Fiscal Year (FY) 2026 Nonprofit Security Grant Program (NSGP)

Notice of Funding Opportunity for Subrecipients

1. Program Overview & Description

Executive Summary

The FY 2026 Nonprofit Security Grant Program (NSGP) enhances the physical/cybersecurity and facility/target hardening of nonprofit organizations' facilities at risk of terrorist or other extremist attacks, ultimately safeguarding the lives and property of the American people.

Key Dates

- Projected Application Start Date: July 1, 2026
- Projected Application End Date: July 16, 2026
- Projected Period of Performance & Budget Period: September 1, 2026 – August 31, 2029

Application Instructions

Applications are submitted via email to the grant inbox. **The subject line MUST say "FEMA FY26 NSGP, (organization name).**

Funding Limits & Cost Share

- Maximum Per Site: A nonprofit organization may apply for up to $200,000 per site/location/physical address per application.
- Multiple Sites: Organizations with multiple physical addresses may apply for up to three sites per funding stream (NSGP-S and NSGP-UA), at a maximum of $200,000 per site, not to exceed $600,000 total per state.
- Cost Share: There is no cost share or matching requirement for the FY 2026 NSGP.

Goals & Objectives:

This program 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: NSGP, 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:

a. 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. 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.

b. 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.

    i. 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.

    ii. Equipment– Strengthening security infrastructure, technology, and protective measures.

    iii. Training & Exercises – long-term vulnerability reduction via preparedness training, public information and warning enhancement, and threat response exercises.

c. Strengthen relationships across nonprofit organizations, state, local, and territorial homeland security agencies for a whole community approach to preparedness. 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 on FY 2026 NSGP Funding Priorities.

2. Subrecipient Eligibility Criteria

To be eligible for a subaward under this program, an organization must meet the following criteria:

- **Tax-Exempt Status:** Must be described under section 501(c)(3) of the Internal Revenue Code of 1986 (IRC) and exempt from tax under section 501(a).

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 not require recognition of exemption, if 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)

- **Risk Profile:** Must be able to demonstrate through its application that the organization is at high risk of a terrorist or other extremist attack.
- **Eligible Types:** Examples include houses of worship, museums, educational facilities, senior centers, community centers, and day camps.

Registration Requirements

Sub-applicants must establish and maintain active accounts across the following systems to be eligible for funding consideration:

- **SAM.gov:** Must have an active account and a Unique Entity Identifier (UEI). Registration must be renewed annually.
- **Employer Identification Number (EIN):** Must obtain an EIN from the IRS.
- **Login.gov:** Required to access and log into SAM.gov.
- **Grants.gov:** Active account required for downloading relevant program packages.

Personnel Restrictions & Requirements

- **Foreign Nationals:** Subrecipients should not include foreign nationals or noncitizens. If an organization employs foreign nationals, they must be properly vetted and adhere to all government statutes and security requirements (including "staff American, stay in America").
- **Biographies & Resumes:** Subrecipients must submit short bios and resumes for organizational leadership and board members, including names, business addresses, and entity types. All resumes are subject to approval. There is a template provided online.

3. Application Contents & Submission Requirements

As part of the FY 2026 NSGP application, each eligible nonprofit must submit the following four documents:

NSGP Investment Justification Form (IJ)

Nonprofit sub-applicants with one site may apply for up to $200,000 for that site. Nonprofit sub-applicants with multiple sites may apply for up to $200,000 per site, for up to three sites per funding stream, with a maximum of $600,000 per state. If applying for multiple sites, a nonprofit sub-applicant must submit a separate, complete IJ for each site. IJs cannot include more than one physical site.

A fillable IJ form is available on the MEMA NSGP webpage. Each IJ must describe the 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 similar projects are submitted 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 sub-applicants 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

Vulnerability/Risk Assessment

Each nonprofit sub-applicant must include a site-specific vulnerability/risk assessment unique to the site for which the IJ is submitted.

Mission Statement

Each nonprofit 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 nonprofit sub-applicant'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

Biographies & Resumes

Subrecipients must submit short bios and resumes for organizational leadership and board members, including names, business addresses, and entity types. All resumes are subject to approval. **There is a template provided online.**

Application Review Information

Application Review Information:

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.

