses are allowable, allocable, reasonable, and necessary under 2 CFR part 200 and in compliance with the grant's NOFO, award terms, and applicable federal regulations.

O. Immigration Conditions

A recipient under this funding opportunity must comply with the FY 2025 Department of Homeland Security Standard Terms and Conditions, v. 3 (Apr. 18, 2025), with the exception Paragraph C.IX (Communication and Cooperation with the Department of Homeland Security and Immigration Officials) and paragraph C.XVII(2)(a)(iii) (Anti-Discrimination Grant Award Certification regarding immigration). Paragraphs C.IX and C.XVII(2)(a)(iii) do not apply to any federal award under this funding opportunity. The FY 2025 Department of Homeland Security Standard Terms and Conditions, v. 3 (Apr. 18, 2025) are available at www.dhs.gov/publication/dhs-standard-terms-and-conditions.

10. Other Information

A. Period of Performance Extension
Extensions to the period of performance are allowed.

See the Preparedness Grants Manual for information on period of performance extensions.

B. Other Information
a. *Environmental Planning and Historic Preservation (EHP) Compliance*
See the Preparedness Grants Manual for information on EHP compliance.

b. *Procurement Integrity*
See the Preparedness Grants Manual for information on procurement integrity.

c. *Financial Assistance Programs for Infrastructure*

1. Recipients and subrecipients must comply with FEMA's implementation requirements of the Build America, Buy America Act (BABAA), which was enacted as part of the Infrastructure Investment and Jobs Act §§ 70901-70927, Pub. L. No. 117-58 (2021); and Executive Order 14005, Ensuring the Future is Made in All of America by All of America's Workers. See also 2 C.F.R. Part 184, Buy America Preferences for Infrastructure Projects and Office of Management and Budget (OMB), Memorandum M-24-02, Implementation Guidance on Application of Buy America Preference in Federal Financial Assistance Programs for Infrastructure.

None of the funds provided under this program may be used for a project for infrastructure unless the iron and steel, manufactured products, and construction materials used in that infrastructure are produced in the United States.

The Buy America preference only applies to articles, materials, and supplies that are consumed in, incorporated into, or affixed to an infrastructure project. As such, it does not apply to tools, equipment, and supplies, such as temporary scaffolding, brought to the construction site and removed at or before the completion of the infrastructure project. Nor does a Buy America preference apply to equipment and furnishings, such as movable chairs, desks, and portable computer equipment, that are used at or within the finished infrastructure project but are not an integral part of the structure or permanently affixed to the infrastructure project.

To see whether a particular FEMA federal financial assistance program is considered an infrastructure program and thus required to implement FEMA's Build America, Buy America

requirements, please see Programs and Definitions: Build America, Buy America Act | FEMA.gov.

2. Waivers

When necessary, recipients (and subrecipients through their pass-through entity) may apply for, and FEMA may grant, a waiver from these requirements.
A waiver of the domestic content procurement preference may be granted by the agency awarding official if FEMA determines that:

- Applying the domestic content procurement preference would be inconsistent with the public interest; or
- The types of iron, steel, manufactured products, or construction materials are not produced in the United States in sufficient and reasonably available quantities or of a satisfactory quality; or
- The inclusion of iron, steel, manufactured products, or construction materials produced in the United States will increase the cost of the overall project by more than 25%.

The process for requesting a waiver from the Buy America preference requirements can be found on FEMA's website at: "Buy America" Preference in FEMA Financial Assistance Programs for Infrastructure | FEMA.gov.

3. Definitions

For definitions of the key terms of the Build America, Buy America Act, please visit Programs and Definitions: Build America, Buy America Act | FEMA.gov.

d. *Mandatory Disclosures*
The non-Federal entity or applicant for a federal award must disclose, in a timely manner, in writing to the federal awarding agency or pass-through entity all violations of federal criminal law involving fraud, bribery, or gratuity violations potentially affecting the Federal award. (2 C.F.R. § 200.113)

e. *Adaptive Support*
See the Preparedness Grants Manual for information on disability integration.

f. *Record Retention*
See the Preparedness Grants Manual for information on record retention.

g. *Actions to Address Noncompliance*
See the Preparedness Grants Manual for information on actions to address noncompliance.

h. *Audits*
See the Preparedness Grants Manual for information on audits.

j. *Protecting Houses of Worship and Public Venues*

The U.S. Department of Homeland Security, Center for Faith (DHS Center) fosters partnerships between government and faith-based organizations (FBOs) to increase the nation's resilience by creating trust and developing relationships. The DHS Center seeks to build bridges across the whole community and to help overcome coordination challenges among FBOs, emergency managers and other stakeholders engaging a broad cross-section of FBOs in all stages of the disaster cycle. The DHS Center serves as a clearinghouse for information, connecting and coordinating with FBOs allowing information to be shared in both directions, informing decision-making at DHS by elevating concerns, ground truth and local situational awareness while providing feedback, updates and guidance to the faith community. Additional resources can be found at https://www.fema.gov/emergency-managers/individuals-communities/faith Faith-Based and Volunteer Partnership Resources.

