Nonprofit Security Grant Program - National Security Supplemental Consortium Application Guide

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. DHS has endeavored to fulfill this commitment here, and we plan to continue delivering on this commitment.

Consortia should consider using this document as a reference when preparing applications for the Nonprofit Security Grant Program - National Security Supplemental (NSGP-NSS).

What is the NSGP-NSS?

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 for target hardening and other security enhancements to protect against terrorist attacks or other threats. 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.

In the National Security Supplemental (*Israel Security Supplemental Appropriations Act, 2024),* DHS received an additional funding package to supplement NSGP funding. $180 million of the funding was awarded as part of the Fiscal Year (FY) 2024 NSGP Notice of Funding Opportunity (NOFO). The remaining $210 million will be awarded as the NSGP-NSS.

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-NSS (NOFO) and Preparedness Grants Manual (PGM) thoroughly. Successful NSGP-NSS 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 Any publications from prior fiscal years, or published before the NOFO, should be used as historical references only since program priorities and requirements can change every year.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 as a Consortium

A consortium application is an opportunity for one nonprofit organization to act as a lead and apply for funding on behalf of itself and any number of other participating NSGP-NSS eligible nonprofit organizations. A consortium of nonprofit organizations must fill out one IJ (done by the consortium lead) and the Consortium Workbook, in addition to the Vulnerability Assessment(s) and Mission Statements. All nonprofit organizations in the consortium application must be compliant with the NSGP-NSS eligibility requirements. 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 shall not distribute grant-funded assets to anyone outside those partner organizations listed in the IJ and Workbook and approved for funding by DHS/FEMA. Additionally, 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.

Consortia lead organizations must apply to the NSGP-NSS 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. You will need to contact your SAA point of contact on 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.

Applying for the Correct Funding Stream

NSGP-NSS has two funding streams: NSGP-NSS-State (NSGP-NSS-S) and NSGP-NSS-Urban Area (NSGP-NSS-UA). 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-NSS 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.

For consortium applications, **all nonprofit organizations within a consortium application must be eligible under the applied-for funding stream**. For example, if a consortium applies to the SAA to receive funding under NSGP-NSS-UA, all nonprofit organizations within the consortium must be located within the same FY 2024 UASI-designated high-risk urban areas.

Consortium Funding Limits

Consortia may apply through the SAA for a subaward totaling up to $1 million. Subawards over $250,000 must comply with the Build America, Buy America Act (BABAA). For more information, see the NOFO. The up to $200,000 per nonprofit member location/physical site/address 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.

Total funding available for consortium applications is limited to 25% of the total NSGP-NSS award allocation, or $52.5 million.

- $26.25 million is available for consortium subapplicants in NSGP-NSS-S.
- $26.25 million is available for consortium subapplicants in NSGP-NSS-UA.

UEI Requirements

Unique Entity Identifier (UEI) are obtained through SAM.gov. *The lead nonprofit organization for a consortium is 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. Lower-tier subrecipients (meaning entities receiving funds passed through by a higher-tier subrecipient) are not required to have a UEI and are not required to register in SAM. This means that nonprofit organizations within consortia that are not the lead organization are **not** required by federal mandate to have a valid UEI at any point in the award lifecycle, unless otherwise mandated by their 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.**

Applicants (the SAA) are also not permitted to require subrecipients (nonprofit organizations awarded NSGP-NSS funding) to complete a full registration in SAM beyond obtaining the UEI.

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.

Each consortium must submit Mission Statements for all participating nonprofit organizations in the consortium, including the lead organization, and any mission implementation policies or practices that may elevate the organization’s risk to the SAA.

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-NSS 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 Vulnerably 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-NSS 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 anytime 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 additional vulnerability assessment requirements.

Consortia have the option to 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.

Investment Justification (IJ)

The IJ is a fillable template, available through Grants.gov, that asks consortia to describe the consortium, risks/threats to the consortium, and proposed projects/activities to mitigate security deficiencies (as identified in the Vulnerability Assessment) utilizing NSGP-NSS funding. The IJ is published with the NOFO and is not available prior to 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 or funding opportunity, as released on Grants.gov.

For additional information on the components of an IJ for consortia, please see the section Investment Justification Checklist.