Nonprofit organizations must submit their FY 2026 NSGP applications by July 16th, 2026 by 11:59PM (EST). 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). The State will make recommendations to DHS/FEMA based on the State scores.

The following are the FY 2026 NSGP 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 subapplicant based on their ideology, beliefs, and/or mission as:
    - an ideology-based/spiritual/religious;
    - educational
    - medical
    - 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 attacks;
- 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.
- Grant projects must be:
    - both feasible and effective at mitigating the identified vulnerability and thus reducing the risks for which the project was designed; and
    - 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.

Security Review

DHS 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. (the State does not complete this portion, this is only for FEMA to complete)

4. Evaluation and Scoring Matrix

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 FEMA Grant Programs Directorate (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.

Final Score Calculation

The initial score assigned during evaluation is weighted using a category multiplier, and bonus points are added for new recipients:

- **Multiplied by 3:** Ideology-based / Spiritual / Religious entities (Houses of Worship, religious schools, medical facilities, etc.).
- **Multiplied by 2:** Secular medical and secular educational institutions.
- **Multiplied by 1:** All other nonprofit organizations.
- **First-Time Recipients:** Sub-applicants who have **never received an NSGP award** will have **15 points added** to their final score.

In the **NSGP Federal Review**, the States' score is multiplied by the applicable multiplier and bonus points are added based on first-time status. 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. This merit-based selection process ensures that funding is directed to the most promising and highest risk subapplications.

Security Review

Following competitive scoring and selection, the names and physical addresses of potential subrecipients are submitted to a security review against U.S. intelligence community reporting to verify that no security risks exist before final funding determinations are made.

5. Funding Restrictions & Allowable Costs

Allowable Costs

Allowable project costs must directly align with facility hardening and physical or cyber security enhancements. They generally fall into the following categories:

- **Planning:** Security or emergency planning expenses, developing/strengthening security plans, evacuation/shelter-in-place plans, emergency contingency plans, and risk/resilience assessments on connected cyber-physical systems.
- **Equipment:** Acquisition and installation of select security items from the Authorized Equipment List (AEL). Key allowable items include:
    - Public address systems (handheld/mobile) and public notification/warning systems.
    - Restricted access, caution, and functional-needs warning signs.
    - Physical Access Control Systems (PACS), credentialing systems, and personnel/vehicle identification systems.
    - Impact-resistant doors and gates; blast/shock/impact-resistant building materials (breakage-resistant glass, window films).
    - Fences, Jersey walls, gates, barriers, bollards, planters, and fixed perimeter/area lighting.
    - Security cameras (CCTV systems utilizing standard, low-light, or infrared technology).
    - Alarm systems, standalone intrusion detection sensors, and acoustic sensor triangulation networks.
    - Cybersecurity software (encryption, malware/anti-virus protection, personal/network firewalls, and host/network-level intrusion detection systems).
    - Generators and Uninterruptible Power Supplies (UPS) to support security infrastructure.
    - Handheld or fixed personnel/package screening equipment (e.g., walk-through magnetometers).

- **Training & Exercises:** Long-term vulnerability reduction via preparedness training (e.g., active shooter training), threat response exercises, and public awareness campaigns.
- **Contracted Security:** Private contracted security guards/personnel.
- **Management & Administration (M&A):** Subrecipients may use and expend **up to 5%** of each subaward for non-operational M&A costs (e.g., travel, accounting, inventory maintenance, and reporting) directly supporting the award.

Unallowable Costs

The following projects, initiatives, and expenditures are strictly ineligible for funding:

- 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.
- Pre-Award Costs: Not allowable for subrecipients.

Prohibition on Covered Equipment or Services: FEMA provides additional resources regarding the prohibition on covered telecommunications equipment and services in its policy titled Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services (FEMA Policy #405-143-1). Any project involving communications or telecommunications equipment or services will be subject to review by the Statewide Interoperability Coordinator (SWIC).

6. Post-Award & Compliance Requirements

Procurement Rules

Subrecipients must follow documented procurement procedures that reflect applicable state, local, tribal, and territorial laws, provided they conform to federal standards (2 C.F.R. §§ 200.318-200.327).