11. Appendix A: Allowable Costs

A. Planning

Planning costs are allowed under this program only as described in this funding notice and the Preparedness Grants Manual.

Funding may be used for security or emergency planning expenses and the materials required to conduct planning activities. Planning must be related to the protection of the facility and the people within the facility and should include consideration of access and functional needs as well as those with limited English proficiency. Planning efforts can also include conducting risk and resilience assessments on increasingly connected cyber and physical systems, on which security depends, using the Resilience Planning Program | CISA and related Cybersecurity and Infrastructure Security Agency (CISA) resources. Examples of planning activities allowable under this program include:

1. Development and enhancement of security plans and protocols;
2. Development or further strengthening of security assessments;
3. Emergency contingency plans;
4. Evacuation/Shelter-in-place plans;
5. Coordination and information sharing with fusion centers; and
6. Other project planning activities with prior approval from FEMA.

B. Organization

Organization costs are not allowed under this program.

C. Equipment

Equipment costs are allowed under this program only as described in this funding notice and the Preparedness Grants Manual.

Allowable costs are focused on facility hardening and physical security enhancements. Funding can be used for the acquisition and installation of security equipment on real property (including buildings and improvements) owned or leased by the nonprofit organization, specifically in prevention of and/or protection against the risk of a terrorist or other extremist attack. This equipment is **limited to select items** on the Authorized Equipment List (AEL). These items, including the item's plain-language description *specific to the NSGP*, are as follows:

AEL Code	Title	Description
03OE-03-MEGA	System, Public Address, Handheld or Mobile	Systems for mass audio notification, including vehicle-mounted high powered speaker systems, or battery powered megaphone/public address systems with corded microphone.
03OE-03-SIGN	Signs	Restricted access and caution warning signs that preprinted or field printable and can be various colors, sizes, and shapes. Examples can include traffic cones, other free-standing signage, mountable items, and signs and devices for individuals with disabilities and others with access and functional needs (e.g., programmable audible caution cones and scrolling marquis signs).
04AP-05-CRED	System, Credentialing	Software application and associated hardware and material for creating site/event credential badges and controlling scene access. Although some hardware may be required, functionality may also be obtainable via subscription as a cloud-based service, as opposed to purchasing software.
04AP-06-VIDA	Software, Video Analytics	Software, either local or cloud-based, that analyzes video input to detect/determine temporal and spatial events, either in real time or using archival video. Analytical priorities might include recognition or patterns (movement or arrangement or persons, vehicles, or other objects). For the NSGP, license plate reader and facial recognition software are not allowed, but software to detect weapons through video analysis is allowed.
04AP-09-ALRT	Systems, Public Notification and Warning	Systems used to alert the public of protective actions or to provide warning to the public in the event of an incident, such as sirens, the Emergency Alert System (EAS), the Integrated Public Alert and Warning System (IPAWS), and Wireless Emergency Alerts (WEA).
04AP-11-SAAS	Applications, Software as a Service	Sometimes referred to as "on-demand software," this application runs on the provider's servers, delivering functionality via the internet to any device having connectivity and the required browser or interface. Access to the application is obtained via a service subscription rather than outright purchase, with all updates and configuration requirements handled by the service provider. *This item is limited to those services that support security systems such as access controls, camera networks, cybersecurity services or other critical infrastructure security.*
05AU-00-TOKN	System, Remote Authentication	Systems used to provide enhanced remote authentication, often consisting of a server or synchronization scheme and a device, token, or smartphone application.
05EN-00-ECRP	Software, Encryption	Encryption software used to protect stored data files or email messages.
05HS-00-MALW	Software, Malware/Anti-Virus Protection	Software for protection against viruses, spyware, and malicious code. May be obtained for individual hosts or for entire network segments.
05HS-00-PFWL	System, Personal Firewall	Personal firewall for operation on individual workstations. This item is usually a software solution, but appliances are also available. See also: 05NP-00-FWAL.
05NP-00-FWAL	Firewall, Network	Firewall (software or standalone appliance) for use in protecting networks. See also 05HS-00-PFWL.
05NP-00-IDPS	System, Intrusion Detection/Prevention	Intrusion Detection and/or Prevention System deployed at either host or network level to detect and/or prevent

