NONPROFIT SECURITY GRANT PROGRAM NATIONAL SECURITY SUPPLEMENTAL APPLICATION GUIDE

FLORIDA DIVISION OF EMERGENCY MANAGEMENT
Preparedness Bureau

Coordinate, collaborate and communicate with our community stakeholders for a resilient Florida.

October 2024

Table of Contents

Program Description

The U.S. Department of Homeland Security (DHS) has announced that nonprofit organizations in designated UASI areas nationwide are eligible to apply for funds as part of the Urban Areas Security Initiative (UASI) Nonprofit Security Grant Program-National Security Supplemental (NSGP-NSS).

Subrecipients must follow the programmatic requirements in the NOFO, FEMA Preparedness Grants Manual, and the applicable provisions of the Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards located in Title 2, Code of Federal Regulations (C.F.R.), Part 200.

FEDERAL AWARD INFORMATION

Department of Homeland Security
Nonprofit Security Grant Program
National Security Supplemental
Assistance Listings Number
(formerly CFDA Number):97.008
Grant Period: 5/1/2025-4/30/2028
https://www.fema.gov/nonprofit-security-grant-program

KEY DATES

NSGP-NSS Application Cycle Opened	**October 28, 2024**
NSGP-NSS-UA and NSGP-NSS-State Applications Due and received to Florida State Administrative Agency (SAA)	**November 29, 2024, by 5:00pm ET** ***NO EXCEPTIONS***
Applications must be submitted to: **Sharepoint.admin@em.myflorida.com**	
NSGP-NSS Applications Submission to FEMA	**Friday, January 24, 2025 COB 5:00pm ET**
Award Notification	**May 10, 2025 (Anticipated)**

Program Purpose

The Nonprofit Security Grant Program-National Security Supplemental (NSGP-NSS) provides funding for physical security enhancements and other security-related activities to nonprofit organizations that are at high risk of a terrorist or other extremist attack. The NSGP-NSS also seeks to integrate the preparedness activities of nonprofit organizations with broader state and local preparedness efforts. In FY 2024, multiple funding allocations have been appropriated for nonprofit organizations located inside or outside the UASI-designated urban areas. As in previous fiscal years, the NSGP-NSS-Urban Area (NSGP-NSS-UA) is a competitive grant program that funds nonprofits located in UASI-designated areas. Under the NSGP-NSS-State (NSGP-NSS-S), each state will receive an allocation for nonprofits located outside of the UASI-designated areas.

Goals and Objectives

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.

Funding 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.

NSGP-NSS Funding Priorities

All priorities in this table concern 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 https://www.cisa.gov/cpg
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

Funding for NSGP-NSS is limited and applicants will be prioritized in the following manner:

1. Ideology-based/Spiritual/Religious
2. Educational, including childcare facilities
3. Medical
4. Other

Application review will be in coordination with the Urban Area Security Initiatives (UASI) working groups.

Applicant Eligibility Criteria

Nonprofit organizations eligible as **subapplicants to the SAA** 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): https://www.irs.gov/charities-non-profits/charitable-organizations/exemption-requirements-501c3-organizations
• Publication 557 (01/2022), Tax-Exempt Status for Your Organization | Internal Revenue Service (irs.gov): https://www.irs.gov/publications/p557
• Charities and Nonprofits | Internal Revenue Service (irs.gov): https://www.irs.gov/charities-and-nonprofits

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

3. For NSGP-NSS-UA, located within a UASI-designated high-risk urban area; or for NSGP-NSS-S, located outside of an UASI-designated high-risk urban area. Located within one of the UASI-designated areas (Jacksonville, Tampa, Orlando and Miami/Fort Lauderdale).

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

For the NSGP-NSS, a consortium of eligible nonprofit organizations is also an eligible subapplicant. A consortium application is an opportunity for an eligible nonprofit organization to act as a lead and apply for funding on behalf of itself and any number of other eligible NSGP-NSS eligible nonprofit organizations. The lead nonprofit organization must fill out the Investment Justification to represent the collective of the consortium. Additionally, consortium applicants are required to fill out and submit a Consortium Workbook to their SAA which captures the necessary data for all participating consortium nonprofit organizations. All nonprofit organizations in the consortium application must be compliant with the NSGP-NSS eligibility requirements listed above. Nonprofit organizations may not apply both individually and as part of a consortium. The lead nonprofit organization and its partners must be the intended beneficiaries of the requested funding. The lead nonprofit organization shall not distribute grant-funded assets or provide grant-funded contractual services to non-compliant partner nonprofit organizations or other ineligible organizations.