- **Competition:** All procurement transactions must provide full and open competition. Restrictive pricing, arbitrary actions, or unnecessary experience/bonding requirements must be avoided.
- **Conflicts of Interest:** Written standards of conduct must be maintained to prevent real, apparent, or organizational conflicts of interest. Employees or agents involved in selection/administration cannot participate if a conflict exists.
- **Contractor Restrictions:** Contractors that assist in drafting specifications, statements of work, grant applications, budgets, or project plans are prohibited from competing for those procurement contracts.
- **Thresholds:** Effective October 1, 2025, the federal micro-purchase threshold is $15,000 and the simplified acquisition threshold is $350,000.

Environmental Planning and Historic Preservation (EHP)

All projects involving physical modifications, building renovations, or equipment installations (e.g., perimeter fencing, security cameras, or fixtures) must participate in the EHP review process. Federal law requires EHP review to be fully completed and approved before federal funds are released to carry out the project.

Build America, Buy America Act (BABA)

None of the funds provided under this program may be used for an infrastructure project unless the iron, steel, manufactured products, and construction materials used are produced in the United States. This preference applies to materials permanently affixed to the project, but does not apply to tools, temporary equipment, or movable furniture.

Reporting & Record Retention

- **Reporting Changes:** Subrecipients must submit updated information for approval anytime there is a change in key personnel.
- **Audit Requirements:** Any subrecipient expending **$1 million or more** in federal awards during its fiscal year must undergo a single or program-specific audit.
- **Record Retention:** Financial records, solicitations, specifications, competitive quotes, purchase orders, invoices, and cancelled checks must be maintained for **at least three years** from the date the final federal financial report is submitted.
- **Access to Records:** Authorized representatives retain the right of timely and reasonable access to any records or personnel pertinent to the subaward for the purpose of site visits, desk reviews, or interviews.

Noncompliance & Termination

Failure to comply with the terms, conditions, or federal statutes governing this award may result in special conditions being placed on the subaward, a temporary hold on funds, or full/partial termination of the award. Subrecipients may choose to terminate an award by sending a written notification detailing the reasons and effective date. Upon completion of all project activities, closeout materials must be submitted within **90 calendar days** of the subaward period of performance end date.

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).

AEL Code	Title	Description
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.
06CP-01-PORT	Radio, Portable	Individual/portable radio transceivers, for notifications and alerts.
06CP-01-	Repeater	Electronic device that receives a weak or low-

AEL Code	Title	Description
REPT		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.

AEL Code	Title	Description
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.
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

AEL Code	Title	Description
		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.
–Code	**Title**	**Description**
PLANNING	Planning	
EXERCISE	Exercise	

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.

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 refer to 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.

Note: Subapplicants budget narratives should indicate costs that includes shipping and/or tax, as applicable. It is not required to break the costs out as separate from the relevant purchase(s).

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.

APPLICATION SCORING MATRIX

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 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.

Investment Justification Requirement	Criteria	Score	Explanation
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 nonprofit organization or closely related organization?	To substantiate the subapplicant's risk to a terrorist or other 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	0	The subapplicant **does not discuss specific** threats or attacks against the organization or a closely related organization.

Investment Justification Requirement	Criteria	Score	Explanation
	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.		
		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	Subapplicants must provide a clear	0	The subapplicant **did not discuss or describe** the organization's susceptibility to attack.

Investment Justification Requirement	Criteria	Score	Explanation
well did the subapplicant describe the organization's susceptibility to destruction, incapacitation, or exploitation by a terrorist or other extremist attack?	description of findings from a completed vulnerability assessment.	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 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

Investment Justification Requirement	Criteria	Score	Explanation
			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.
		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	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

Investment Justification Requirement	Criteria	Score	Explanation
other extremist attack?			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 vulnerability.
Milestones			
How well did the subapplicant describe the milestones and the associated key activities that lead to	The subapplicant should describe the milestones needed to accomplish the goals of the NSGP funding and should include the	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

Investment Justification Requirement	Criteria	Score	Explanation
the milestone event over the NSGP period of performance?	key activities that will be necessary to accomplish those milestones.		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	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 support implementation.

Investment Justification Requirement	Criteria	Score	Explanation
implementation of the Investment?		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.