AEL Code	Title	Description
		unauthorized or aberrant (i.e., abnormal) behavior on the network.
06CP-01-PORT	Radio, Portable	Individual/portable radio transceivers, for notifications and alerts.
06CP-01-REPT	Repeater	Electronic device that receives a weak or low-level signal and retransmits that signal to extend usable range.
06CC-02-PAGE	Services/Systems, Paging	Paging services/systems/applications; one-way text messaging for notifications or alerts.
06CP-03-ICOM	Intercom/Intercom System	Communication system for a limited number of personnel in close proximity to receive alerts or notifications
06CP-03-PRAC	Accessories, Portable Radio	Speaker/microphone extensions to portable radios.
10GE-00-GENR	Generators	Generators (gasoline, diesel, propane, natural gas, etc.) and their required installation materials, including 10PE-00-PTSW (a power switch) if not already included, to support a redundant power supply for security systems, alarms, lighting, and other physical security/cybersecurity infrastructure or systems.
13IT-00-ALRT	System, Alert/Notification	Alert/notification software that allows for real-time dissemination of information for situational awareness or alerts among a group via means such as smartphones, landlines, pagers, etc. This item may also be a subscription cloud-based service using a web browser interface or a mobile application instead of a software.
10PE-00-UPS	Supply, Uninterruptible Power (UPS)	Systems that compensate for power loss to serviced equipment (e.g., short-duration battery devices, standby generator devices for longer duration).
14CI-00-COOP	System, Information Technology Contingency Operations	Back-up computer hardware, operating systems, data storage, and application software necessary to provide a working environment for contingency operations. May be a purchased as a remote service or a dedicated alternate operating site.
14EX-00-BCAN	Receptacles, Trash, Blast-Resistant	Blast-resistant trash receptacles.
14EX-00-BSIR	Systems, Building, Blast/Shock/Impact Resistant	Systems to mitigate damage from blasts, shocks, or impacts, such as column and surface wraps, wall coverings, portable or fix ballistic boards/barriers, breakage/shatter resistant glass, window wraps/films/velums, etc.
14SW-01-ALRM	Systems/Sensors, Alarm	Systems and standalone sensors designed to detect access violations or intrusions using sensors such as door/window switches, motion sensors, acoustic sensors, seismic sensors, and thermal sensors. May also include temperature sensors for critical areas.
14SW-01-ASTN	Network, Acoustic Sensor Triangulation	Network of deployed acoustic sensors and one or more processing nodes for data integration and analysis. Such networks can be set to one or more ranges of frequencies to detect sounds such as gunshots, heavy weapons discharge, explosions, man-portable air defense system launches, vehicle noises, etc., and utilize acoustic triangulation to provide accurate location data. Such networks can be wired, wireless, or hybrid, and are capable of operation near critical infrastructure assets or in wide areas.
14SW-01-DOOR	Doors and Gates, Impact Resistant	Reinforced doors and gates with increased resistance to external impact for increased physical security.

AEL Code	Title	Description
14SW-01-LITE	Lighting, Area, Fixed	Fixed high-intensity lighting systems for improved visibility in areas such as building perimeters, parking lots, and other critical zones to increase physical security.
14SW-01-PACS	System, Physical Access Control	Locking devices and entry systems for control of physical access to facilities.
14SW-01-SIDP	Systems, Personnel Identification	Systems for positive identification of personnel as a prerequisite for entering restricted areas or accessing information systems.
14SW-01-SIDV	Systems, Vehicle Identification	Systems for identification of vehicles, ranging from decals to radio frequency identification or other transponder devices. (License plate reader and facial recognition software are NOT allowed.)
14SW-01-SNSR	Sensors/Alarms, System and Infrastructure Monitoring, Standalone	Standalone sensors/alarms for use on critical systems or infrastructure items (e.g., security systems, power supplies, etc.) to provide warning when these systems fail or are near failure.
14SW-01-VIDA	Systems, Video Assessment, Security	Camera-based security systems utilizing standard, low light, or infrared technology. (License plate reader and facial recognition software are NOT allowed.)
14SW-01-WALL	Barriers: Fences; Jersey Walls	Obstacles designed to channel or halt pedestrian or vehicle-borne traffic to protect a physical asset or facility such as barriers, bollards, planters, benches etc. (Earthen barriers, berms, trees, or other botanical obstacles are NOT allowed.)
15SC-00-PPSS	Systems, Personnel/Package Screening	Hand-held or fixed systems such as walk-through magnetometers used to screen personnel and packages for hazardous materials/devices.
21GN-00-INST	Installation	Installation costs for authorized equipment purchased through FEMA grants.
21GN-00-TRNG	Training and Awareness	See Appendix A, Section D "Training and Exercises"

