Fiscal Year 2025 Nonprofit Security Grant Program (NSGP) Subapplicant Quick Start Guide

Release Date: Jul 28, 2025

The U.S. Department of Homeland Security (DHS) is firmly committed to ensuring that its funding opportunities and application processes are clear and transparent, and that they do not create confusion or contain undue complexity.

Nonprofit organizations should consider using this document as a reference when preparing applications for the Nonprofit Security Grant Program (NSGP).

What is the NSGP?

The NSGP is a competitive grant program appropriated annually through DHS and administered by the Federal Emergency Management Agency (FEMA). It is intended to help nonprofit organizations increase their physical security posture against acts of terrorism or other extremist attacks. Eligible organizations are registered 501(c)(3) nonprofits or otherwise are organizations as described under 501(c)(3) of the Internal Revenue Code (IRC) and tax-exempt under section 501(a) of the IRC. This includes entities designated as “private” (e.g., private institutions of higher learning), as private colleges and universities can also be designated as 501(c)(3) entities. More information on tax-exempt organizations can be found at: https://www.irs.gov/charities-non-profits/charitable-organizations.

> **Note:** Publications and new program guidance are released periodically based on the current fiscal year. Please ensure that you have consulted the most current NSGP Notice of Funding Opportunity (NOFO) and Preparedness Grants Manual (PGM) thoroughly. Successful NSGP subrecipients must comply with all applicable requirements outlined in the NOFO and PGM. Any publications from prior fiscal years, or

published before the NOFO, should be used as historical references only since program priorities and requirements can change every year.

How to Apply

Interested nonprofit organizations (subapplicants) must apply to the NSGP through their State Administrative Agency (SAA) (the applicant). Each SAA has an established application submission process with a state-specific deadline to submit all required materials. ***The application submission deadline in FEMA's NSGP NOFO applies to the SAA only—NOT nonprofit organizations.*** You will need to contact your SAA point of contact for state-specific deadlines and supplemental application materials or requirements unique to your state or territory. The list of SAAs can be found at: https://www.fema.gov/grants/preparedness/state-administrative-agency-contacts. FEMA program support can be contacted by emailing fema-nsgp@fema.dhs.gov.

Nonprofit organizations must fully answer each question in all sections of the Investment Justification(s) (IJ). In their IJ, nonprofit organizations should summarize the most critically important and impactful information. Each Investment Justification can request up to $200,000 per location/physical site/address. A nonprofit organization may submit application packages for up to three sites per NSGP-Urban Area (UA) and NSGP-State (S) funding stream, for a maximum of $600,000 per subapplicant organization per state or territory. The amount of funding requested (maximum of $600,000) and number of submissions per nonprofit organization (maximum of six applications, three under NSGP-S and three under NSGP-UA) may **not** exceed these limits per state or territory. In states with no Urban Area, no more than three applications per nonprofit organization are allowable.

Nonprofit organizations must have a Unique Entity Identifier (UEI), which is obtained through SAM.gov. Nonprofit organizations are not required to have a UEI issued **at the time of application** but **MUST** have a valid UEI to receive a subaward from the SAA. Nonprofit organizations must register in SAM.gov to obtain the UEI **but are not required to maintain an active registration in SAM.gov.** Guidance on obtaining a UEI in SAM.gov can be found at GSA UEI Update and the Federal Service Desk Knowledge Base. It may take four weeks to obtain a UEI, and applicants should plan accordingly. **Obtaining a UEI does not**

cost anything; it is free of charge.

> **Tip**: NSGP has two funding streams: NSGP-State (NSGP-S) and NSGP-Urban Area (NSGP-UA). Applicants must identify and apply for the correct funding stream, which is based on the physical geographical location/address of the facility and whether it is within a high-risk urban area. A full list of eligible high-risk urban areas is in the NSGP NOFO. The list of urban areas can change annually, and the final list of eligible urban areas is included in the NOFO for the corresponding fiscal year. Contact your SAA for questions about the appropriate funding stream based on your organization's location. Note that traditional city limits do not always equate to the designated Urban Area's footprint. Applications submitted to the incorrect funding stream will not be considered.

