Fiscal Year 2022 Nonprofit Security Grant Program Subapplicant Quick Start Guide

Release Date: May 13, 2022

Nonprofit organizations should use this document as a reference when preparing to submit applications under the Nonprofit Security Grant Program (NSGP).

What is the NSGP?

The NSGP is a competitive grant program appropriated annually through the Department of Homeland Security (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 as defined by law. 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. Find more information on tax-exempt organizations at IRS.gov.

> **Tip:** As new program guidance is published annually, ensure that you have read 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.
>
> (Note: Publications are updated annually based on the fiscal year (FY). FY 2021 and prior publications should be used as historical references only since program priorities and requirements can change every year.)

How to Apply

To apply for NSGP funds, interested nonprofit organizations must apply through their State Administrative Agency (SAA). Each SAA has an established application submission process with a state-specific deadline to submit all required materials. ***The application submission deadline in the NOFO applies to the SAA and is the deadline for SAAs to submit all administratively reviewed application materials to FEMA***. You will need to contact your SAA point of contact on state-specific deadlines and supplemental application materials or requirements unique to your state. View the list of SAAs.

Nonprofit organizations must fully answer each question in all the sections of the Investment Justification(s). In their Investment Justification (IJ), nonprofit organizations should summarize the most critically important, impactful, and salient information. You may submit up to three (3) Investment Justifications, which function as an application document, per organization for up to three (3) unique physical locations/addresses. You must submit one (1) unique Investment Justification form and required documents as part of a complete submission package for each physical location/unique address. Each Investment Justification can request up to $150,000 per location for a total of $450,000 across three (3) Investment Justifications for three (3) unique physical locations/addresses. The amount of funding requested, and number of submissions, may **not** exceed these limits.

Nonprofit organizations must have a Unique Entity Identifier (UEI), which is obtained through SAM.gov. Nonprofit organizations must only 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 SAM.gov Update.

> **Tip:** NSGP has two funding streams: NSGP-State (NSGP-S) and NSGP-Urban Area (NSGP-UA). Identify and apply for the proper funding stream (NSGP-S OR NSGP-UA) based on the physical geographical location/address of the facility and whether or not it is within a high-risk urban area. A full list of eligible high-risk urban areas is in the NSGP NOFO. Contact your SAA for questions about the appropriate funding stream based on your organization's location. 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 state, 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), state or local law enforcement assessment, contractor 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. The vulnerably assessment is uniquely different than a risk/threat assessment: in essence, 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.

Tip: In preparation to describe how they intend to use NSGP grant funding, non-profit 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

The Investment Justification is a fillable template provided and required by FEMA (which will be made available through Grants.gov) that asks nonprofits 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.

Supplemental Documents

Each state is unique in how they manage and administer the NSGP. The SAA may require specific supplemental documents or templates in addition to those required by FEMA as part of the state's internal NSGP application submission requirement. However, when preparing the Investment Justification, organizations must answer questions completely and cannot rely on references to or cite page numbers of any supplemental documents as they are not submitted to nor reviewed by FEMA. Only the Investment Justification is submitted to FEMA by the SAA.

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

Scoring and Funding Recommendations

Upon submission of your completed application to the SAA, the state will review, score, and rank every complete application it has received from eligible nonprofit organizations. The results of the scoring process will be forwarded to FEMA and will inform the federal review of the Investment Justifications based on the criteria outlined in the NSGP NOFO. Following the federal review and based on a combination of state and federal scoring, nonprofit organizations are recommended for funding. The final list of recommended nonprofit organizations to be funded is provided to the Secretary of Homeland Security for final approval.

Investment Justification Checklist

Nonprofit organizations must fully answer each question in all the sections of the Investment Justification(s) for the form to be considered complete. In their Investment Justification, nonprofit organizations should summarize the most critically important, impactful, and salient information. The 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. While historic risk may be included for context, the Investment Justification should focus on current threats and risks.

Reminder: Applicants may submit up to three (3) Investment Justifications with one (1) unique Investment Justification form and required documents for each unique physical location/address. Each Investment Justification can request up to $150,000 per location for a total of $450,000 across three unique physical locations/addresses between the NSGP-UA program and NSGP-S program. The amount of

funding requested, and number of submissions, may not exceed these limits.