Note: If successful, the lead consortium member will accept the subaward on behalf of the consortium, implement the approved projects/contracts for all consortium member sites, and manage the subaward throughout the period of performance, to include ensuring that all terms and conditions of the subaward are met.

*An application submitted by an otherwise eligible non-federal entity (i.e., the applicant) may be deemed ineligible when the person that submitted the application is not: 1) a ***current employee, personnel, official, staff or leadership*** of the non-federal entity; and 2) ***duly authorized to apply*** for an award on behalf of the non- federal entity at the time of application. Further, the Authorized Organization Representative (AOR) must be a duly authorized current employee, personnel, official, staff or leadership of the recipient and ***provide an email address unique to the recipient (SAA) at the time of application and upon any change in assignment during the period of performance***. ***Consultants or contractors of the recipient are not permitted to be the AOR of the recipient.***

Funding Maximum Amounts

NSGP-NSS-UA: The maximum award amount each NSGP-NSS-UA nonprofit organization can apply for funding is up to **$200,000.00** Applicants with one site may apply for up to **$200,000.00** for that site. Applicants with multiple sites may apply for up to **$200,000.00** per site, for up to three sites, for a maximum of **$600,000.00** per sub-applicant. Applicants that apply for projects at multiple sites, regardless of whether the projects are similar in nature, it must include an assessment of the vulnerability and risk unique to each site. That is, one vulnerability assessment per location/physical address. **Failure to do so may be cause for rejection of the application.**

NSGP-NSS-STATE: The maximum award amount each NSGP-S nonprofit organization can apply for funding is up to **$2000,000.00**. Applicants with one site may apply for up to **$200,000.00** for that site; Applicants with multiple sites may apply for up to **$200,000.00** per site, for up to three sites, for a maximum of **$600,000.00** per sub-applicant. Applicants that apply for projects at multiple sites, regardless of whether the projects are similar in nature, it must include an assessment of the vulnerability and risk unique to each site. **Failure to do so may be cause for rejection of the application.**

Consortium applications are also eligible under the NSGP-NSS. In this case, an eligible entity would apply on behalf of themselves and other eligible entities as a subapplicant to the SAA. Consortia may apply through the SAA for an award totaling $1 million. Awards over $250,000 must comply with the Build America, Buy America Act (BABAA). The $200,000 per site maximum still applies for each individual nonprofit organization within the consortium. ***If successful, the lead consortium member will accept the subaward on behalf of the consortium, implement the approved projects/contracts for all consortium member sites, and manage the subaward throughout the period of performance, to include ensuring that all terms and conditions of the subaward are met.***

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.

Nonprofit Security Allowable Activities

Allowable NSGP-NSS costs are focused on security related activities. Funding can be used for security related planning; training; exercise; contracted security personnel and the acquisition and installation of security equipment on real property owned or leased by the non-profit at the time of the application.

Planning

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 considerations 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 and related CISA resources.

Examples of allowable planning activities include, but are not limited to:

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

Training and Exercise

Training conducted using NSGP-NSS funds must address a specific threat and/or vulnerability, as identified in the nonprofit organization’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-NSS must be included in the nonprofit organization’s Investment Justification (IJ).

Training costs are limited to an organization’s security personnel staff, members, and volunteers only.

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

Allowable training topics are limited to the protection of critical infrastructure key resources, including physical and cybersecurity, target hardening, and terrorism awareness/employee preparedness such as Community Emergency Response Team (CERT) training, indicators and behaviors indicative of terrorist 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. 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.

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 Resource–s – Preparedness Toolkit (fema.gov). Recipients are encouraged to enter their exercise data and AAR/IP in the Preparedness Toolkit.

Contracted Security Personnel

Contracted security personnel are allowed under this program only as described in the NOFO and Manual and comply with guidance set forth in IB 421b and IB 441. NSGP-NSS funds may not be used to purchase equipment for contracted security. **The Investment Justification must include specific details about any proposed contract security personnel costs, to include the proposed contracted security costs described in the Investment Justification should include the hourly/daily rate, the number of personnel and anticipated number of hours/days the personnel will work over the course of the period of performance.**

- NSGP-NSS funds **may not** be used to purchase equipment for contracted security personnel.
- Contract security personnel activities **must** be competitively procured. Procurement via sole source for contract security personnel is not allowable.
- Applicants are no longer required to provide written justification for Contract security personnel costs (Price Act Waiver requirement) that **exceeds** fifty percent (50%) of the Federal request amount.