Other dropdowns in the Section IV-B of IJ, while not part of the AEL, include the following:

–Code	Title	Description
Contract Security	Private Contact Security Personnel/Guards	See Appendix A, Section G "Contracted Security Personnel"
M&A	Management and Administration (M&A)	See Section 3.I. "Management and Administration (M&A)"
PLANNING	Planning	See Appendix A, Section A "Planning"
EXERCISE	Exercise	See Appendix A, Section D "Training and Exercises"

Unless otherwise stated, equipment must meet all mandatory statutory, regulatory, and FEMA-adopted standards to be eligible for purchase using these funds, including the Americans with Disabilities Act. In addition, recipients will be responsible for obtaining and maintaining all necessary certifications and licenses for the requested equipment, whether with NSGP funding or other sources of funds (see the Maintenance and Sustainment section below for more information).

Recipients and subrecipients may purchase equipment not listed on the AEL, but **only** if they first seek and obtain **prior approval** from FEMA. Note: Subapplicants should indicate in their

budget narratives if a cost includes shipping and/or tax. It is not required to break the costs out as separate from the relevant purchase(s).

Applicants and subapplicants should analyze the cost benefits of purchasing versus leasing equipment, especially high-cost items and those subject to rapid technical advances. Large equipment purchases must be identified and explained. For more information regarding property management standards for equipment, please reference 2 C.F.R. Part 200, including but not limited to 2 C.F.R. §§ 200.310, 200.313, and 200.316. Also see 2 C.F.R. §§ 200.216, 200.471, and FEMA Policy #405-143-1 – Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services, regarding prohibitions on covered telecommunications equipment or services. Additionally, recipients that are using NSGP funds to support emergency communications equipment activities must comply with the SAFECOM Guidance on Emergency Communications Grants, including provisions on technical standards that ensure and enhance interoperable communications. This SAFECOM Guidance can be found at the Funding and Sustainment page on CISA.gov.

The installation of certain equipment may trigger EHP requirements. Please reference the EHP sections in this NOFO and the Preparedness Grants Manual for more information. Additionally, some equipment installation may constitute construction or renovation. Please see the Construction and Renovation subsection for additional information.

D. Training and Exercises

Training and exercise costs are allowed under this program only as described in this funding notice and the Preparedness Grants Manual.

Subrecipients may use NSGP funds for the following training-related costs:

1. Employed or volunteer security staff to attend security-related training within the United States;
2. Employed or volunteer staff to attend security-related training within the United States with the intent of training other employees or members/congregants upon completing the training (i.e., "train-the-trainer" type courses); and
3. Nonprofit organization's employees, or members/congregants to receive on-site security training.

Allowable training-related costs under the NSGP are limited to attendance fees for training and related expenses, such as materials, supplies, and/or equipment. Overtime, backfill, and travel expenses are **not** allowable costs.

Allowable training topics are limited to the protection of critical infrastructure key resources, including physical and cybersecurity, facility hardening, and terrorism/other extremism awareness/employee preparedness such as Community Emergency Response Team (CERT) training, indicators and behaviors indicative of terrorist/other extremist threats, Active Shooter training, and emergency first aid training. Additional examples of allowable training courses include: "Stop the Bleed" training, kits/equipment, and training aids; First Aid and other novice level "you are the help until help arrives" training, kits/equipment, and training aids; and

Automatic External Defibrillator (AED) and AED/Basic Life Support training, kits/equipment, and training aids.

Training conducted using NSGP funds must address a specific threat and/or vulnerability, as identified in the subapplicant's IJ. Training should provide the opportunity to demonstrate and validate skills learned as well as to identify any gaps in these skills. ***Proposed attendance at training courses and all associated costs using the NSGP must be included in the subapplicant's IJ.***

Funding may be used to conduct security-related exercises. This includes costs related to planning, meeting space and other meeting costs, facilitation costs, materials and supplies, and documentation. Exercises afford organizations the opportunity to validate plans and procedures, evaluate capabilities, and assess progress toward meeting capability targets in a controlled, low risk setting. All shortcomings or gaps—including those identified for children and individuals with access and functional needs—should be identified in an improvement plan. Improvement plans should be dynamic documents with corrective actions continually monitored and implemented as part of improving preparedness through the exercise cycle.

