The U. S. Department of Homeland Security (DHS)
Notice of Funding Opportunity (NOFO)
Nonprofit Security Grant Program National Security Supplemental
****Modified for sub-applicants****

Program Description

1. **Issued By**
   U.S. Department of Homeland Security (DHS)/Federal Emergency Management Agency (FEMA)/Grant Programs Directorate (GPD)

2. **Assistance Listings Number**
   97.008

3. **Assistance Listings Title**
   Nonprofit Security Grant Program

4. **Funding Opportunity Title**
   Nonprofit Security Grant Program - National Security Supplemental (NSGP-NSS)

5. **Funding Opportunity Number**
   DHS-24-GPD-008-00-98

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

7. **Appropriation Authority for Program**
   National Security Supplemental (Israel Security Supplemental Appropriations Act, 2024, Pub. L. No. 118-50, Title II, Protection, Preparedness, Response, and Recovery).

8. **Announcement Type**
   Initial

9. **Program Category**
   Preparedness: Community Security

10. **Program Overview, Objectives, and Priorities**

    a. **Overview**
    The NSGP-NSS supplements one of three 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. See Section C.3 "Subrecipient Eligibility" for more information.

    DHS is focused on building a national culture of preparedness and protecting against terrorism and other threats to our national security. The threats to our Nation have

evolved during the past two decades. We now face continuous cyber threats by sophisticated actors, threats to soft targets and crowded places, and threats from domestic violent extremists, who represent one of the most persistent threats to the nation today. Therefore, DHS/FEMA has identified one national priority area related to some of the most serious threats that recipients should address with their NSGP-NSS funds: **enhancing the protection of soft targets/crowded places**.

DHS is also focused on forging partnerships to strengthen information sharing and collaboration among federal, state, local, tribal, and territorial law enforcement. There are *no* requirements for information sharing between nonprofit organizations and law enforcement; however, the NSGP-NSS seeks to bring nonprofit organizations into broader state and local preparedness efforts by removing barriers to communication and being more inclusive. DHS/FEMA encourages information sharing, while the goal of the NSGP-NSS is centered on improving and increasing a nonprofit organization's physical/cyber security and facility/target hardening to enhance the protection of soft targets/crowded places. All NSGP-NSS activities must be linked to enhancing the security and safety at the physical site of the nonprofit organization.

b. Goal, Objectives, and Priorities

Goal: The NSGP-NSS will improve and increase the physical/cyber security 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. All NSGP-NSS activities must be linked to enhancing the security and safety at the physical site of the nonprofit organization. Concurrently, the NSGP-NSS will integrate the preparedness activities of nonprofit organizations that are at risk of a terrorist or other extremist attack with broader state and local preparedness efforts.

Objectives: The objective of the NSGP-NSS is to provide funding for physical and cybersecurity enhancements and other security-related activities to nonprofit organizations that are at risk of a terrorist or other extremist attack within the period of performance. The NSGP-NSS also seeks to integrate the preparedness activities of nonprofit organizations with broader state and local preparedness efforts. Lastly, via funding spent on Planning, Organizational, Equipment, Training, and Exercises (POETE) towards enhancing the protection of soft targets and crowded places, the NSGP-NSS seeks to address and close capability gaps identified in individual nonprofit organization Vulnerability Assessments.

Priorities: Given the evolving threat landscape, DHS/FEMA has evaluated the national risk profile and set priorities that help ensure appropriate allocation of scarce security dollars. In assessing the national risk profile, one area warrants the most concern under the NSGP-NSS:

1. Enhancing the protection of soft targets/crowded places.

Likewise, there are several enduring security needs that crosscut the homeland security enterprise. The following are second-tier priority areas that help recipients implement a comprehensive approach to securing communities:

1. Effective planning;
2. Training and awareness campaigns; and

3. Exercises.

A continuing area of concern is the threat posed by malicious cyber actors. Additional resources and information regarding cybersecurity and cybersecurity performance goals are available through the Cybersecurity and Infrastructure Security Agency, Cross-Sector Cybersecurity Performance Goals, and the National Institute of Standards and Technology.

The table below provides a breakdown of these priority areas for the NSGP-NSS, showing both the core capabilities enhanced and lifelines supported, as well as examples of eligible project types for each area. More information on allowable investments can be found in the Funding Restrictions and Allowable Costs section below.

NSGP-NSS 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
	• Cybersecurity
	• 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
		• 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)

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. Alignment to Program Purpose and the DHS and FEMA Strategic Plan
Among the five basic homeland security missions noted in the DHS Strategic Plan for Fiscal Years 2020-2024, NSGP-NSS supports the goal to Strengthen National Preparedness and Resilience.