Equipment

Equipment costs are allowed under this program only as described in the NOFO and the accompanying appendix in the Preparedness Grants Manual. Allowable costs are focused on facility hardening and physical security enhancements. Applicants should analyze the costs and benefits of purchasing versus easing equipment, especially high costs items and those subject to rapid technical advances. Large equipment purchases must be identified and explained. **Proposed equipment costs associated using the NSGP can only be from the allowable categories provided must be included in the nonprofit organization's Investment Justification.**

Allowable equipment under the NSGP is **limited to select items** on the Department of Homeland Security Authorized Equipment List. These items are as follows:

•03OE-03-MEGA	System, Public Address, Handheld or Mobile
•03OE-03-SIGN	Signs
•04AP-05-CRED	System, Credentialing
•04AP-09-ALRT	Systems, Public Notification and Warning
•04AP-11-SAAS	Applications, Software as a Service
•05AU-00-TOKN	System, Remote Authentication
•05EN-00-ECRP	Software, Encryption
•05HS-00-MALW	Software, Malware/Anti-Virus Protection
•05HS-00-PFWL	System, Personal Firewall
•05NP-00-FWAL	Firewall, Network
•05NP-00-IDPS	System, Intrusion Detection/Prevention
•06CP-01-PORT	Radio, Portable
•06CP-01-REPT	Repeater
•06CC-02-PAGE	Services/Systems, Paging
•06CP-03-ICOM	Intercom
•06CP-03-PRAC	Accessories, Portable Radio
•10GE-00-GENR	Generators
•10PE-00-UPS	Supply, Uninterruptible Power (UPS)
•13IT-00-ALRT	System, Alert/Notification
•14CI-00-COOP	System, Information Technology Contingency Operations
•14EX-00-BCAN	Receptacles, Trash, Blast-Resistant
•14EX-00-BSIR	Systems, Building, Blast/Shock/Impact Resistant
•14SW-01-ALRM	Systems/Sensors, Alarm
•14SW-01-ASTN	Network, Acoustic Sensor Triangulation
•14SW-01-DOOR	Doors and Gates, Impact Resistant
•14SW-01-LITE	Lighting, Area, Fixed
•14SW-01-PACS	System, Physical Access Control
•14SW-01-SIDP	Systems, Personnel Identification
•14SW-01-SIDV	Systems, Vehicle Identification
•14SW-01-SNSR	Sensors/Alarms, System and Infrastructure Monitoring, Standalone
•14SW-01-VIDA	Systems, Video Assessment, Security
•14SW-01-WALL	Barriers: Fences; Jersey Walls
•15SC-00-PPSS	Systems, Personnel/Package Screening
•21GN-00-INST	Installation
•21GN-00-TRNG	Training and Awareness

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

Telecommunications Equipment/Services

Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services Recipients and subrecipients of FEMA federal financial assistance are subject to the prohibitions described in section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (FY 2019 NDAA), Pub. L. No. 115-232 (2018) and 2 C.F.R. §§ 200.216, 200.327 200.471, and Appendix II to 2 C.F.R. Part 200.

Beginning August 13, 2020, the statute – as it applies to FEMA recipients, subrecipients, and their contractors and subcontractors – prohibits obligating or expending federal award funds on certain telecommunications and video surveillance products and contracting with certain entities for national security reasons.

Effective August 13, 2020, FEMA recipients and subrecipients **may not** use any FEMA funds under open or new awards to:

(1) Procure or obtain any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology of any system;
(2) Enter into, extend, or renew a contract to procure or obtain any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology of any system; or
(3) Enter into, extend, or renew contracts with entities that use covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system.

Replacement Equipment and Services: FEMA grant funding may be permitted to procure replacement equipment and services impacted by this prohibition, provided the costs are otherwise consistent with the requirements in this manual and the applicable NOFO.

For additional guidance, please refer to Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services (Interim) in the Preparedness Grants Manual.