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:

- Demographic information, including the name, address, nonprofit organization type, organization function, and organization affiliation;
- 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
- Additional narrative information, including how each nonprofit organization's projects address the objective of the consortium application as outlined in the lead nonprofit organization's IJ.

A fully completed Consortium Workbook is required for all consortia. Consortium workbooks should be saved using the following file convention for NSGP-NSS-UA applications:

NSGP-NSS_UA_C_<State Abbreviation>_<Urban Area>_<Consortium Lead Name>

and for NSGP-NSS-S:

NSGP-NSS_S_C_<State Abbreviation>_<Consortium Lead Name>

For additional information, please see the section Consortium Workbook Checklist.

Supplemental Documents

Each state or territory is unique in how they manage and administer the NSGP-NSS. The SAA may require additional documents or specific application materials as part of the state or territory's internal NSGP-NSS application submission requirement. However, when preparing the IJ, consortia 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 and the consortium workbook 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 subapplicants based on the criteria outlined in the NSGP-NSS 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, subapplicants are recommended for funding. The final list of recommended subapplicants to be funded is provided to the Secretary of Homeland Security for final approval.

Consortium applications will be scored and ranked **separately** from individual nonprofit organizations. Each consortium will receive their own rank and score based on the criteria outlined in the NOFO.

Additional Points

Additional "bonus" points are added to the final scores of subapplicants based on their service to disadvantaged communities. To advance considerations of equity in awarding NSGP-NSS grant funding, FEMA will add 10 additional points to the scores of organizations that are located within a disadvantaged community. FEMA will apply the Council on Economic Quality's Climate and Economic Justice Screening Tool (CEJST) to each subapplicant using the address of their physical location to identify whether a community is considered "disadvantaged" per the tool's methodology (CEJST Methodology). Bonus points will be applied for consortium applications based on the qualifying characteristics of the lead nonprofit organization.

Multipliers are also applied as part of the NSGP-NSS scoring process. To calculate an applicant's final score, the subapplicant's SAA score will be multiplied:

- By a factor of four for nonprofit organizations facing heightened threat resulting from the Israel-Hamas war ***(note – subapplicants must draw a clear connection between the heightened threat they face and the Israel-Hamas war in their project narratives to qualify for this multiplier)***;
- By a factor of three for all other ideology-based/spiritual/religious entities (e.g., houses of worship, ideology-based/spiritual/religious educational institutions, ideology-based/spiritual/religious medical facilities, etc.);
- By a factor of two for secular educational and medical institutions; and
- By a factor of one for all other nonprofit organizations.

Below are general examples of organizational scenarios that may be eligible for the factor of 4 multiplier. Any nonprofit organization that can demonstrate it faces heightened threat is eligible for the multiplier, regardless of the organization's purpose, mission, viewpoint, membership, or affiliations. Examples of nonprofits that may qualify include, but are not limited to:

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

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

Consortium Award Management

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.

The lead consortium member will be responsible for any Environmental Planning and Historic Preservation (EHP) requirements. Anything involving modifications to a building or site will likely require EHP review. For more information about the NSGP-NSS' s EHP process, see FEMA Policy: Grant Programs Directorate Environmental Planning and Historic Preservation.

All successful applicants for NSGP-NSS are required to comply with DHS Standard Terms and Conditions, and as the SAA is the *applicant* with the consortium as the *subapplicant*, the SAA is responsible for the management of the relationship with the lead consortium member and ensuring that the consortium adheres to the terms and conditions outlined in the subaward.

Additionally, the lead consortium member will be responsible for any Build America, Buy America Act (BABAA) requirements if awarded over $250,000. If awarded over $250,000, none of the funds provided under the NSGP-NSS may be used for a project for infrastructure unless the iron and steel, manufactured products, and construction materials used in that infrastructure are produced in the United States. The Buy America preference only applies to articles, materials, and supplies that are consumed in, incorporated into, or affixed to an infrastructure project. As such, it does not apply to tools, equipment, and supplies, such as temporary scaffolding, brought to the construction site and removed at or before the completion of the infrastructure project. Nor does a Buy America preference apply to equipment and furnishings, such as movable chairs, desks, and portable computer equipment, that are used at or within the finished infrastructure project but are not an integral part of the structure or permanently affixed to the infrastructure project. For additional details, please see the NSGP-NSS NOFO or FEMA's official policy on BABAA, FEMA Policy 207-22-0001: Buy America Preference in FEMA Financial Assistance Programs for Infrastructure.