The 2022-2026 FEMA Strategic Plan outlines three bold, ambitious goals in order to position FEMA to address the increasing range and complexity of disasters, support the diversity of communities we serve, and complement the nation's growing expectations of the emergency management community. The NSGP-NSS supports FEMA's efforts to instill equity as a foundation of emergency management (Goal 1), as well as promote and sustain a ready FEMA and prepared nation (Goal 3). We invite our stakeholders and partners to also adopt these priorities and join us in building a more prepared and resilient nation.

11. Performance Measures
The performance metric for this program is:

- Percentage of funding awarded to the Soft Targets/Crowded Places national priority area by POETE (Planning, Organization, Equipment, Training, and Exercise) solution area, which includes:
  - Funding awarded for contract security;
  - Funding awarded for target hardening;
  - Funding awarded for cybersecurity measures; and
  - Funding awarded for training, awareness campaigns, and exercises.

As noted in the NSGP-NSS's objectives in Section A.10.b, via funding spent on POETE towards enhancing the protection of soft targets and crowded places, the NSGP-NSS seeks to address and close capability gaps identified in individual nonprofit organization Vulnerability Assessments. FEMA will calculate and analyze the above metrics through a review of recipient Biannual Strategy Implementation Report updates and award monitoring to ensure that the funds are expended for their intended purpose and achieve the stated outcomes in the grant application.

B. Federal Award Information

1. Available Funding for the NOFO (Maine only): $1,567,500.00

2. *Projected* Number of Awards: **7**

3. Maximum Award Amount:
Nonprofit organizations must apply through the State of Maine, Emergency Management Agency. See Section C.1 "Eligible Applicants" for more information about sub applicant roles and responsibilities. For NSGP-NSS, 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*. A nonprofit organization with locations in multiple states may apply for up to three sites within each state and funding stream.

If a nonprofit sub applicant 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 will be cause for rejection of the application.

4. **Period of Performance:** 36 months

   Extensions to the period of performance are allowed. For additional information on period of performance extensions, please refer to the Preparedness Grants Manual (FM-207-23-001).

5. **Projected Period of Performance Start Date(s):** 05/01/2025

6. **Projected Period of Performance End Date(s):** 03/31/2028

7. **Projected Budget Period(s)**
   There will be only a single budget period with the same start and end dates as the period of performance.

8. **Funding Instrument Type**: Grant

C. Eligibility Information

1. Eligible Sub applicants

The State is the only eligible applicant to apply for funding to FEMA. Nonprofit organizations are eligible as sub applicants to the Stae. As such, nonprofit organizations must apply for NSGP-NSS through the State, who then submits application information to FEMA.

Additional information on the sub applicant process specific to nonprofit organizations is included in Section D.10 "Content and Form of Application Submission" of this funding notice.

2. Applicant Eligibility Criteria

The SAA is the only eligible applicant.

3. Subawards and Beneficiaries

a. ***Subaward Allowability***
Subawards are allowed under the NSGP-NSS. Once the State receives that grant award, all funds subsequently provided to eligible nonprofit organizations are considered subawards.

b. ***Subrecipient Eligibility***
Nonprofit organizations eligible as **sub applicants to the State** are those organizations that are:

1. 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)

2. Able to demonstrate, through the application, that the organization is at risk of a terrorist or other extremist attack; and

Examples of eligible sub applicant organizations can include houses of worship, educational institutions, senior centers, community centers, day camps, medical facilities, and museums, among many others.

Sub applicants may <u>NOT</u> apply to FEMA directly.

Additionally, the final beneficiary of the NSGP-NSS grant award must be an eligible nonprofit organization and cannot be a for-profit/fundraising extension of a nonprofit organization or organizations. While these for-profit or fundraising extensions may be associated with the eligible nonprofit organization or organizations, NSGP-NSS 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.

c. ***Other Subaward Information***

Please see the following sections for additional information on requirements or restrictions related to subawards/subrecipients:

- Section D.4 “Requirements: Obtain a Unique Entity Identifier (UEI) and Register in the System for Award Management”;
- Section D.12 “Funding Restrictions and Allowable Costs”;
- Section E.1 “Application Evaluation Criteria”;
- Section E.2 “Review and Selection Process”;

- Section F.4.b "Ensuring the Protection of Civil Rights";
- Section F.6 "Monitoring and Oversight";
- Section G.1.f "Environmental Planning and Historic Preservation";
- Section H.1 "Terminations Provisions";
- Section H.2 "Program Evaluation."; and
- Section H.3 "Financial Assistance Programs for Infrastructure."

d. ***Beneficiaries or Participants***
This NOFO and any subsequent federal awards create no rights or causes of action for any participant or beneficiary.