Management and Administration (M&A)

Nonprofit organizations that receive a subaward under this program may expend up to five percent (5%) of their NSGP-NSS funds for M&A purposes associated with the subaward. M&A activities are costs defined as directly relating to the M&A of the grant, such as financial management and monitoring, etc. 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. **Proposed M&A costs associated using the NSGP-NSS must be included in the nonprofit organization's Investment Justification.**

This is a COST REIMBURSEMENT grant program, therefore, if your organization is selected to receive funding, the organization is responsible for ordering and purchasing eligible equipment. Those eligible reimbursement expenses should be submitted to the SAA with copies of purchase orders, invoices, and copies of the front and back of the cancelled checks, or other proof of payment deemed acceptable by the SAA.

Unallowable Nonprofit Security Grant Program Activities:

This list is not exhaustive, therefore, if there are any questions regarding allowable costs, please contact the SAA. For additional information on allowable costs, see the Preparedness Grants Manual.

- 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;
- Cameras for license plate readers/license plate reader software;
- Cameras for facial recognition software;
- Weapons or weapons-related training; and
- Knox boxes.

What type entities are not eligible to apply under NSGP-NSS?

- Utility Companies
- For-profit transportation entities, such as a company offering bus service
- For-profit hospitals
- Organizations active in politics, lobbying, advocacy work
  - Volunteer Fire Departments
  - Community Service Organizations (Kiwanis, Rotary and Lions Clubs)
  - Homeowner Associations, Labor Unions, etc.
- Agriculture or horticultural organizations
  - County fairs and flower societies are examples of these types of groups.
- For-profit colleges/ universities
- Government Entities
- For profit public venues

    - Stadiums, Amusement Parks, Clubs, etc.
- Municipal/Public Schools
    - Elementary, middle, or high schools

This is not an exhaustive list. If there are any questions about an organizations' eligibility to apply For NSGP-NSS, please contact the SAA. For further guidelines on unallowable NSGP-NSS costs, please refer to page 40 of the NOFO.

How do I Prepare?

Ensure applicant has active Unique Entity Identifier:

On April 4, 2022, the Data Universal Numbering System (DUNS) Number was replaced by a new, non-proprietary identifier requested in, and assigned by, the System for Award Management (SAM.gov). This new identifier is the Unique Entity Identifier (UEI). All entities wishing to do business with the federal government must have a unique entity identifier (UEI). The UEI number is issued by the SAM system. Requesting a UEI using SAM.gov is straightforward*:*

- Refer to https://sam.gov/content/entity-registration if you want to get a Unique Entity ID (SAM) for your organization. Please note, applicants are NOT required to go through the full SAM registration process in order to obtain a UEI.
- If your entity is registered in SAM.gov today, your Unique Entity ID (SAM) has already been assigned and is viewable in SAM.gov. This includes inactive registrations. The Unique Entity ID is currently located below the DUNS Number on your entity registration record. Remember, you must be signed in to your SAM.gov account to view entity records.

Documentation of your organization's active Unique Entity Identifier must be submitted as a part of the application.

Explain how proposed project supports terrorism preparedness:

The NSGP-NSS funding supports investments that improve the ability of jurisdictions nationwide to:

- Prevent a threatened or an actual act of terrorism;
- Prepare for all hazards and threats, while explaining the nexus to terrorism preparedness;
- Protect citizens, residents, visitors, and assets against the greatest threats and hazards relating to acts of terrorism; and/or
- Respond quickly to save lives, protect property and the environment, and meet basic human needs in the aftermath of an act of terrorism or other catastrophic incidents.

Be prepared to submit a complete application with the required documentation:

As part of the NSGP-NSS application, each eligible nonprofit applicant must submit a complete application which includes the required documentation listed below and must be **RECEIVED** by the SAA by **Friday, November 29, 2024, by 5:00pm (ET)**. An application submission will be deemed incomplete if either requirement has not been submitted.

- Completed Investment Justification (PDF template attached). All IJs must be submitted the PDF fillable format – ***IJs cannot be scanned and must be submitted separately from other supporting documents.***
- Vulnerability/Risk Assessment Unique to the Site (**that includes the Physical address and Location**)
- Mission Statement (**on Organization's Letterhead**)
- Documentation from the IRS demonstrating a 501(c)(3) is required for organizations that are not Ideology-based/Spiritual/Religious
- Signature Page signed by the Authorized Official Representative of the nonprofit Organization.
- Organizational Chart
- If applicable, any supporting documentation that supports threats to the facility such as police reports/Insurance Reports

NSGP-NSS Investment Justification (IJ):

Nonprofit organizations with one site may apply for up to $200,000 for that site. Nonprofit organizations (not applying as part of a consortium) 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. If a nonprofit subapplicant applies for multiple sites, it must submit one complete IJ per each site. IJs cannot include more than one physical site.