Investment Justification Checklist

The lead nonprofit organization must fully answer each question in all the sections of the Investment Justification (IJ) for the form to be considered complete. ***Consortia 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 sections and includes the specific required contents of a complete NSGP-NSS IJ. When asking for collective or shared summaries through the IJ, the lead nonprofit organization is encouraged to think holistically about how the risks, threats, vulnerabilities, and proposed projects are connected across the consortium.

Section I – Applicant Information

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.

☐ Legal Name of the Lead Organization/Physical Address of the Facility/County

☐ Consortium Application Identification

☐ Owning vs. Leasing/Renting and Permission to Make Enhancements

☐ Application is Part of vs. Not Part of a Consortium

☐ Active Lead Organization out of the Listed Location (i.e., fully operations at the time of application)

☐ Other Lead Organizations in the Facility

☐ Mission Statement Summary

☐ Lead Organization Type

☐ Lead Organization Function

☐ Lead Organization's Affiliation

☐ 501(c)(3) Tax-Exempt Designation

☐ Unique Entity Identifier (UEI) obtained via SAM.gov

- The lead organizations for consortia are not required to have a UEI at the time of application but (as a potential first tier subrecipient), **must obtain and provide a valid UEI to the SAA as the (grantee) in order to enter into a subrecipient agreement (subaward) with the SAA.** Nonprofit organizations within consortia (potential second tier subrecipients), are not the lead organization and therefore not required by federal requirements to have a valid UEI unless otherwise required by their SAA.

☐ 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

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.

☐ Summarize the symbolic value of the consortium's sites as a highly recognized national or historical institutions, or significant institutions within the community that renders the sites as possible targets of terrorist or other extremist attack.

☐ Summarize 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

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

☐ Heightened Threat: Confirm whether the consortium faces a heightened threat resulting from the Israel-Hamas war.

☐ Threat: Summarize the identification and substantiation of specific threats, incidents, or attacks against the consortium nonprofit organizations 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: Summarize your consortium'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: Summarize potential negative effects/impacts on your consortium's assets, systems, and/or function if disrupted, damaged, or destroyed due to a terrorist or other extremist attack.

Section IV – Facility Hardening

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.

☐ Describe how the proposed projects/activities will harden (make safer/more secure) the consortium's facilities 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-NSS, as stated in the NSGP-NSS 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-NSS.

☐ 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

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.

☐ Describe the key activities of the consortium that will lead to milestones in the program/project and grants management over the course of the NSGP-NSS grant award period of performance.

- NOTE: Anything involving modifications to a building or site will likely require Environmental Planning and Historic Preservation (EHP) review. In that case, EHP review should be one of the first milestones listed. Environmental Planning and Historic Preservation (EHP) Compliance

Section VI – Project Management

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.

☐ 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

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.

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

Funding History

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.

☐ Include past funding amounts, past projects, and fiscal year of previous subawards of the lead nonprofit organization 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-NSS NOFO.

☐ IJ's content and project goals are logical and reasonable.

☐ FEMA-provided IJ form for the current funding opportunity is submitted.

☐ Lead nonprofit organization has reviewed the grant writer's work (if applicable).

☐ IJ is signed by the consortium lead nonprofit organization's point of contact, *not the grant writer* (if applicable).

☐ IJ is unique to the consortium's nonprofit organizations, physical locations/sites/addresses, and vulnerabilities listed.

☐ IJ clearly identifies shared threat, vulnerability and consequences of risk(s) facing all nonprofit organizations within the consortium and demonstrates how the proposed investments respond to or support the recovery from the identified shared risks.

☐ IJ requests $1,000,000 or less.

Consortium Workbook Checklist

The Consortium Workbook provides an opportunity to expand upon the details provided in the consortium ’ s IJ. The lead nonprofit organization must provide all required information in the Consortium Workbook for the form to be considered complete.

The Consortium Workbook Checklist is divided by tabs in the Excel sheet and includes the specific required contents of a complete NSGP-NSS Consortium Workbook.

Instructions

Provides instructions on how to fill out the Consortium Workbook. Read all instructions before entering information.