4. Cost Share or Match
There is no cost share requirement for the NSGP-NSS. Sub applicants that propose a cost share will not receive additional consideration in the scoring.

D. Application and Submission Information

1. Key Dates and Times

a. ***Application Start Date:*** 1/15/2024
b. ***Application Submission Deadline:*** 12/31/2024
c. All applications **must** be received by the established deadline.

The State of Maine will not review applications that are received after the deadline or consider these late applications for funding.

2. Agreeing to Terms and Conditions of the Award
By submitting an application, sub applicants agree to comply with the requirements of this NOFO and the terms and conditions of the award, should they receive an award.

3. Address to Request Application Package
Applications are processed through the State application system. To access the system, go to https://webportalapp.com/sp/mema-fy24-nsgps .

a. ***Program-Specific Required Forms and Information*** The following program-specific forms or information are required to be submitted in As part of the NSGP-NSS application, each eligible sub applicant must submit the three documents below by the deadline.

I. NSGP-NSS IJ
Nonprofit organizations with one site may apply for up to $200,000 for that site. Nonprofit organizations 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 B.3 for more information about this maximum. ***If a nonprofit sub applicant applies for multiple sites, it must submit one complete IJ per each site.*** [2] ***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 on the MEMA website. The IJ must describe each investment proposed for funding. The investments or projects described in the IJ

must:

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

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

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

II. VULNERABILITY/RISK ASSESSMENT

Each sub applicant must include a vulnerability/risk assessment **unique to the site** the IJ is being submitted for.

III. MISSION STATEMENT

Each sub applicant 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 sub applicant's self-identification in the IJ to validate that the organization is one of the following types: 1) Ideology-based/Spiritual/Religious (Houses of Worship, Educational Institutions, Medical Facilities, etc.); 2) Educational (secular); 3) Medical (secular); or 4) Other. The organization type is a factor when calculating the final score of the application; see Section E "Application Review Information," subsection "Final Score."

4. Funding Restrictions and Allowable Costs

All costs charged to awards covered by this NOFO must comply with the Uniform Administrative Requirements, Cost Principles, and Audit Requirements at 2 C.F.R. Part 200, unless otherwise indicated in the NOFO, the terms and conditions of the award, or the Preparedness Grants Manual. This includes, among other requirements, that costs must be incurred, and products and services must be delivered, within the period of performance of the award. *See* 2 C.F.R. § 200.403(h) (referring to budget periods, which for FEMA awards under this program is the same as the period of performance).

Federal funds made available through this award may be used for the purpose set forth in this NOFO, the Preparedness Grants Manual, and the terms and conditions of the award and must be consistent with the statutory authority for the award. Award funds may not be used for matching funds for any other federal awards, lobbying, or intervention in federal regulatory or adjudicatory proceedings. In addition, federal funds may not be used to sue the Federal Government or any other government entity. See the Preparedness Grants Manual for more information on funding restrictions and allowable costs.

a. *Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services*

See the Preparedness Grants Manual for information on prohibitions on expending FEMA award funds for covered telecommunications equipment or services.

b. *Pre-Award Costs*

Subrecipients cannot claim pre-award costs.

b. *Management and Administration (M&A) Costs*

M&A costs are allowed by the National Security Supplemental (*Israel Security Supplemental Appropriations Act, 2024*). M&A costs are for activities directly related to the management and administration of the award. M&A activities are those defined as directly relating to the management and administration of NSGP-NSS funds, such as financial management and monitoring. M&A expenses must be based on actual expenses or known contractual costs. Requests that are simple percentages of the award, without supporting justification, will not be allowed or considered for reimbursement. M&A costs for the NSGP-NSS are calculated as up to 5% of the total award allocated, not on final expenditures at close out.

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.

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

c. Direct Costs

I. 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 CISA resources. Examples of planning activities allowable under this program include:

i. Development and enhancement of security plans and protocols;
ii. Development or further strengthening of security assessments;
iii. Emergency contingency plans;
iv. Evacuation/Shelter-in-place plans;
v. Coordination and information sharing with fusion centers; and
vi. Other project planning activities with prior approval from FEMA.

II. ORGANIZATION

Organization costs are not allowed under this program.