Application Elements

The following materials, including any additional required or requested materials specific to the SAA, must be submitted to the SAA as part of a complete application package. A submission that is missing any required document(s) will be considered incomplete and will not be reviewed.

Mission Statement

A mission statement is a formal summary of the aims and values of an organization. The three components of a mission statement include the purpose, values, and goals of the organization. The provided statement should discuss the "who, what, and why" of your organization.

> **Tip**: It is highly recommended that the mission statement is documented on official letterhead. This element helps inform and validate a nonprofit organization's categorical self-identification based on its ideology, beliefs, mission, function, or constituency

served/supported.

Vulnerability Assessment

A vulnerability assessment is used to identify and validate physical security deficiencies of your organization/facility and is the foundation of an NSGP application. Vulnerability assessments can be provided in the form of a Cybersecurity and Infrastructure Security Agency (CISA) Self-Assessment (Facility Security Self-Assessment | CISA), a state or local law enforcement assessment, an outside contractor's assessment, or other valid method of assessment. The SAA may require a specific format/type of vulnerability assessment, so be sure to review the state-specific guidelines for their application requirements. CISA's Protective Security Advisors can assist in providing a vulnerability assessment as needed. For more information, review the CISA Central webpage.

The Vulnerability Assessment is different from a risk/threat assessment. A risk assessment involves looking *outside* of an organization to determine external threats that exist that could potentially lead to security issues, whereas a vulnerability assessment involves looking *inside* the organization for internal vulnerabilities and weaknesses. Projects/activities requested through the NSGP should align to mitigate items identified in the Vulnerability Assessment.

Vulnerability assessments are typically valid for as long as the items included in the assessment remain unaddressed/vulnerable. FEMA recommends updating these assessments any time there is a significant renovation, change, or resolution to a vulnerability, *OR* every five years. FEMA does not currently impose specific requirements on vulnerability assessments. Be sure to verify with your SAA if there are any vulnerability assessment requirements.

> **Tip**: In preparation to describe how they intend to use NSGP grant funding, nonprofit organizations should think broadly and holistically in their approach to security measures designed to protect buildings and safeguard people. Some physical security control examples include locks, gates, and guards (e.g., contract security). Although these may be effective measures, there are many additional layers to physical

security that can help protect the organization, including creating comprehensive physical security plans, conducting training and exercises (e.g., active shooter, evacuation), identifying countermeasures against intrusion (e.g., access controls), preventing physical security breaches (e.g., security enhanced doors/windows), and monitoring for physical security threats (e.g., cameras, surveillance). Descriptions of allowable costs and activities can be located in the NOFO and the PGM. Unallowable costs will not be reimbursed.

Investment Justification (IJ)

The IJ is a fillable template, available through Grants.gov, that asks nonprofit organizations to describe the organization, risks/threats to the organization, and proposed projects/activities to mitigate security deficiencies (as identified in the Vulnerability Assessment) utilizing NSGP funding. The IJ is published with the NOFO and is not available before the publication of the program materials. The IJ is subject to change each fiscal year, and prior years' templates will not be accepted. Only use the form for the current fiscal year, as released on Grants.gov.

Supplemental Documents

Each state or territory is unique in how they manage and administer the NSGP. The SAA may require additional documents or specific application materials as part of the state or territory's internal NSGP application submission requirement. However, when preparing the IJ, nonprofit organizations must answer questions completely and cannot refer out to any supplemental documents as they are not submitted to nor reviewed by FEMA. The SAA only submits the IJ to FEMA.

Tip: Contact your SAA for state-specific submission requirements.

Scoring and Funding Recommendations

Upon submission of your completed application, the SAA will review, score, and rank every complete application it has received from eligible nonprofit organizations based on the criteria outlined in the NSGP NOFO. The results of the SAA scoring process will be forwarded to FEMA. FEMA's federal review focuses on checks to ensure SAAs have followed the applicable guidance in their prioritization of projects, validating recipient eligibility (e.g., that a recipient meets all the criteria for the program), validating allowability of the proposed project(s), and checking for any derogatory information on the organization applying. Following the federal review and SAA scoring, nonprofit organizations are recommended for funding. The final list of recommended nonprofit organizations to be funded is provided to the DHS Secretary for final approval.