Applicants must use the attached PDF Fillable Investment Justification template provided by DHS/FEMA. Each applicant must develop a formal Investment Justification that addresses each investment proposed for funding. The investments or projects described in the Investment Justification must:

- If applying for multiple sites, applicant must submit **one complete Investment Justification per each site**.
- Be for the location(s)/physical address (es) (NOT P.O. Boxes) that the nonprofit currently occupies at the time of application.
- Address an identified risk, including threat and vulnerability, regardless of whether submitting for similar projects at multiple sites.
- Demonstrate the ability to provide enhancement consistent with the purpose of the program and guidance provided by DHS/FEMA.
- Be both feasible and effective at reducing the risks for which project was designed.
- Be able to be fully complete projects within the three-year period of performance; and

- Be consistent with all applicable requirements outlined in the NOFO and the Preparedness Grants Manual.

The Target Hardening narrative total, AEL list total, federal funding request amount, and NSGP-NSS Total Project Cost must all match.

Vulnerability/Risk Assessment

Each applicant must provide a vulnerability/risk assessment that includes the **physical address and name of the organization.** The assessment must be **unique to the site** the Investment Justification is being submitted for It is recommended that applicants work with local police departments to complete a vulnerability assessment and/or notify police of identified vulnerabilities.

Important Notice: If your Vulnerability/Risk assessment does not include the location/physical address unique to the site, the application will not be reviewed and scored.

- Cybersecurity & Infrastructure Security Agency (CISA) has developed a baseline security self-assessment that is designed for a person with little to no experience to complete the security assessment. This assessment is geared towards Houses of Worship but can be used for any NSGP applicant. Resources to complete a self-assessment can be found Houses of Worship | CISA

Note: It is very important that the projects listed in the application link to or addresses vulnerabilities identified in vulnerability/risk assessments. Example: If requesting door locks, the vulnerability assessment should explain what weaknesses exist in access control throughout the building.

NSGP-NSS Consortium -Specific Investment Justification (IJ) Requirements:

The lead nonprofit organization within the consortium must submit the same documents as part of the consortium application; however, the responses must represent the collective of the consortium. Additional guidance for consortium applications is provided below.

Each nonprofit organization with one site in the consortium may apply for up to $200,000 for that site. Consortium applications are limited to a maximum of $1,000,000 per consortium.

Applicants must use the attached PDF Fillable Investment Justification template provided by DHS/FEMA. Each applicant must develop a formal Investment Justification that addresses each investment proposed for funding. The investments or projects described in the Investment Justification must:

- If applying for multiple sites, applicant must submit **one complete Investment Justification per consortium**.

- Address an identified risk, including threat and vulnerability, regardless of whether submitting for similar projects at multiple sites.
- Demonstrate the ability to provide enhancement consistent with the purpose of the program and guidance provided by DHS/FEMA.
- Be both feasible and effective at reducing the risks for which project was designed.
- Be able to be fully complete projects within the three-year period of performance; and
- Be consistent with all applicable requirements outlined in the NOFO and the Preparedness Grants Manual.

In Part I of the IJ, Nonprofit Organization Subapplicant Information, the lead nonprofit organization of the consortium must fill out the required fields based **solely on the lead** nonprofit organization's information.

In Part II of the IJ, Background Information, the lead nonprofit organization of the consortium must summarize the shared background information of **all nonprofit organizations within the consortium**.

In Part III of the IJ, Risk, the lead nonprofit organization of the consortium must summarize the threats, vulnerabilities, and potential consequences facing **all nonprofit organizations within the consortium**. Additional space for further detail is available in the Consortium Workbook.

In Part IV of the IJ, Facility Hardening, the lead nonprofit organization of the consortium must summarize how the proposed activities or investments of the consortium address the shared vulnerabilities identified in Part III. For Section IV-B, the lead organization must input the total funding requested for **all nonprofit organizations within the consortium** under each AEL investment.