Below is the Investment Justification Checklist that includes the required contents of a complete NSGP Investment Justification:

Section I – Applicant Information

- Legal Name of the Organization/Physical Address of the Facility/County
- Year the Original Facility was Constructed
- Owning vs. Leasing/Renting and Permission to Make Enhancements
- Year the Organization Began Operating from the Facility
- Other Organizations in Facility
- Mission Statement Summary
- Organization Type
- Organization's Affiliation
- 501(c)(3) Tax-Exempt Designation
- Unique Entity Identifier (UEI) obtained via the System for Award Management (replaces DUNS)
- Funding Stream
  - Designated high-risk urban area (if applicable)
- Federal Funding Request (total estimated cost of projects/activities)

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 terrorism.
- Describe any role in responding to or recovering from terrorist attacks, 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.).

- Vulnerability: Describe your organization's susceptibility to destruction, incapacitation, or exploitation by a terrorist attack.
- Consequence: Describe potential negative effects/impacts on your organization's assets, systems, and/or function if disrupted, damaged, or destroyed due to a terrorist attack.

Section IV – Facility Hardening

- Describe how the proposed projects/activities will harden (make safer/more secure) the facility and/or mitigate the identified risk(s) and/or vulnerabilities based on the vulnerability assessment.
- Describe how the proposed target hardening focuses on the prevention of and/or protection against the risk/threat of a terrorist attack.
- Confirm that the proposed projects are allowable in accordance with the priorities of the NSGP (NOFO, PGM).
- 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.

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.

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 and projects under NSGP.

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 the foundation of an NSGP application.

- Underserved Communities or Populations: Communities and populations who traditionally face barriers in accessing and using publicly available resources, and includes those underserved because of geographic location, religion, sexual orientation, gender identity, underserved racial and ethnic populations, underserved because of special needs (such as language barriers, disabilities, citizenship status, or age), and any other community or population determined to be underserved by the Secretary of the Department of Homeland Security, as appropriate.

- Subapplicant/Subrecipient: Individual nonprofit organizations are considered the subapplicants or the subrecipients of the NSGP grant. 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, but the award itself will be made directly to the state or territory's 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 SAAs. However, given the SAA has a high level of administrative burden in managing the NSGP, typically a shorter period of performance than 36 months is 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 metropolitan locations designated in FEMA's Urban Area Security Initiative (UASI) program each year based on the 100 most populous metropolitan statistical areas (MSAs). Nonprofit organizations with physical locations in one of those high-risk urban areas are eligible under the NSGP-Urban Area (UA) program; all other nonprofits are eligible under the NSGP-State (S) program. The list of high-risk urban areas under UASI changes every year based on risk. A list of eligible high-risk urban areas will be included in each year's NSGP NOFO. Because high-risk urban areas often extend beyond the local city limits and because the localities included within the corresponding MSA are not always included in the high-risk urban area, 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. If a nonprofit 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 and territory offices that manage the NSGP awards. These offices are the primary applicants to and recipients of NSGP funds. The SAA will make NSGP subawards to subrecipients (e.g., nonprofit organizations).

- Potential for an adverse outcome assessed as a function of hazard/threats, assets and their vulnerabilities, and consequence. In the context of NSGP applications, nonprofit organizations should describe their current threat/risk of terroristic attack and how those identified vulnerabilities (in the vulnerability assessment) could potentially be exploited.

- 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.

- 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.

- 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.

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 FY 2021 are provided for historical reference only.

Department of Homeland Security (DHS) Federal Emergency Management Agency (FEMA), Grant Programs Directorate

- Program Overview: Nonprofit Security Grant Program

- State Administrative Agency (SAA) Contact List: State Administrative Agency (SAA) Contacts
- NSGP Notices and Documents: Notice of Funding Opportunity
- Grants Management Requirements and Procurement Under Grants: FEMA Grants
- Preparedness Grants Manual: Preparedness Grants Manual (See Appendix C for NSGP-specific information)
- Grants Preparedness Webinar: Preparedness Webinars
- Investment Justification Template: Home | GRANTS.GOV (Keyword Search: "FY 2022 NSGP")
- Grants Management Technical Assistance Online Training: Grants Management
- Grants Learning Center and Resources: Learn Grants
- Procurement Under Grants Resources Page: Contracting with Federal Funds for Goods and Services Before, During and After Disasters | FEMA.gov
- Authorized Equipment List: Authorized Equipment List
- Environmental Planning and Historic Preservation Information: Environmental Planning and Historic Preservation (EHP) Compliance
- General NSGP Inquiries and Listserv Sign Up: FEMA-NSGP@fema.dhs.gov