III. 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-NSS*, 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

AEL Code	Title	Description
		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 unauthorized or aberrant (i.e., abnormal) behavior on the network.

AEL Code	Title	Description
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

AEL Code	Title	Description
		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.
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.)

AEL Code	Title	Description
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 Section D.12.f.iv "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 Section D.12.f.vii "Contracted Security Personnel"
M&A	Management and Administration (M&A)	See Section D.12.c "Management and Administration (M&A)"
PLANNING	Planning	See Section D.12.f.i "Planning"
EXERCISE	Exercise	See Section D.12.f.iv "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-NSS funding or other sources of funds (see the Maintenance and Sustainment section below for more information).

Sub applicants 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.

The Installation of certain equipment may trigger Environmental Planning and Historic Preservation (EHP) requirements. Please reference the EHP sections in this NOFO and the Preparedness Grants Manual for more information.

IV. 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-NSS funds for the following training-related costs:

vii. Employed or volunteer security staff to attend security-related training within the United States;
viii. 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
ix. Nonprofit organization's employees, or members/congregants to receive on-site security training.

Allowable training-related costs under the NSGP-NSS 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-NSS funds must address a specific threat and/or vulnerability, as identified in the sub applicant's Investment Justification (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-NSS must be included in the sub applicant'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.

V. 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.

VI. CONSTRUCTION AND RENOVATION

NSGP-NSS 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. All sub recipients of NSGP-NSS funds must request and receive prior approval from FEMA before any NSGP-NSS funds are used for any construction or renovation

VII. 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 IB 441. NSGP-NSS funds may not be used to purchase equipment for contracted security.

d. *Unallowable Costs*

The following projects and costs are considered **ineligible** for award consideration:

- Organization costs, and operational overtime costs;
- Hiring of public safety personnel;
- 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 IJ;
- Initiatives in which federal agencies are the beneficiary or that enhance federal property;
- Initiatives which study technology development;
- Proof-of-concept initiatives;
- Initiatives that duplicate capabilities being provided by the Federal Government;
- Organizational operating expenses;
- Reimbursement of pre-award security expenses (see Section D.12.b);
- Cameras for license plate readers/license plate reader software;
- Cameras for facial recognition software;
- Weapons or weapons-related training; and
- Knox boxes.

E. Application Review Information

1. Application Evaluation Criteria

a. *Programmatic Criteria*

NSGP-NSS-S 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(s) (project description and justification) addresses the identified risk(s).

The following are the NSGP-NSS-S evaluation process and criteria:

- 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 sub applicant based on their ideology, beliefs, and/or mission as: 1) an ideology-based/spiritual/religious (houses of worship, educational institutions, medical facilities, etc.); 2) educational (secular); 3) medical (secular); or 4) other nonprofit entity;
- Heightened threat resulting from the Israel-Hamas war;
- 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 sub applicant 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 sub applicant's vulnerability assessment(s);
- 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
- Demonstration that the sub applicant is located within a disadvantaged community; see Section E, Application Review Information – Review and Selection Process, for additional information on how this demonstration will affect scores.

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.

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

b. ***Financial Integrity Criteria***

Prior to making a federal award, FEMA is required by 31 U.S.C. § 3354, as enacted by the Payment Integrity Information Act of 2019, Pub. L. No. 116-117 (2020); 41 U.S.C. § 2313; and 2 C.F.R. § 200.206 to review information available through any Office of Management and Budget (OMB)-designated repositories of governmentwide eligibility qualification or financial integrity information, including whether SAM.gov identifies the applicant as being excluded from receiving federal awards or is flagged for any integrity record submission. FEMA may also pose additional questions to the applicant to aid in conducting the pre-award risk review. Therefore, application evaluation criteria may include the following risk-based considerations of the applicant:

i. Financial stability.
ii. Quality of management systems and ability to meet management standards.
iii. History of performance in managing federal award.
iv. Reports and findings from audits.
v. Ability to effectively implement statutory, regulatory, or other requirements.

c. ***Supplemental Financial Integrity Criteria and Review***

Prior to making a federal award where the anticipated total federal share will be greater than the simplified acquisition threshold, currently $250,000:

i. FEMA is required by 41 U.S.C. § 2313 and 2 C.F.R. § 200.206(a)(2) to review and consider any information about the applicant, including information on the applicant's immediate and highest-level owner, subsidiaries, and predecessors, if applicable, that is in the designated integrity and performance system accessible through the System for Award Management (SAM), which is currently the Federal Awardee Performance and Integrity Information System (FAPIIS).

ii. An applicant, at its option, may review information in FAPIIS and comment on any information about itself that a federal awarding agency previously entered.

iii. FEMA will consider any comments by the applicant, in addition to the other information in FAPIIS, in making a judgment about the applicant's integrity, business ethics, and record of performance under federal awards when completing the review of risk posed by applicants as described in 2 C.F.R. § 200.206.

d. Security Review

DHS Intelligence and Analysis receives a list of potential NSGP-NSS 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. 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.