The Homeland Security Exercise and Evaluation Program (HSEEP) provides a set of guiding principles for exercise programs, as well as a common approach to exercise program management, design and development, conduct, evaluation, and improvement planning. For additional information on HSEEP, refer to Homeland Security Exercise and Evaluation Program | FEMA.gov. In accordance with HSEEP guidance, subrecipients are reminded of the importance of implementing corrective actions iteratively throughout the progressive exercise cycle. This link provides access to a sample After Action Report (AAR)/Improvement Plan (IP) template: Improvement Planning – HSEEP Resources – Preparedness Toolkit (fema.gov). Recipients are encouraged to enter their exercise data and AAR/IP in the Preparedness Toolkit.

E. Maintenance and Sustainment

Maintenance and sustainment costs, such as maintenance contracts, warranties, repair or replacement costs, upgrades, and user fees are allowable. For additional information, see the Preparedness Grants Manual.

F. Construction and Renovation

NSGP funding may not be used for construction and renovation projects without prior written approval from FEMA. In some cases, the installation of equipment may constitute construction and/or renovation. If you have any questions regarding whether an equipment installation project could be considered construction or renovation, please contact your Preparedness Officer. All recipients of NSGP funds must request and receive prior approval from FEMA before any NSGP funds are used for any construction or renovation. Additionally, recipients are required to submit a SF-424C Budget and budget detail citing the project costs and an SF-424D Form for standard assurances for the construction project. The total cost of any construction or renovation paid for using NSGP funds may not exceed the greater amount of $1 million or 15% of the NSGP award.

G. Contracted Security Personnel

Contracted security personnel are allowed under this program only as described in this NOFO and must comply with guidance set forth in Information Bulletin 421b and Information Bulletin 441. NSGP funds may not be used to purchase equipment for contracted security.

12. Appendix B: FY 2025 NSGP-UA Eligible High-Risk Urban Areas Allocations

FY 2025 NSGP-UA Eligible High-Risk Urban Areas

State/Territory	High-Risk Urban Area	FY 2025 Allocation	5% for M&A
Arizona	Phoenix Area	$2,761,861	$138,093
California	Anaheim/Santa Ana Area	$991,958	$49,598
	Bay Area	$10,255,429	$512,771
	Los Angeles/Long Beach Area	$7,672,863	$383,643
	Riverside Area	$745,877	$37,294
	Sacramento Area	$1,457,822	$72,891
	San Diego Area	$1,034,416	$51,721
Colorado	Colorado Springs Area	$243,211	$12,161
	Denver Area	$1,995,778	$99,789
District of Columbia	National Capital Region	$6,499,856	$324,993
Florida	Jacksonville Area	$541,963	$27,098
	Miami/Fort Lauderdale Area	$7,768,314	$388,416
	Orlando Area	$891,419	$44,571
	Tampa Area	$1,425,201	$71,260
Georgia	Atlanta Area	$2,349,193	$117,460
Hawaii	Honolulu Area	$312,987	$15,649
Illinois	Chicago Area	$6,308,933	$315,447
Indiana	Indianapolis Area	$807,084	$40,354
Louisiana	New Orleans Area	$269,761	$13,488
Maryland	Baltimore Area	$3,449,969	$172,498
Massachusetts	Boston Area	$373,887	$18,694
Michigan	Detroit Area	$2,756,609	$137,830
Minnesota	Twin Cities Area	$1,064,287	$53,214
Missouri	Kansas City Area	$674,287	$33,714
	St. Louis Area	$813,568	$40,678
Nevada	Las Vegas Area	$739,146	$36,957
New Jersey	Jersey City/Newark Area	$24,769,130	$1,238,457
New York	New York City Area	$29,938,456	$1,496,923
North Carolina	Charlotte Area	$766,531	$38,327
Ohio	Cincinnati Area	$261,630	$13,082
	Cleveland Area	$390,072	$19,504