Because of the timing of the FY 2025 NSGP, the NSGP-S and NSGP-UA funding will be issued as risk-based allocations to each state and territory. Subawards will still be governed by the standard competitive process. However, this will occur after award of the state- and territory-based allocations to ensure that all funds can be obligated prior to the end of the fiscal year. More information will be released later on the FY 2025 subapplication process.

Additional Points

Additional "bonus" points are added to the final scores of subapplicants based on their funding history. For subapplicants that have not received funding in the past, 15 additional points will be added to the final score.

Investment Justification Checklist

Nonprofit organizations must fully answer each question in all sections of the Investment Justification for the form to be considered complete. In their Investment Justification, nonprofit organizations should summarize the most critically important and impactful information. The Fiscal Year 2025 Investment Justification is the only document submitted to FEMA by the SAA and should be crafted using the identified threats/risks to your organization, the results of the Vulnerability Assessment of a physical location/structure/building, and details of the requested projects/activities to mitigate or remediate those vulnerabilities with associated estimated costs. ***Nonprofit organizations should describe their current threat/risk. Although historic risk may be included for context, the IJ should focus on current threats and risks.***

The IJ Checklist is divided by section and includes the specific required contents of a complete NSGP IJ. The "Overall Verification" checklist provides general, overall checks for nonprofit organizations to use to verify their work prior to IJ submission.

> **Reminder**: Applicants may submit up to six application packages for each unique physical location/address/site a nonprofit organization might have. Each Investment Justification can request up to $200,000 per location, with an upper limit of $600,000 per nonprofit organization across six unique physical locations/addresses, with a maximum of three submissions to each funding stream (NSGP-UA and NSGP-S). The amount of funding requested, and number of submissions, may not exceed these limits.

Section I – Applicant Information

- Legal Name of the Organization/Physical Address of the Facility/County
- Owning vs. Leasing/Renting and Permission to Make Enhancements
- Active Operation out of the Listed Location (i.e., fully operations at the time of application)
- Other Organizations in the Facility
- Mission Statement Summary
- Organization Type
- Organization Function
- Organization's Affiliation
  - The nonprofit subapplicant must apply on their own behalf, NOT on behalf of other entities, including government or for-profit entities.
- 501(c)(3) Tax-Exempt Designation
- Unique Entity Identifier (UEI) obtained via SAM.gov
  - Entities are not required to have a UEI at the time of application but must have a valid UEI in order to receive funds.
- Funding Stream
  - Designated high-risk urban area (if applicable).
- Federal Funding Request (total estimated cost of projects/activities)
- The total amount auto will populate in the IJ form.

Section II – Background

- Describe the symbolic value of your organization's site as a highly recognized national or historical institution, or significant institution within the community that renders the site a possible target of terrorist or other extremist attack.
- Describe any current/active role in responding to or recovering from terrorist/other extremist, human-caused, and/or natural disasters, specifically highlighting the efforts that demonstrate integration of nonprofit preparedness with broader state and local preparedness efforts.

Section III – Risk

- Threat: Describe the identification and substantiation of specific threats, incidents, or attacks against the nonprofit organization or a closely related organization, network, or cell (examples include police report, insurance claim, internet threats, etc.).
  - Threats/risks have a terrorism/other extremism nexus.
- Vulnerability: Describe your organization's susceptibility to destruction, incapacitation, or exploitation by a terrorist or other extremist attack.
  - Summary findings from the Vulnerability Assessment included in the IJ are accurate and based on the Vulnerability Assessment submitted to the SAA.
- Consequence: Describe potential negative effects/impacts on your organization's assets, systems, and/or function if disrupted, damaged, or destroyed due to a terrorist or other extremist attack.