DHS Cybersecurity and Infrastructure Security Agency (CISA)

- Faith-Based Organization Security Resources: Faith Based Organizations and Houses of Worship
- Mitigating Attacks on Houses of Worship: Mitigating Attacks on Houses of Worship Security Guide
- House of Worship Self-Assessment: Houses of Worship Security Self-Assessment and
  Houses of Worship Security Self-Assessment User Guide and Survey
- Promoting Vigilance through the Power of Hello: Employee Vigilance - Power of Hello and
  Power of Hello Translations
- De-Escalation for Critical Infrastructure Owners and Operators: De-escalation Series
- Securing Public Gatherings Resources: Securing Public Gatherings
- Hometown Safety and Security Resources: Hometown Security
- Active Shooter Resources: Active Shooter Preparedness, Active Shooter Workshop,

Translated Active Shooter Resources, and Emergency Action Plan Guide and Template
- Bombing Prevention Resources: Office for Bombing Prevention (OBP)
- CISA Tabletop Exercise Packages: CISA Tabletop Exercises Packages
- Cyber Resources and Assessment Services: Cyber Resource Hub and Cyber Essentials
- Security At First Entry (SAFE): CISA SAFE Fact Sheet
- Personal Security Considerations: All Stakeholders
- Tips for Cybersecurity: CISA Tips
- Reducing the Risk of a Successful Cyber Attack: Cyber Hygiene Services
- Request Assistance from a CISA Protective Security Advisor (PSA): Protective Security Advisors or Central@cisa.gov

DHS Center for Faith-Based and Neighborhood Partnerships

- Resource Overview: Faith-Based and Neighborhood Partnerships
- Faith-based and Neighborhood Partnerships: Partnerships Resources
- Preparing for Human-Caused or Natural Disaster: Plan Ahead for Disasters
- President Biden Reestablishes the White House Office of Faith-Based and Neighborhood Partnerships: Fact Sheet
- Additional Information from HHS Center for Faith-based and Neighborhood Partnerships:
  Center for Faith-based and Neighborhood Partnerships
- General Inquiries and Listserv Sign Up: Partnerships@fema.dhs.gov

DHS Office for Civil Rights & Civil Liberties

- Office Overview: Civil Rights and Civil Liberties
- Make a Civil Rights Complaint: Make a Complaint
- CRCL Compliance Branch: Compliance Investigations or CRCLCompliance@hq.dhs.gov
- Join a Local Roundtable: Community Engagement or CommunityEngagement@hq.dhs.gov
- General Inquires: CRCL@dhs.gov

DHS/FEMA Office of Law Enforcement and Engagement Integration

- Office Overview: Law Enforcement and Integration

- General Inquires or to Share Events: LawEnforcementEngagement@fema.dhs.gov

DHS Center for Prevention, Programs and Partnerships (CP3)

- Center Overview: 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 TVTP
- Building Peer-to-Peer Engagements: Briefing Topic
- Joint Counterterrorism Assessment Team publication: First Responder's Toolbox
- POC for National Organizations: send email to CP3StrategicEngagement@hq.dhs.go
- Request a Community Awareness Briefing: send email to cabbriefingrequests@hq.dhs.gov
- General Inquires: TerrorismPrevention@hq.dhs.gov

Department of Justice (DOJ) Community Relations Service

- Office Overview: Community Relations Service
- Faith and Community Resources: Protecting Places of Worship Forum and Protecting Places of Worship Fact Sheet
- Information on Hate Crimes: Addressing Hate Crimes
- General Inquires: Harpreet.S.Mokha@usdoj.gov or askcrs@usdoj.gov

DOJ Civil Rights Division

- Division Overview: Civil Rights Division
- Contact Civil Rights Division or Report a Violation: Start a Report

U.S. Department of Education

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

Office of Intelligence & Analysis

- 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

Federal Bureau of Investigation (FBI)

- Resource Overview: FBI Resources
- FBI Field Offices: Contact List
- Report a Hate Crime: Submit online at FBI Tip form or call 1-800-CALL-FBI

Other Resources

- United State Secret Service: National Threat Assessment Center
- National Strategy for Countering Domestic Terrorism: Fact Sheet