2. Review and Selection Process

e. *NSGP-NSS-S Process*

State Review

Application packages are submitted by the sub applicant to the State based on the established criteria. The State will review applications and recommend to DHS/FEMA which sub applicants should be selected for funding. As part of the state review, the State must:

- Conduct an eligibility review;
- Review and score only **complete** application packages (including mission statements and vulnerability assessments using the NSGP-NSS Scoring Criteria provided by DHS/FEMA;
- Validate the **self-certified organization type listed in the IJ** by assessing the central purpose of the nonprofit organization(s) described in the mission statement(s);
- Prioritize all NSGP-NSS IJs by ranking each IJ. Each IJ will receive a **unique rank** (#1 [one] being the highest ranked through the total number of applications scored)

- Submit the results of the review of **complete applications from eligible sub applicants** to DHS/FEMA using the Prioritization Tracker;
- Submit sub applicant application details for ***applications received but not recommended for funding (including incomplete applications and ineligible sub applicants), as well as justification as to why they are not being recommended for funding*** to DHS/FEMA using the Prioritization Tracker (IJs for applications not being recommended for funding should not be submitted to FEMA);
- Submit all IJs, even those that are not recommended for funding;
- Record all IJs received and total budget requests in the prioritization tracker, including those *not* recommended for funding, such as incomplete IJs and IJs from sub applicants deemed ineligible; and
- Retain the mission statements and vulnerability assessments submitted by each sub applicant.

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

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

The State reviewers will score each question in the IJ according to the scoring matrix in Appendix A.

Federal Review
The IJs submitted by each State will be reviewed by DHS/FEMA federal staff. Federal staff will also verify that the sub applicant is located outside of a FY 2024 UASI-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 sub applicant applying per Section E.1.d "Security Review."

Final Score
To calculate an application's final score, the sub applicant's State score will be multiplied:

- By a factor of four for nonprofit organizations facing heightened threat resulting from the Israel-Hamas war ***(sub applicants must draw a clear connection between the heightened threat they face and the Israel-Hamas war in their project narratives to qualify for this multiplier)***.

  Any nonprofit organization that can demonstrate it faces heightened threat resulting from the Israel-Hamas war is eligible for this multiplier, regardless of the organization's purpose, mission, viewpoint, membership, or affiliations. Below are a few illustrative examples of scenarios that may qualify a nonprofit organization for this multiplier.:

  - A Nonprofit organization that can demonstrate a clear threat of violence based on its actual or perceived views, positions, or advocacy related to aspects of the Israel-Hamas war.
  - A private, secular university that faces threats from violent extremists that are associated with increased protest activity relating to the Israel-Hamas war, resulting in the need for additional public safety assets.
  - An Arab organization that has been targeted, due to its ethnic affiliation, by violent extremists through online hate referencing the Israel-Hamas war.
  - A Jewish day school that was vandalized by violent extremists seeking to commit attacks based on the Israel-Hamas war.
  - An LGBTQI+ organization that faced violent protests during Pride events related to aspects of the Israel-Hamas war.
  - A mosque that has received threats of violence based on the worldwide unrest because of the ongoing Israel-Hamas war.
  - A Sikh organization where a violent extremist attempted to access a holiday celebration due to the organization's perceived position on the

Israel-Hamas war.

These cases are merely illustrative, not exhaustive, of the types of nonprofits and conditions under which this multiplier would apply. For sub applicants who claim this multiplier, they must draw a clear connection between the heightened threat they face due to the ongoing conflict in the Middle East, though descriptive examples of real-word situations to include, but not limited to, supporting documents such as insurance claims, threat reporting, police reports, and online threats. ***Note: This multiplier is specific to the NSGP-NSS funding opportunity only.***

- By a factor of three for ideology-based/spiritual/religious entities (e.g., houses of worship, ideology-based/spiritual/religious educational institutions, ideology-based/spiritual/religious medical facilities);
- By a factor of two for secular educational and medical institutions; and
- By a factor of one for all other nonprofit organizations.