Section IV – Facility Hardening

- Describe how the proposed projects/activities will harden (i.e., make safer/more secure) the facility and/or mitigate the identified risk(s) and/or vulnerabilities based on the Vulnerability Assessment.
  - Threats/risks are linked to existing physical vulnerabilities.
  - Requested funding logically follows the information provided from the Vulnerability Assessment.
- Describe how the proposed target hardening focuses on the prevention of and/or protection against the risk/threat of a terrorist or other extremist attack.
- Confirm that the proposed projects are allowable in accordance with the priorities of the NSGP, as stated in the NSGP NOFO.

- Confirm that the proposed projects are feasible (meaning there is a reasonable expectation based on predicable planning assumptions to complete all tasks, projects and/or activities within the subaward period of performance) and proposed milestones under the NSGP.
- Application does not present any actual or perceived conflict between grant writers/consultants and contractors/vendors sourced for projects.
- Contract security/any hiring outside of the nonprofit organization is explicitly written to not be sole sourced. Nonprofit organizations must always abide by federal and state procurement guidance.

Section V – Milestones

- Describe any key activities that will lead to milestones in the program/project and grants management over the course of the NSGP grant award period of performance.
  - NOTE: Anything involving modifications to a building or site will likely require Environmental and Historic Preservation (EHP) review. In that case, EHP review should be one of the first milestones. For more information about the NSGP's EHP process, see Environmental & Historic Preservation Guidance for FEMA Grant Applications | fema.gov.

Section VI – Project Management

- Describe the proposed management team's roles, responsibilities, and governance structure to support the implementation of the projects/activities.
- Assess the project management plan/approach.

Section VII – Impact

- Describe the outcome and outputs of the proposed projects/activities that will indicate that the investment was successful.

Funding History

- Include past funding amounts, past projects, and fiscal year of previous subawards under the NSGP.

Overall Verification: Prior to Submission

- Application package is complete. FEMA will not review incomplete application packages.
- All proposed projects/activities are allowable per the NSGP NOFO.
- IJ's content and project goals are logical and reasonable.
- FEMA-provided IJ form for the current fiscal year is submitted.
- Nonprofit organization has reviewed the grant writer's work (if applicable).
- IJ is signed by the nonprofit organization's point of contact, *not the grant writer* (if applicable).
- IJ is unique to the nonprofit organization, physical location/site/address, and vulnerabilities listed.
- IJ requests $200,000 or less.

Definitions

- Vulnerability Assessment: The Vulnerability Assessment is a documented review of your facility that identifies gaps in security. Addressing gaps as they are identified in the Vulnerability Assessment keeps a facility and its occupants, visitors, or members safer. This document is part of the foundation of an NSGP application.
- Subapplicant/Subrecipient: Individual nonprofit organizations are considered the subapplicants to the NSGP, or the subrecipients of the NSGP. The SAA is the primary applicant and recipient. Each nonprofit organization must individually submit an application to their SAA, which will then submit it to FEMA for consideration. The award itself will be made directly to the SAA. The SAA will then manage the grant and be the main point of contact for the nonprofit organizations for everything related to their grant award.
- Period of Performance: The period of performance is the length of time that recipients and subrecipients have to implement their project(s), accomplish all goals, and expend all grant funding. The period of performance under the NSGP is 36 months for the SAAs. However, a period of performance shorter than 36 months is typically given to nonprofit subrecipients. There may be situational extensions to the period of performance based on undue hardships, but recipients and subrecipients should not assume any extensions will be granted and plan for full project completion within the designated period of performance. **All costs must be incurred, and all services or goods must be completed or delivered, within the period of performance**. Unless the subrecipient and SAA have requested and received approval from FEMA for

pre-award costs, any expenditures made prior to official notification of award from the SAA and before the start of the subrecipient's period of performance will be considered unallowable.