In Part V of the IJ, Milestone, the lead nonprofit organization of the consortium must provide the key milestones from **all nonprofit organizations within the consortium**'s proposed activities.
In Part VI of the IJ, Project Management, an individual must be identified from **solely the lead** nonprofit organization that will oversee the projects carried out by the nonprofit organizations in the consortium and assess their plan.

In Part VII of the IJ, Impact, the lead nonprofit organization of the consortium must describe the key measurable outputs and outcomes for **all nonprofit organizations within the consortium**'s investments.
In Funding History and the Nonprofit Subapplicant Contact Information sections, the lead nonprofit organization of the consortium must fill out the required fields based **solely on the lead** nonprofit organization's information.

NSGP-NSS CONSORTIUM WORKBOOK

Full Consortium Workbook instructions can be found in the instructions tab of the Consortium Workbook. The Consortium Workbook must expand upon the information provided in the consortium lead nonprofit organization's IJ.

The Consortium Workbook must contain the number of nonprofit organizations within the consortium and the following information for each nonprofit organization within the consortium:

i. **Demographic information**, including the name, address, nonprofit organization type, organization function, and organization affiliation;

ii. **Required programmatic information**, including eligibility information, UEI number (lead consortium member only), past funding history, total funding requested per site, and a point of contact for each nonprofit organization; and

iii. **Additional narrative information**, including how each nonprofit organization's projects address the objective of the consortium

Vulnerability/Risk Assessment

Consortia have the option to either submit either **individual** vulnerability/risk assessments for **each** nonprofit in the consortium or a **shared** vulnerability/risk assessment that reflects the **collective** risks faced by all consortium members as summarized in the IJ.

- Cybersecurity & Infrastructure Security Agency (CISA) has developed a baseline security self-assessment that is designed for a person with little to no experience to complete the security assessment. This assessment is geared towards Houses of Worship but can be used for any NSGP applicant. Resources to complete a self-assessment can be found Houses of Worship | CISA

Mission Statement

Each applicant must include its Mission Statement and any implementation policies or practices that may elevate the organization's risk. The SAA will use the Mission Statement along with the applicant's self-identification in the Investment Justification to validate that the organization is one of the following types below. **Please note: The Mission Statement must be submitted on the organization's letterhead**.

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

Ideology-based/Spiritual/Religious;	Educational
Medical	Other

501(c)(3) Exemption Document

For organizations that the IRS requires to apply for and receive a recognition of exemption under section 501(c)(3), documentation of the organization's exemption status must be submitted in the application.

Applicant Signature Page

The attached application Signature Page ***must*** be signed by the Applicant's Authorized Representative. An application submitted by an otherwise eligible non-federal entity (i.e., the applicant) may be deemed ineligible when the person that submitted the application is not: 1) a ***current employee, personnel, official, staff or leadership*** of the non-federal entity; and 2) ***duly authorized to apply*** for an award on behalf of the non-federal entity at the time of application. Further, the Authorized Organization Representative (AOR) must be a duly authorized current employee, personnel, official, staff or leadership of the recipient and ***provide an email address unique to the recipient at the time of application and upon any change in assignment during the period of performance***. ***Consultants or contractors of the recipient are not permitted to be the AOR of the recipient.***

Organizational Chart

An organizational is a graphic representation of the structure of an organization showing the relationships of the positions or jobs within it.

WHEN ARE APPLICATIONS DUE?

All applications and supporting documentation must be **RECEIVED** by the SAA by Friday**, November 29, 2024 by 5:00pm (ET).** Applications received after this date and time will not be eligible for consideration.

To facilitate processing, completed grant applications and supporting documentation must be sent via email to **Sharepoint.admin@em.myflorida.com**. Your application and supporting documentation must be received no later than the due date and time listed above.

FAILURE TO PROVIDE EITHER OF THE AFOREMENTIONED REQUIRED DOCUMENTS WILL BE DEEMED AN INCOMPLETE APPLICATION SUBMISSION

WHAT DO I NEED TO APPLY?