Consortium Overview

☐ Full Legal Name of the Lead Organization Applying for Funding

☐ Number of Nonprofit Organizations in the Consortium, Including the Lead Organization

☐ Amount of Federal **Funding Requested by the Lead Nonprofit Organization** for their Location

☐ Total Funding Amount Requested for the **Entire Consortium**

- Automatically calculated based on the lead organization funding amount and any funding amounts added to the total federal funding requested (Column F) in the Nonprofit Organization Details Tab.
- This number should equal the amount requested in the IJ.

Nonprofit Organizations Details

☐ Full Legal Name of All Organizations Participating in the Consortium

☐ Complete Physical Address of the Building that Houses each Participating Organization

- This should include the street address (not a PO Box), City, State, and Zip Code.

☐ Name of the Point of Contact for each Nonprofit Organization

☐ Phone Number of the Point of Contact for each Nonprofit Organization

☐ Email of the Point of Contact for each Nonprofit Organization

☐ Amount of Federal Funding Requested by each Nonprofit in the Consortium

☐ Yes or No Based on Whether the Nonprofit Provided a Mission Statement

- NOTE: Mission Statements are required for all organizations.

☐ Yes or No Based on Whether the Organization Self-Identifies as Facing Heightened Threat Resulting from the Israel-Hamas War

☐ Type of Nonprofit Category for the Organization from the Drop-Down List

☐ Function of Organization from the Drop-Down List

☐ Describe "Other" if this Option was Selected in the Type of Nonprofit Category or the Function of Organization

☐ Religious Affiliation of the Nonprofit Organization

☐ Describe "Other" if this Option was Selected in Religious Affiliation

☐ Verify the Eligibility of the Nonprofit Organization Using the NSGP-NSS NOFO Requirements

☐ (If required by your SAA) The UEI Number

☐ Yes or No Based on Whether the Nonprofit has Previously Received NSGP Funding

☐ 'Individual' or 'Shared' Based on Whether the Consortium Application Included One Vulnerability Assessment per Nonprofit Organization (Individual) or One Shared Vulnerability Assessment (Shared)

☐ Threat Description: In considering a threat, describe the identification and substantiation of specific threats or attacks against the nonprofit organization or a closely related organization, network, or cell. Description can include findings from a threat or risk assessment, police report(s), and/or insurance claims specific to the location being applied for including dates of specific threats.

☐ Vulnerabilities Description: Describe the organization's susceptibility to destruction, incapacitation, or exploitation by a terrorist or other extremist attack.

☐ Potential Consequences Description: Describe the potential negative effects on the organization's assets, systems, and/or function if damaged, destroyed, or disrupted by a terrorist or other extremist attack.

☐ Facility Hardening Description: Describe each proposed activity or investment, identify the vulnerability that it addresses, and detail the cost associated with the activity or investment. For each activity/investment, include the quantity, estimated hourly rate or estimated price per unit, and proposed usage. Note: This section should include narrative information about all costs. The objective is for the information contained in this section to allow reviewers to validate the need of all costs. Allowable costs include facility hardening activities, such as planning and exercise related costs, contracted security personnel, and security-related training courses and programs limited to the protection of critical infrastructure key resources. Funding can also be used for the acquisition and installation of security equipment on real property (including buildings and surrounding property) owned or leased by the nonprofit organization, specifically in prevention of and/or in protection against the risk of terrorist or other extremist attack.

☐ Impact Description: Describe the measurable outputs and outcomes that will indicate that this Investment is successful at the end of the period of performance.

AEL Information

☐ Organization Name and Address

- Organization name and address are automatically populated based on the entries in the Nonprofit Organization Details tab.

☐ AEL Code for each Column (#1 - #10) and Title for each AEL Requested as Part of the Investment

☐ Vulnerabilities the Equipment/Project/Activity (AEL #1 - #10) Addresses for the Corresponding AEL Number

☐ Estimated Funding Requested (Round up to the Nearest Dollar) for the Corresponding AEL (#1 - #10) Number

Key Milestones

☐ Organization Name and Address

- Organization name and address are automatically populated based on the entries in the Nonprofit Organization Details tab.

☐ Descriptions and Associated Key Activities (#1 - #10) that Lead to the Milestone Event Over the NSGP Period of Performance

☐ Start Date for the Corresponding Key Milestone(s) (#1 – #10)

- Start dates should reflect the start of the associated key activities.