State/Territory	High-Risk Urban Area	FY 2025 Allocation	5% for M&A
	Columbus Area	$427,968	$21,398
Oregon	Portland Area	$755,024	$37,751
Pennsylvania	Philadelphia Area	$1,326,016	$66,301
	Pittsburgh Area	$917,688	$45,884
Tennessee	Nashville Area	$551,344	$27,567
Texas	Austin Area	$731,575	$36,579
	Dallas/Fort Worth/Arlington Area	$4,212,094	$210,605
	Houston Area	$4,350,649	$217,532
	San Antonio Area	$891,826	$44,591
Virginia	Hampton Roads Area	$554,191	$27,710
	Richmond Area	$426,971	$21,349
Washington	Seattle Area	$1,279,535	$63,977
Wisconsin	Milwaukee Area	$493,621	$24,681

13. Appendix C: FY 2025 NSGP-S Allocations

State/Territory	FY 2025 Allocation	5% for M&A	State/Territory	FY 2025 Allocation	5% for M&A
Alabama	$3,000,000	$150,000	Montana	$1,800,000	$90,000
Alaska	$1,650,000	$82,500	Nebraska	$2,100,000	$105,000
American Samoa	$1,050,000	$52,500	Nevada	$1,800,000	$90,000
Arizona	$2,400,000	$120,000	New Hampshire	$1,950,000	$97,500
Arkansas	$2,400,000	$120,000	New Jersey	$2,250,000	$112,500
California	$5,450,000	$272,500	New Mexico	$2,100,000	$105,000
Colorado	$2,100,000	$105,000	New York	$3,750,000	$187,500
Connecticut	$2,550,000	$127,500	North Carolina	$3,950,000	$197,500
Delaware	$1,800,000	$90,000	North Dakota	$1,800,000	$90,000
District of Columbia	$0	$0	Northern Mariana Islands	$1,050,000	$52,500
Florida	$3,750,000	$187,500	Ohio	$4,050,000	$202,500
Georgia	$3,600,000	$180,000	Oklahoma	$2,700,000	$135,000
Guam	$1,050,000	$52,500	Oregon	$2,250,000	$112,500
Hawaii	$1,650,000	$82,500	Pennsylvania	$3,300,000	$165,000
Idaho	$2,100,000	$105,000	Puerto Rico	$2,400,000	$120,000
Illinois	$3,600,000	$180,000	Rhode Island	$1,800,000	$90,000
Indiana	$3,150,000	$157,500	South Carolina	$3,150,000	$157,500

State/Territory	FY 2025 Allocation	5% for M&A	State/Territory	FY 2025 Allocation	5% for M&A
Iowa	$2,400,000	$120,000	South Dakota	$1,800,000	$90,000
Kansas	$2,100,000	$105,000	Tennessee	$3,150,000	$157,500
Kentucky	$2,850,000	$142,500	Texas	$4,700,000	$235,000
Louisiana	$2,550,000	$127,500	U.S. Virgin Islands	$1,050,000	$52,500
Maine	$1,950,000	$97,500	Utah	$2,550,000	$127,500
Maryland	$1,950,000	$97,500	Vermont	$1,650,000	$82,500
Massachusetts	$3,300,000	$165,000	Virginia	$2,400,000	$120,000
Michigan	$3,150,000	$157,500	Washington	$2,550,000	$127,500
Minnesota	$2,250,000	$112,500	West Virginia	$2,100,000	$105,000
Mississippi	$2,400,000	$120,000	Wisconsin	$2,850,000	$142,500
Missouri	$2,400,000	$120,000	Wyoming	$1,650,000	$82,500

14. Appendix D: Evaluation Criteria and Scoring

SAA Reviewers will score applications based on specific criteria aligned to the NSGP's intent. The table below details the specific criteria aligned to each of the IJ requirements, and the maximum number of points an application can receive for each criterion. The SAA Reviewers will score applications based on specific criteria aligned to the IJ requirements. Each question will be scored based on the complexity within the requirement.

Investment Justification Requirement	Criteria	Score	Explanation
Applicant Information Section			
Did the subapplicant provide all the required information in the Applicant Information Section?	The subapplicant should provide all information as it is applicable in the informational section.	Yes	The subapplicant **did** provide all the required information.
		No	The subapplicant **did not** provide all the required information.
Background Information Section			
Did the subapplicant provide a description of their nonprofit organization to include symbolic value of the site as a highly recognized national or historical institution or significant institution within the community that renders the site as a possible target of terrorism and other extremist attacks?	Subapplicants must describe their organization, its mission/purpose, the symbolic value of the building/organization, and how these factors may make it the target of an attack.	0	The subapplicant **did not provide a description** of the organization including the symbolic value of the site as a highly recognized institution that renders the site a possible target of terrorism or other extremist attacks.
		1	The subapplicant **provided a poor description** of the organization including the symbolic value of the site as a highly recognized institution that