To advance considerations of equity in awarding NSGP-NSS grant funding, FEMA will add 10 additional points to the scores of sub applicants that are located within a disadvantaged community. FEMA will apply the Council on Environmental Quality's Climate and Economic Justice Screening Tool (CEJST)[4] to each sub applicant using the address of their physical location. FEMA will add 10 points to applications from organizations in communities identified as "disadvantaged" by CEJST. Only the lead nonprofit organization in a is evaluated using CEJST.

Sub applicants will be selected from highest to lowest scored within their respective state/territory until the available state target allocation has been exhausted. In the event of a tie during the funding determination process, priority will be given to sub applicants located in disadvantaged communities, then those that have not received prior year funding, and then those prioritized highest by their State. Should additional NSGP-NSS-S funding remain unobligated after reviewing all state/territory submissions, FEMA will use the final scores, in part, to determine how the remaining balance of funds will be allocated. Submissions will be selected for funding until the remaining balance of funds is exhausted.

DHS/FEMA will use the final results to make funding recommendations to the Secretary of Homeland Security. All final 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.

F. Federal Award Administration Information

1. Notice of Award

See the Preparedness Grants Manual for information on Notice of Award.
FEMA will provide the federal award package to the State electronically via FEMA GO. Award packages include an Award Letter, Summary Award Memo, Agreement Articles, and Obligating Document. An email notification of the award package will be sent through

FEMA's grant application system to the State's authorized representative that submitted the application.

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

3. **Required Notice of Non-Selection**
   Starting in FY 2024, SAAs are required to inform sub applicants of their non-selection **no later than 90 days** from the date they accept their NSGP-NSS award.

4. **Administrative and National Policy Requirements**
   In addition to the requirements of in this section and in this NOFO, FEMA may place specific terms and conditions on individual awards in accordance with 2 C.F.R. Part 200.

   a. ***DHS Standard Terms and Conditions***
   All successful applicants and sub applicant s for DHS grant and cooperative agreements are required to comply with DHS Standard Terms and Conditions, which are available online at: DHS Standard Terms and Conditions.

   The applicable DHS Standard Terms and Conditions will be those in effect at the time the award was made. What terms and conditions will apply for the award will be clearly stated in the award package at the time of award.

   b. ***Ensuring the Protection of Civil Rights***
   As the Nation works towards achieving the National Preparedness Goal, it is important to continue to protect the civil rights of individuals. Recipients and subrecipients must carry out their programs and activities, including those related to the building, sustainment, and delivery of core capabilities, in a manner that respects and ensures the protection of civil rights for protected populations.

   Federal civil rights statutes, such as Section 504 of the Rehabilitation Act of 1973 and Title VI of the Civil Rights Act of 1964, along with DHS and FEMA regulations, prohibit discrimination on the basis of race, color, national origin, sex, religion, age, disability, limited English proficiency, or economic status in connection with programs and activities receiving federal financial assistance from FEMA, as applicable.

   The DHS Standard Terms and Conditions include a fuller list of the civil rights provisions that apply to recipients. These terms and conditions can be found in the DHS Standard Terms and Conditions. Additional information on civil rights provisions is available at https://www.fema.gov/about/offices/equal-rights/civil-rights.

   Monitoring and oversight requirements in connection with recipient compliance with federal civil rights laws are also authorized pursuant to 44 C.F.R. Part 7 or other applicable regulations.

   In accordance with civil rights laws and regulations, recipients and subrecipients must

ensure the consistent and systematic fair, just, and impartial treatment of all individuals, including individuals who belong to underserved communities that have been denied such treatment.

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

d. ***Mandatory Disclosures***
The applicant (State) for a Federal award must disclose, in a timely manner, in writing to the Federal awarding agency, the agency's Office of Inspector General, or pass-through entity if applicable, all violations, and whenever it has credible evidence, of Federal criminal law involving conflicts of interest, fraud, bribery, or gratuity violations potentially affecting the Federal award. (2 C.F.R. § 200.113)

Please note applicants and recipients may report issues of fraud, waste, abuse, and mismanagement, or other criminal or noncriminal misconduct 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.

5. Reporting
Recipients are required to submit various financial and programmatic reports as a condition of award acceptance. Future awards and funds drawdown may be withheld if these reports are delinquent.

See the Preparedness Grants Manual for information on reporting requirements.