To be eligible:

- □ Applicant(s) must be:
  - An eligible nonprofit entity.
  - Able to demonstrate, through the application, that the organization is at high risk of a terrorist or other extremist attack.
  - Be located within one of the UASI-designated areas (Jacksonville, Tampa, Orlando, and Miami/Fort Lauderdale) to apply for NSGP-NSS-UA funding.
  - Located outside UASI designated areas, applicants are only eligible to apply for NSGP-NSS-S funding.
- □ Applicant must not be listed on the suspended and debarred vendor list.
- □ Applicant must have a valid Unique Entity ID
- □ Applicants must read and comply with 2 CFR 200.317 to 2 CFR 200.327 regulations.
- □ Applicant must have written procurement standards per 2 CFR 200.318(a).
- □ Applicant must have written conflict of interest standards per 2 CFR 200.318(c).

- ☐ Applicant must read 2 CFR § 200.216 and 2 CFR § 200.471 and understands that certain telecommunications and video surveillance services or equipment are prohibited from being purchased using grant funds.
- ☐ Applicant must take necessary steps to assure that minority businesses, women's business enterprises, and labor surplus area firms are used when possible per 2 CFR 200.321.
- ☐ Applicant agrees that this federal funding does not supplant (replace) state, local, and agency monies in their organization's budget for the requested items in this application.

Please refer to the Notice of Funding Opportunity Nonprofit Security Grant Program National Security Supplemental for additional information regarding eligibility and application review.

HOW TO APPLY

Nonprofit applications and required documents **MUST** be submitted and received by the State Administrative Agency by **TBA 5:00PM (EST)** ***NO EXCEPTIONS*.** All applications **MUST** be submitted via SharePoint Portal. Applications and/or documents received after this date and time will not be eligible for consideration.

To apply for the NSGP-NSS grant:

Please follow the instructions below:

1. To gain access to SharePoint, applicants **MUST** send an email with information below to: **sharepoint.admin@em.myflorida.com**. **Do not include attachments in this email**. This information must match the information entered into the "NONPROFIT SUBAPPLICANT CONTACT INFORMATION" section of the Investment Justification form:

    - Nonprofit Organization Name
    - Nonprofit Sub-applicant Contact Name
    - Nonprofit Sub-applicant Contact Phone Number
    - Nonprofit Sub-applicant Physical Address/Location
    - Nonprofit Sub-applicant Contact Email Address

Please note: Our offices are closed on the weekends, and during state observed holidays. *If an applicant email request is received during a time of Holiday Office Closure, an automatic out of office reply will be sent indicating the office closure details, stating that your email was received, and stating a response will be sent the next business day.*

2. The Sub-applicant contact listed above will receive an email from our SharePoint Administrator with instructions on how to sign in to SharePoint and fill out the upload form.
3. After gaining access to SharePoint and the data entry form, the point of contact will need to select who the application was written by, their designated urban area (NSGP-UA or NSGP-State) for which they are applying, and upload required documents.
4. Once you are satisfied that everything has been submitted in full, and within the proper guidelines, you must select the indicator for Final Submission.

5.

Document Submission on SharePoint Form:

- Documents **MUST** be named appropriately and uploaded as individual documents. They **must not** be merged into a single document.
- The Investment Justification must be submitted in the PDF fillable format and cannot be scanned. If the Investment Justification is scanned it will not be deemed eligible for submission and review.
- Supporting documents must be uploaded as separate documents from the Investment Justification (i.e. Vulnerability Assessment, Mission Statement, etc.). For a complete list of required documents, please refer to the attached SAA's Application Guide (page 17).

Naming Conventions:

The following naming conventions must be utilized for UA or State application submissions:

- NSGP-NSS_UA_<State Abbreviation>_<Urban Area>_<Nonprofit Name>"

Example: NSGP-NSS_UA_FL_MiamiFortLauderdale_Nonprofit Name

- NSGP-NSS_S_<State Abbreviation>_<Nonprofit Name>"

Example: NSGP-NSS_S_FL_Nonprofit Name

***The Investment Justification must be submitted in the PDF fillable format and cannot be scanned. If the Investment Justification is scanned it will not be deemed eligible for submission and review. ***

<u>NSGP -NSS– UA and State Application Review Process</u>

NSGP-NSS applications are to be submitted by nonprofit organizations to their respective SAA. Applications will be reviewed through a two-phase state and federal review process for completeness, adherence to programmatic guidelines, feasibility, and how well the Investment Justification (project description and justification) addresses the identified risk(s). The SAA will make recommendations to DHS/FEMA based on their target allocation and according to the chart listed in the NSGP-NSS-S process subsection.