Investment Justification Requirement	Criteria	Score	Explanation
			renders the site a possible target of terrorism or other extremist attacks.
		2	The subapplicant **provided an adequate description** of the organization including the symbolic value of the site as a highly recognized institution that renders the site a possible target of terrorism or other extremist attacks.
		3	The subapplicant **provided a full, clear, and effective description** of the organization including the symbolic value of the site as a highly recognized institution that renders the site a possible target of terrorism or other extremist attacks.
Did the subapplicant provide a description of their nonprofit organization to include any role in responding to or recovering from events that integrate nonprofit preparedness with broader state/local preparedness efforts?	Subapplicants must clearly describe their individual organization's previous or existing role in response to or in recovery efforts to terrorist or other extremist attacks. This should tie into the broader preparedness efforts of state and/or local government.	0	The subapplicant **did not provide a description** of the organization that included any role in responding to or recovering from events that integrate nonprofit preparedness with broader state/local efforts.
		1	The subapplicant **provided some description** of the organization that included any role in responding to or recovering from events that integrate nonprofit preparedness with broader state/local efforts.
		2	The subapplicant **provides a full, clear, and effective description** of the organization that included any role in responding to or recovering from events that integrate nonprofit preparedness with broader state/local efforts.
Risk			
Did the subapplicant discuss specific threats or attacks against the	To substantiate the subapplicant's risk to a terrorist or other	0	The subapplicant **does not discuss specific** threats or attacks against the organization or a

Investment Justification Requirement	Criteria	Score	Explanation
nonprofit organization or closely related organization?	extremist attack, subapplicants may describe incidents that have occurred at or threats that have been made to their organization. Subapplicants may also draw from incidents that have occurred at closely related/similar organizations either domestically or internationally; the subapplicant should make the connection that they are at risk for the same reasons. Local crimes such as burglary, theft, or vandalism without a terrorism, extremism, or hate-related nexus may provide contextual justification for NSGP funding.		closely related organization.
		1	The subapplicant **provided minimal discussion** of threats or attacks against the organization or a closely related organization.
		2	The subapplicant **provided poor discussion** of threats or attacks against the organization or a closely related organization.
		3	The subapplicant **provided adequate discussion** of threats or attacks against the organization or a closely related organization.
		4	The subapplicant **provided good discussion** of threats or attacks against the organization or a closely related organization.
		5	The subapplicant **provided multiple, detailed, and specific** threats or attacks against the organization or a closely related organization.
In considering the vulnerabilities, how well did the subapplicant describe the organization's susceptibility to destruction, incapacitation, or exploitation by a terrorist or other extremist attack?	Subapplicants must provide a clear description of findings from a completed vulnerability assessment.	0	The subapplicant **did not discuss or describe** the organization's susceptibility to attack.
		1	The subapplicant **provided minimal description** of the organization's susceptibility to attack.
		2	The subapplicant **provided poor description** of the organization's susceptibility to attack.
		3	The subapplicant **provided adequate description** of the organization's susceptibility to attack.
		4	The subapplicant **provided good description** of the organization's susceptibility to attack.
		5	The subapplicant **provided**

Investment Justification Requirement	Criteria	Score	Explanation
			clear, relevant, and compelling description of the organization's susceptibility.
In considering potential consequences, how well did the subapplicant address potential negative effects on the organization's asset, system, and/or network if damaged, destroyed, or disrupted by a terrorist or other extremist attack?	Subapplicants should describe how an attack would impact them, the community served, and if possible/applicable, beyond the immediate individuals served (nearby critical infrastructure, businesses, transportation, schools, etc.).	0	The subapplicant **did not discuss or describe** the potential negative consequences the organization may face.
		1	The subapplicant **provided minimal description** of the potential negative consequences the organization may face.
		2	The subapplicant **provided poor description** of the potential negative consequences the organization may face.
		3	The subapplicant **provided adequate description** of the potential negative consequences the organization may face.
		4	The subapplicant **provided good description** of the potential negative consequences the organization may face.
		5	The subapplicant **provided a clear, relevant, and compelling description** of the potential negative consequences the organization may face.
Facility Hardening			
How well does the subapplicant describe the proposed facility hardening activities, projects, and/or equipment and relate their proposals to the vulnerabilities described in the "Risk" Section?	In narrative form, subapplicants must clearly explain what the proposed activities, projects, and/or equipment are, identify their estimated cost, and describe how they will mitigate or address vulnerabilities identified in their vulnerability assessment.	0	The subapplicant **does not propose** facility hardening or the proposals do not mitigate identified risk(s) and/or vulnerabilities.
		1	Proposed activities, projects, or equipment **may provide minimal** facility hardening **or are only minimally related** to some of the identified risk(s) and/or vulnerabilities.
		2	Proposed facility hardening activities, projects, or equipment **would likely mitigate** identified risk(s) and/or vulnerabilities.