- High-risk Urban Area: High-risk urban areas are the metropolitan locations designated in the NSGP NOFO. The urban area list is subject to change each year. Nonprofit organizations with physical locations in one of these identified high-risk urban areas are eligible under the NSGP-Urban Area (UA) program, while all other nonprofit organizations are eligible under the NSGP-State (S) program. Contact your SAA to confirm whether your organization is located within a designated high-risk urban area for the purposes of the NSGP-UA program; city limits do not always equate to the designated urban area footprint. If a nonprofit organization does not apply for the correct funding stream based on location, the application will be automatically eliminated.
- State Administrative Agency (SAA): SAAs are the designated state or territory offices that manage the NSGP awards. These offices are the primary applicants to FEMA and recipients from FEMA of NSGP funds. The SAA will make NSGP subawards to subrecipients (i.e., nonprofit organizations).
- Risk: Potential for an adverse outcome assessed as a function of hazard/threats, assets and their vulnerabilities, and consequences. In the context of NSGP applications, nonprofit organizations should describe their current threat/risk of terrorist or other extremist attack and how those identified vulnerabilities (in the Vulnerability Assessment) could potentially be exploited.
- Threat: Indication of potential harm to life, information, operations, the environment and/or property; may be a natural or human-created occurrence and considers capabilities, intentions, and attack methods of adversaries used to exploit circumstances or occurrences with the intent to cause harm.
- Vulnerability: Physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard; includes characteristic of design, location, security posture, operation, or any combination thereof, that renders an asset, system, network, or entity susceptible to disruption, destruction, or exploitation.
- Consequence: Effect of an event, incident, or occurrence; commonly measured in four ways: human, economic, mission, and psychological, but may also include other factors such as impact on the environment.
- Terrorism: Any activity that:

1. Involves an act that: A) is dangerous to human life or potentially destructive of critical infrastructure or key resources; and B) is a violation of the criminal laws of the United States or of any state or other subdivision of the United States; and
2. Appears to be intended to: A) intimidate or coerce a civilian population; B) influence a policy of a government by intimidation or coercion; or C) affect the conduct of a government by mass destruction, assassination, or kidnapping.

Additional definitions can be found in the DHS Lexicon Terms and Definitions.

Abbreviations

Abbreviation	Definition
CISA	Cybersecurity and Infrastructure Security Agency
DHS	U.S. Department of Homeland Security
EHP	Environmental Planning and Historic Preservation
FEMA	Federal Emergency Management Agency
IJ	Investment Justification
IRC	Internal Revenue Code
NOFO	Notice of Funding Opportunity
NSGP-S	Nonprofit Security Grant Program - State
NSGP-UA	Nonprofit Security Grant Program - Urban Area
PGM	Preparedness Grants Manual
SAA	State Administrative Agency
UEI	Unique Entity Identifier

Resources

This section contains a list of resources that NSGP applicants may find useful in the development of their Investment Justifications. Potential applicants can use the links listed below to access information and resources that can assist in the NSGP application process and project implementation. Resources referring to prior fiscal years are provided for historical reference only.

DHS FEMA, Grant Programs Directorate

- Learn more: Nonprofit Security Grant Program
- State Administrative Agency (SAA) Contact List: State Administrative Agency (SAA) Contacts
- NSGP Notices of Funding Opportunity and Documents: Nonprofit Security Grant Program | FEMA.gov
  - Grants Management Requirements and Procurement Under Grants: Preparedness Grants Manual (See Section 9 for NSGP-specific information)
- Investment Justification: Grants.gov (Keyword Search: FY 2025 NSGP)
- Grants Management Technical Assistance Online Training: Grants Management
- Grants Learning Center and Resources: Learn Grants
- Authorized Equipment List: Authorized Equipment List
- Environmental Planning and Historic Preservation Information: Environmental Planning and Historic Preservation (EHP) Compliance
- For general inquiries or to join email distribution list: Email FEMA-NSGP@fema.dhs.gov
- Emergency Management Planning Guides for Specific Locations: Planning Guides | FEMA.gov
- Stop the Bleed: Save a Life | StopTheBleed.org

DHS Cybersecurity and Infrastructure Security Agency (CISA)

- Faith-Based Organization Security Resources: CISA's Faith-Based Organizations and Houses of Worship
- Tabletop Exercise Package: CISA's Tabletop Exercises
- Vigilance, Power of Hello: CISA's Power Hello
- De-Escalation Resources: CISA's De-escalation Resources
- Shields Up Campaign: CISA's Shields Up