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 nonprofit organizations that have not received prior year funding, then those prioritized highest by their SAA. DHS/FEMA will use the 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.

□ IJ scores should not be skewed toward giving applicants in a state an advantage during the Federal review process.

  ○ Scores should not be distributed on a bell curve, with a handful of high scoring applicants, a handful of low applicants, and most scores falling within the middle.

- Scoring of the IJ by the SAA and Urban Area Working Group should reflect any concerns with the application.

    - If an application does not directly answer a question, the scoring should reflect a reduced score.
    - Any applicant that fails to clearly link requested funding in Section IV-Target Hardening to it vulnerability Assessment should receive a reduced score.
    - Any section that has a narrative field blank should receive a reduced score.
    - Applicants that fail to identify one or more specific core capabilities in IJ Section VII-
    - Outcomes, should receive a reduced score.
- Applicants should not be scored and recommended for funding for the following reasons:
    - Failure to provide a vulnerability assessment.
    - Failure to provide a mission statement.
    - Not a 501© (3) designated organization.
    - Submission of application past the SAA established deadline.

- Applications can be scored, but should not be recommended for funding for the following reasons:
    - Multiple unallowable projects listed on the IJ.
    - Past performance issues.
- Ensure nonprofit applicants are aware they must comply with all award terms and conditions.
    - Award term & conditions pass down from the non-Federal Entity (i.e., the SAA) to subrecipients (nonprofits), per 2 C.F.R. 200.332.
    - Although award terms and condition are not finalized until an award is made to the SAA, they vary little from year to year.

    ***Refer nonprofit organization to the NSGP-NSS award terms and conditions.**
- All applicants that require a post-award scope and budget change requires approval and may be denied by FEMA without compelling justification given the competitive nature of the grant program.
    - Any proposed changes must be supported by the vulnerability assessment.
    - Nonprofits selected for award that subsequently renovate their facilities to affect the vulnerability Assessment upon which the application as based will not be approved for a scope change.
- If an organization was previously awarded the NSGP grant, they are eligible to apply for an NSGP-NSS grant in FY 2024.
- Given the competitive nature of the grant program, no post award-scope changes are allowed due to a change in the facility location.
- A nonprofit may not move any federally installed equipment to a location.
- The attached application Signature Page must be signed by the Applicant's Authorized Representative. An application submitted by an otherwise eligible non-federal entity (i.e., the applicant) may be deemed ineligible when the person that submitted the application is not: 1) a current employee, personnel, official, staff or leadership of the non-federal entity; and 2) duly authorized to apply for an award on behalf of the non-federal entity at the time of application.

Further, the Authorized Organization Representative (AOR) must be a duly authorized current employee, personnel, official, staff or leadership of the recipient and provide an email address unique to the recipient at the time of application and upon any change in assignment during the period of performance. **Consultants or contractors of the recipient are not permitted to be the AOR of the recipient.**

The SAA will base the ranking on the SAA's subject-matter expertise and discretion with consideration of the following factors:

- **Need**: The relative need for the nonprofit organization compared to the other applicants; and

Impact: The feasibility of the proposed project and how effectively the proposed project addresses the identified need.

Please refer to the Notice of Funding Opportunity Nonprofit Security Grant Program National Security Supplemental for additional information regarding the application review process.

Questions Regarding the Application

For additional information or questions, you may contact:

Ms. Felicia P. Pinnock, Program Manager
850-815-4343/Cell Number: 850-879-0176
Email: Felicia.Pinnock@em.myflorida.com

Ms. Kizzy K. Caban, Lead Program Reviewer
Office Number: 850-815-4348
Email: Kizzy.Caban@em.myflorida.com

Ms. Stephanie Weems, Program Reviewer
Office Number: 850-815-4508
Email: Stephanie.Weems@em.myflorida.com

Ms. Shempekka Mosely, Program Reviewer
Office Number: 850-815-4305
Email: Shempekka.Mosely@em.myflorida.com

Mr. Jerrod Peoples, Program Reviewer
Office Number: 448-220-47113
Email: Jerrod.Peoples@em.myflorida.com

Resources and Attachments

Please see the attached Notice of Funding Opportunity Nonprofit Security Grant Program National Security Supplemental, Investment Justification Template and Consortium Workbook.

DIVISION OF EMERGENCY MANAGEMENT

FDEM

OFFICE OF THE GOVERNOR