6. Monitoring and Oversight
The regulation at 2 C.F.R. § 200.337 provides DHS and any of its authorized representatives with the right of access to any documents, papers, or other records of the recipient [and any subrecipients] that are pertinent to a federal award in order to make audits, execute site visits, or for 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. Pursuant to this right and per 2 C.F.R. § 200.329, DHS may conduct desk reviews and make site visits to review project accomplishments and management control systems to evaluate project accomplishments and to provide any required technical assistance. During site visits, DHS may review a recipient's or subrecipient's files pertinent to the federal award and interview and/or discuss these files with the recipient's or subrecipient's personnel. Recipients and subrecipients must respond in a timely and accurate manner to DHS requests for information relating to a federal award.

See the Preparedness Grants Manual for information on monitoring and oversight.

7. Protecting Houses of Worship and Public Venues
Across the United States, Americans congregate in faith-based venues to worship, learn, play, and bond as a community. However, public gatherings are vulnerable, and adversaries may perceive houses of worship as attractive targets where they can inflict mass casualties, cause substantial psychological impacts, and draw extensive media coverage. The DHS Center for Faith-Based & Neighborhood Partnerships (DHS Center) partners with

interagency and whole community partners to offer numerous resources to assist faith-based and community organizations with their efforts to prepare for all types of hazards, whether natural or man-made. Technical assistance is provided through presentations, workshops, training, webinars, tabletop exercises, and training. Access to these free resources can be found at DHS Center for Faith-Based and Neighborhood Partnerships Resources | FEMA.gov.

8. **Important Changes to Procurement Standards in 2 C.F.R. Part 200**
   On April 22, 2024, OMB updated various parts of Title 2 of the Code of Federal Regulations, among them the procurement standards. These revisions apply to all FEMA awards with a federal award date or disaster declaration date on or after October 1, 2024, unless specified otherwise. The changes include updates to the federal procurement standards, which govern how FEMA award recipients and subrecipients must purchase under a FEMA award.

   More information on OMB's revisions to the federal procurement standards can be found in Purchasing Under a FEMA Award: 2024 OMB Revisions Fact Sheet.

Appendix A: Evaluation Criteria and Scoring

State Reviewers will score applications based on specific criteria aligned to the NSGP-NSS'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 sub applicant provide all the required information in the Applicant Information Section?	The sub applicant should provide all information as it is applicable in the informational section.	Yes	The sub applicant **did** provide all the required information.
		No	The sub applicant **did not** provide all the required information.
Background Information Section			
Did the sub applicant provide a description of their organization to include symbolic value as a highly recognized national or historical institution or significant institution within the community that renders the sub applicant as a possible target of terrorism and other extremist attacks?	Sub applicants must describe their organization, its mission/purpose, the symbolic value of the building(s)/organization(s), and how these factors may make it the target of an attack.	0	The sub applicant **did not provide a description** of the organization including the symbolic value as a highly recognized institution that renders the sub applicant a possible target of terrorism or other extremist attacks.
		1	The sub applicant **provided a poor description** of the organization including the symbolic value as a highly recognized institution that renders the sub applicant a possible target of terrorism or other extremist attacks.
		2	The sub applicant **provided an adequate description** of the organization including the symbolic value as a highly recognized institution that renders the sub applicant a possible target of terrorism or other extremist attacks.

Investment Justification Requirement	Criteria	Score	Explanation
		3	The sub applicant **provided a full, clear, and effective description** of the organization including the symbolic value as a highly recognized institution that renders the sub applicant a possible target of terrorism or other extremist attacks.
Did the sub applicant provide a description of their organization to include any role in responding to or recovering from events that integrate organization preparedness with broader state/local preparedness efforts?	Sub applicants 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 sub applicant **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 sub applicant **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 sub applicant **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 sub applicant self-identify as facing heightened threat resulting from the Israel-Hamas war?		No	The sub applicant **does not self-identify** as facing heightened threat resulting from the Israel-Hamas war.
		Yes	The sub applicant **self-identifies** as facing heightened threat resulting

Investment Justification Requirement	Criteria	Score	Explanation
			from the Israel-Hamas war.
Did the sub applicant discuss specific threats or attacks against the organization, a closely related organization?	To substantiate the sub applicant's risk to a terrorist or other extremist attack, sub applicants may describe incidents that have occurred at or threats that have been made to their organization. Sub applicants may also draw from incidents that have occurred at closely related/similar organizations either domestically or internationally; the sub applicant 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-NSS funding.	0	The sub applicant **does not discuss specific** threats or attacks against the organization, or a closely related organization.
		1	The sub applicant **provided minimal discussion** of threats or attacks against the organization, or a closely related organization.
		2	The sub applicant **provided poor discussion** of threats or attacks against the organization, or a closely related organization.
		3	The sub applicant **provided adequate discussion** of threats or attacks against the organization, or a closely related organization.
		4	The sub applicant **provided good discussion** of threats or attacks against the organization, or a closely related organization.
		5	The sub applicant **provided multiple, detailed, and specific** threats or attacks against the organization, or a closely related organization.
In considering the vulnerabilities, how well did the sub applicant describe	Sub applicants must provide a clear description of findings from a	0	The sub applicant **did not discuss or describe** the organization's susceptibility to