- Counter Improvised Explosive Device Resources: CISA's Counter-IED Awareness Products
- Protective Security Advisor Program: CISA's Protective Security Advisors
- Securing Public Gatherings: CISA's Securing Public Gatherings
- Physical Security Considerations for Temporary Facilities: Fact Sheet
- Vehicle Ramming Attack Mitigation: CISA's Vehicle Ramming Mitigation
- K-12 School Security Guide: CISA's School Security Guide
- Mitigating Attacks on Houses of Worship: Mitigating Attacks on Houses of Worship Security Guide
- House of Worship Self-Assessment: Security Self-Assessment
- Physical Security Resources: Physical Security
- Active Shooter Resources: Active Shooter Preparedness, Active Shooter Workshop, Translated Active Shooter Resources, and Emergency Action Plan Guide and Template
- CISA Tabletop Exercise Package Questions: Email cisa.exercises@cisa.dhs.gov
- Bombing Prevention Resources: Office for Bombing Prevention (OBP)
- Cyber Resources and Assessment Services: Cyber Resource Hub and Cyber Essentials
- Security At First Entry (SAFE): CISA SAFE Fact Sheet
- Cybersecurity Best Practices: Cybersecurity Best Practices | Cybersecurity and Infrastructure Security Agency CISA
- Reducing the Risk of a Successful Cyber Attack: Cyber Hygiene Services

DHS Center for Faith-Based and Neighborhood Partnerships

- Learn more: Faith-Based and Neighborhood Partnerships
- Resources for Faith-based and Neighborhood Partnerships: Partnerships Resources
- Preparing for Human-Caused or Natural Disaster: Plan Ahead for Disasters
- To sign up for the email listserv or contact the center: Email Partnerships@fema.dhs.gov

DHS Center for Prevention, Programs and Partnerships (CP3)

- Learn more: Center for Prevention Programs and Partnerships
- CP3 grant opportunities: Targeted Violence and Terrorism Prevention
- If You See Something, Say Something™: Awareness Resources

- Countering Terrorism and Targeted Violence: Strategic Framework Resources
- Targeted Violence and Terrorism Prevention (TVTP): Community Engagement for TVTP
- Risk Factors FAQ Sheet: Risk Factors and Indicators
- Building Peer-to-Peer Engagements: Briefing Topic
- Joint Counterterrorism Assessment Team publication: First Responder's Toolbox
- CP3 Point of Contact for National Organizations: Email CP3StrategicEngagement@hq.dhs.gov
- Request a Community Awareness Briefing: Email cabbriefingrequests@hq.dhs.gov
- For general inquiries: Email TerrorismPrevention@hq.dhs.gov

Department of Justice (DOJ) Community Relations Service (CRS)

- Learn more: Community Relations Service
- Faith and Community Resources: Protecting Places of Worship Forum
- Information on Hate Crimes: Addressing Hate Crimes
- For general inquiries: Email askcrs@usdoj.gov
- DOJ Civil Rights Division - Learn More: Civil Rights Division
- Contact Civil Rights Division or Report a Violation: Start a Report

U.S. Department of Education

- Learn more: Department of Education Grants Overview
- Training and Risk Management Tools: Risk Management Tools
- School Safety Resources: Find School Safety Resources

DHS Office of Intelligence & Analysis (I&A)

- Suspicious Activity Reporting (SAR): Nationwide SAR Initiative (NSI)
- Safety for Faith-Based Events and Houses of Worship: NSI Awareness Flyer
- National Threat Evaluation and Reporting (NTER): NTER Program
- DHS Domestic Terrorism Branch: Email DHS.INTEL.CTMC.DTBranch@hq.dhs.gov

Federal Bureau of Investigation (FBI)

- Resource Overview: FBI Resources

- FBI Field Offices: Contact List
- Report Federal Crimes: Submit online at FBI Tip form or call 1-800-CALL-FBI

Other Resources

- United State Secret Service: National Threat Assessment Center
  - Additional Information from HHS Center for Faith-based and Neighborhood Partnerships: Center for Faith-based and Neighborhood Partnerships