Investment Justification Requirement	Criteria	Score	Explanation
		3	Proposed facility hardening activities, projects, or equipment are **clearly aligned with and effectively mitigate** the identified risk(s) and/or vulnerabilities.
Did the subapplicant's proposed facility hardening activity focus on the prevention of and/or protection against the risk of a terrorist or other extremist attack?	The proposed activities, projects, and equipment should directly tie to the prevention of and/or protection against the risk of terrorist or other extremist attacks.	0	The proposed facility hardening activities **do not focus** on the prevention of and/or protection against the risk of terrorist or other extremist attacks.
		1	The proposed facility hardening activities **are somewhat focused** on the prevention of and/or protection against the risk of terrorist or other extremist attacks.
		2	The proposed facility hardening activities **are adequately focused** on the prevention of and/or protection against the risk of terrorist or other extremist attacks.
		3	The proposed facility hardening activities **are clearly and effectively focused** on the prevention of and/or protection against the risk of terrorist or other extremist attacks.
Are all proposed equipment, activities, and/or projects tied to a vulnerability that it could reasonably address/mitigate?	The proposed equipment, activities, and/or projects should mitigate/address the vulnerability tied to it.	0	**No vulnerabilities are listed** and/or the proposed equipment, activities, or projects **do not address listed vulnerabilities**.
		1	The proposed equipment/activities/projects **are somewhat reasonable** to address the listed vulnerability.
		2	The proposed equipment/activities/projects **are mostly reasonable** to address the listed vulnerability.
		3	The proposed equipment/activities/projects **effectively address** the listed

Investment Justification Requirement	Criteria	Score	Explanation
			vulnerability.
Milestones			
How well did the subapplicant describe the milestones and the associated key activities that lead to the milestone event over the NSGP period of performance?	The subapplicant should describe the milestones needed to accomplish the goals of the NSGP funding and should include the key activities that will be necessary to accomplish those milestones.	0	The subapplicant **did not provide** information on milestones and associated key activities.
		1	The subapplicant **provided some description** of milestone events and the associated key activities over the NSGP POP.
		2	The subapplicant **provided adequate description** of milestone events and the associated key activities over the NSGP POP.
		3	The subapplicant **fully and effectively described** milestone events and the associated key activities over the NSGP POP.
Did the subapplicant include milestones and associated key activities that are feasible over the NSGP period of performance?	Milestones should be realistic, potentially include the entire period of performance (36 months), be inclusive of all proposed activities, and consider the Environmental Planning and Historic Preservation review process. Milestones should not exceed 36 months and should not begin prior to the Period of Performance	0	The subapplicant **did not include** milestones and key activities that are feasible over the NSGP POP.
		1	The subapplicant included milestones and key activities that are **somewhat feasible** over the NSGP POP.
		2	The subapplicant included milestones and key activities that **are feasible** over the NSGP POP.
Project Management			
How well did the subapplicant justify the effectiveness of the proposed management team's roles and responsibilities and the governance structure to support implementation of the Investment?	Brief description of the project manager(s) and level of experience.	0	The subapplicant **did not justify** the effectiveness of the proposed management team or the structure in place to support the implementation.
		1	The subapplicant **somewhat justified** the effectiveness of the proposed management team and the structure in place to the

Investment Justification Requirement	Criteria	Score	Explanation
			support implementation.
		2	The subapplicant **fully justified** the effectiveness of the proposed management team and the structure in place to the support implementation.
Impact			
How well did the subapplicant describe the outcomes/outputs that would indicate that the Investment was successful?	Measurable outputs and outcomes should directly link to the vulnerabilities and consequences outlined in the "Risk" Section.	0	The subapplicant **did not describe** the outcomes and/or outputs that would indicate the Investment was successful.
		1	The subapplicant **provided minimal information** on the outcomes and/or outputs that would indicate the Investment was successful.
		2	The subapplicant **provided some information** on the outcomes and/or outputs that would indicate the Investment was successful.
		3	The subapplicant **provided an adequate discussion** of the outcomes and/or outputs that would indicate the Investment was successful.
		4	The subapplicant **provided a full and detailed description** of the outcomes and/or outputs that would indicate the Investment was successful.