☐ Completion Date for the Corresponding Key Milestone(s) (#1 – #10)

- Completion dates should reflect when the milestone event will occur.

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-NSS application.

- Disadvantaged Communities: The NSGP-NSS uses the term “disadvantaged communities” to apply to any community identified as “disadvantaged” by CEJST. CEJST uses datasets as indicators of burdens, which are organized into categories. A community is highlighted as disadvantaged on the CEJST map if it is in a census tract that is (1) at or above the threshold for one or more environmental, climate, or other burdens; and (2) at or above the threshold for an associated socioeconomic burden.

- Subapplicant/Subrecipient: Individual nonprofit organizations and consortium of nonprofit organizations are considered the subapplicants to the NSGP-NSS, or the subrecipients of the NSGP-NSS. The SAA is the primary applicant and recipient. Nonprofit organizations may individually submit an application or apply as part of a group of nonprofits in a consortium 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 and consortium for everything related to their grant award. In the case of a consortium application, only one application package from the identified lead will be accepted.

- 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-NSS is 36 months for the SAAs, However, a period of performance shorter than 36 months is typically given to 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 FEMA's Urban Area Security Initiative (UASI) program each year. The UASI list is available in each year's NSGP-NSS NOFO and 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-NSS-Urban Area (UA) program, while all other nonprofit organizations are eligible under the NSGP-NSS-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-NSS-UA program; city limits do not always equate to the designated UASI 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-NSS awards. These offices are the primary applicants to FEMA and recipients from FEMA of NSGP-NSS funds. The SAA will make NSGP-NSS 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 consequence. In the context of NSGP-NSS applications, nonprofit organizations should describe their current threat/risk of terroristic 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
CEJST	Council on Economic Quality’s Climate and Economic Justice Screening Tool
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-NSS-S	Nonprofit Security Grant Program – National Security Supplemental - State
NSGP-NSS-UA	Nonprofit Security Grant Program – National Security Supplemental - Urban Area
PGM	Preparedness Grants Manual
SAA	State Administrative Agency
UASI	Urban Area Security Initiative
UEI	Unique Entity Identifier

Resources

This section contains a list of resources that NSGP-NSS 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-NSS 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: FEMA Grants
- Preparedness Grants Manual: Preparedness Grants Manual (See Appendix C for NSGP-specific information)
- Preparedness Webinars: Preparedness Webinars
- Investment Justification: Grants.gov (Keyword Search: FY 2024 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: send an email to FEMA-NSGP@fema.dhs.gov
- Emergency Management Planning Guides for Specific Locations: Planning Guides | FEMA.gov
- What to do until help arrives: You Are the Help Until Help Arrives (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
- Hometown Safety and Security Resources: Hometown Security
- 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: 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
- Personal Security Considerations: Personal Security Considerations (cisa.gov)
- 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

- President Biden Reestablishes the White House Office of Faith-Based and Neighborhood Partnerships: Fact Sheet
- Resources for Faith-based and Neighborhood Partnerships: Partnerships Resources
- Preparing for Human-Caused or Natural Disaster: Plan Ahead for Disasters
- Additional Information from HHS Center for Faith-based and Neighborhood Partnerships: Center for Faith-based and Neighborhood Partnerships
- To sign up for the email listserv or contact the center: send email to Partnerships@fema.dhs.gov

DHS Office for Civil Rights & Civil Liberties (CRCL)

- Learn more: Civil Rights and Civil Liberties
- Learn more: Office of Law Enforcement and Integration
- Make a Civil Rights Complaint: Make a Complaint
- CRCL Compliance Branch: Compliance Investigations or send email to CRCLCompliance@hq.dhs.gov
- Community Outreach: Community Engagement or send email to CommunityEngagement@hq.dhs.gov to join a local round table
- FEMA Office of Equal Rights: External Civil Rights Division | FEMA.gov
- For general inquiries: send email to CRCL@dhs.gov
- For general inquiries or to share events: send email to LawEnforcementEngagement@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: send email to cabbriefingrequests@hq.dhs.gov
- For general inquiries: send email to 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 and Protecting Places of Worship Fact Sheet
- 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: DHS.INTEL.CTMC.DTBranch@hq.dhs.gov

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