Investment Justification Requirement	Criteria	Score	Explanation
the organization 's susceptibility to destruction, incapacitation, or exploitation by a terrorist or other extremist attack?	completed vulnerability assessment(s).		attack.
		1	The sub applicant **provided minimal description** of the organization's susceptibility to attack.
		2	The sub applicant **provided poor description** of the organization's susceptibility to attack.
		3	The sub applicant **provided adequate description** of the organization's susceptibility to attack.
		4	The sub applicant **provided good description** of the organization's susceptibility to attack.
		5	The sub applicant **provided clear, relevant, and compelling description** of the organization's susceptibility.
In considering potential consequences, how well did the sub applicant 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?	Sub applicant s 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 sub applicant **did not discuss or describe** the potential negative consequences the organization may face.
		1	The sub applicant **provided minimal description** of the potential negative consequences the organization may face.
		2	The sub applicant **provided poor description** of the potential negative consequences the

Investment Justification Requirement	Criteria	Score	Explanation
			organization may face.
		3	The sub applicant **provided adequate description** of the potential negative consequences the organization may face.
		4	The sub applicant **provided good description** of the potential negative consequences the organization may face.
		5	The sub applicant **provided a clear, relevant, and compelling description** of the potential negative consequences the organization may face.
Facility Hardening			
How well does the sub applicant 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, sub applicant s 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 sub applicant **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.
		3	Proposed facility hardening activities, projects, or equipment are **clearly aligned with and effectively**

Investment Justification Requirement	Criteria	Score	Explanation
			mitigate the identified risk(s) and/or vulnerabilities.
Did the sub applicant '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

Investment Justification Requirement	Criteria	Score	Explanation
			vulnerability.
		3	The proposed equipment/activities/projects **effectively address** the listed vulnerability.
Milestones			
How well did the sub applicant describe the milestones and the associated key activities that lead to the milestone event over the NSGP-NSS period of performance?	The sub applicant should describe the milestones needed to accomplish the goals of the NSGP-NSS funding and should include the key activities that will be necessary to accomplish those milestones.	0	The sub applicant **did not provide** information on milestones and associated key activities.
		1	The sub applicant **provided some description** of milestone events and the associated key activities over the NSGP-NSS POP.
		2	The sub applicant **provided adequate description** of milestone events and the associated key activities over the NSGP-NSS POP.
		3	The sub applicant **fully and effectively described** milestone events and the associated key activities over the NSGP-NSS POP.
Did the sub applicant include milestones and associated key activities that are feasible over the NSGP-NSS 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 sub applicant **did not include** milestones and key activities that are feasible over the NSGP-NSS POP.
		1	The sub applicant included milestones and key activities that are **somewhat feasible** over the NSGP-NSS POP.
		2	The sub applicant included milestones and key activities that **are feasible** over the NSGP-NSS POP.
Project Management			
How well did the sub applicant justify the effectiveness of the	Brief description of the project manager(s) and level of experience.	0	The sub applicant **did not justify** the effectiveness of the proposed management

Investment Justification Requirement	Criteria	Score	Explanation
proposed management team's roles and responsibilities and the governance structure to support implementation of the Investment?			team or the structure in place to support the implementation.
		1	The sub applicant **somewhat justified** the effectiveness of the proposed management team and the structure in place to the support implementation.
		2	The sub applicant **fully justified** the effectiveness of the proposed management team and the structure in place to the support implementation.
Impact			
How well did the sub applicant 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 sub applicant **did not describe** the outcomes and/or outputs that would indicate the Investment was successful.
		1	The sub applicant **provided minimal information** on the outcomes and/or outputs that would indicate the Investment was successful.
		2	The sub applicant **provided some information** on the outcomes and/or outputs that would indicate the Investment was successful.
		3	The sub applicant **provided an adequate discussion** of the outcomes and/or outputs that would indicate the Investment was successful.
		4	The sub applicant **provided a full and detailed description** of the outcomes and/or outputs that would indicate the Investment was successful.