Commonwealth of Massachusetts
Executive Office of Public Safety and Security
Office of Grants and Research
Notice of Availability of Grant Funds

Federal Fiscal Year 2024
Nonprofit Security Grant Program
National Security Supplemental Funding

Maura T. Healey	**Kimberley Driscoll**
Governor	**Lieutenant Governor**
Terrence M. Reidy	**Kevin J. Stanton**
Secretary	**Executive Director**

FFY24 Nonprofit Security Grant Program
National Security Supplemental Funding
Notice of Availability of Grant Funds (AGF)
Office of Grants and Research

November 22, 2024

Introduction
The Massachusetts Office of Grants and Research (OGR) promotes public safety and security through the management of grants funds and research programs focused on crime prevention and intervention, traffic safety, law enforcement and homeland security initiatives. OGR is not only the state administering agency (SAA) for federal funds received from the Department of Homeland Security (DHS) Federal Emergency Management Agency (FEMA), Department of Justice (DOJ) and the National Highway Traffic Safety Administration (NHTSA) but also administers safety and security grants authorized by the Massachusetts Legislature. OGR manages more than $279 million in state and federal grants that are distributed to state, municipal, education, nonprofit and tribal agencies across the Commonwealth.

OGR will make funding available for **nonprofit 501(c)(3) organizations** (such as faith-based institutions, medical and health care facilities, and other human service entities) to competitively solicit one-time grant funding to enhance the protection of soft targets/crowded places as well as secure the community's effective planning, training and awareness campaigns, and exercises. The federal funding amount available for this AGF is dependent upon the federal target allocation to the State, which is $2,137,500. This allocation is for nonprofits outside the UASI-designated high-risk Urban Area (UA). The final federal allocation to the UA, which is composed of the UASI Metro-Boston area[1], is approximately $2,000,000 (final amount will be determined by FEMA). This Availability of Grant Funds (AGF) will provide all the information needed to apply for the **FFY24 Nonprofit Security Grant Program National Security Supplemental (NSGP-NSS)**.

Overview of Funding Opportunity
These funds are intended to focus on enhancing the ability of nonprofits to prevent, protect against, prepare for, and respond to terrorist or other extremist attacks. The program will improve the physical/cyber security and facility/target hardening of nonprofit organizations' facilities at risk of a terrorist of other extremist attack, ultimately safeguarding the lives and property of the American people. All funded projects must be for the purpose of enhancing the security and safety at the physical site of the nonprofit organization. These funds also aim to integrate nonprofits' preparedness activities with broader state and local preparedness efforts.

This opportunity is composed of two funding streams:
- **The Nonprofit Security Grant Program National Security Supplemental - Urban Area** (NSGP-NSS-UA) is a competitive grant program that will fund nonprofits located in federally designated high-risk Metro Boston urban area. *In Massachusetts, the UASI*

---

[1]*In Massachusetts, the UASI Metro Boston area is Boston, Brookline, Cambridge, Chelsea, Everett, Quincy, Revere, Somerville, and Winthrop.*

Metro Boston area is Boston, Brookline, Cambridge, Chelsea, Everett, Quincy, Revere, Somerville, and Winthrop. FEMA will determine the final allocation for the NSGP-NSS-UA. Massachusetts anticipates that the NSGP-NSS-UA will likely be proportionate to the NSGP-NSS-S allocation.

- **The Nonprofit Security Grant Program National Security Supplemental - State** (NSGP-NSS-S) is a competitive grant program that will fund nonprofits located outside the UASI-designated high-risk urban area. Massachusetts has received an allocation of $2,137,500 for the NSG-NSS-S.

All applications must be submitted to the OGR. As the SAA for DHS funding, OGR is the ONLY entity in Massachusetts that may then submit FFY 2024 NSGP-NSS applications directly to the DHS/FEMA. Final award decisions will be made by DHS/FEMA

Maximum Funding Request for MA Applicants	
Maximum Funding Request for NSGP-UA	Up to $200,000/site
Maximum Funding Request for NSGP-S	Up to $200,000/site

Key Dates:

DATE	TASK
November 22, 2024	AGF Posted
December 9, 2024, at 11:00 am	Application Assistance Webinar Register here
December 17, 2024, at 3:00 pm	Application Submission Deadline
May 2025-April 2027	Performance Period

Project Period of Performance
All funded projects or activities will end no later than **April 30, 2027**. Please adhere to this timeframe in the Investment Justification's Milestones section.

Eligible Applicants
Nonprofit organizations (as described under section 501(c)(3) of the Internal Revenue Code of 1986) located in Massachusetts that are at high-risk of a terrorist or other extremist attack are eligible to apply. For NSGP-NSS-UA, organizations must also be located within an FY 2024 UASI-designated high-risk urban area. For NSGP-NSS-S, organizations must be located outside of an FY 2024 UASI-designated high-risk urban area.

Criteria for identifying eligible applicants who are at high-risk of terrorist attacks include, but are not limited to:

- Evidence of prior threats or attacks (from within or outside the U.S.) by a terrorist

organization, network/cell against the applicant or closely related organizations (e.g. police reports or insurance claims).   Please identify and substantiate any heightened threat resulting from the Israel-Hamas war.
- Symbolic value of the site(s) that renders the site a possible target of terrorism.
- Role of the applicant in responding to or recovering from terrorist attacks.
- Findings from previous risk, threat, or vulnerability assessments.

Nonprofits with Multiple Sites
Applicants must be a nonprofit 501(c)(3) organization and demonstrate, through the application, that the organization is at high risk of a terrorist or other extremist attack. For NSGP-NSS-UA and NSGP-NSS-S, each nonprofit organization may only request funding for one site/location/physical address per application. Applicants may solicit up to $200,000 per site under this competitive grant. Nonprofit organizations with multiple sites/locations/physical addresses may choose to apply for additional sites for up to $200,000 per site, for a maximum of three sites per funding stream, not to exceed $600,000 total. Separate applications must be submitted for each location. Nonprofit organization with sites in both NSGP-NSS-S and NSGP-NSS-UA areas may apply for a total of up to six sites, but the total of their applications cannot exceed $600,000. If a nonprofit submits applications for projects at multiple sites, regardless of whether the projects are similar in nature, each individual site must include an assessment of the vulnerability and risk unique to each site. That is, one vulnerability assessment must be submitted for each location/physical address. Failure to do so may be cause for rejection of the application.

Consortia Applicants
For the NSGP-NSS, a group of nonprofit organizations may collaborate to submit a consortium application (also known as a joint application) in which one nonprofit acts as the lead applicant and applies for funding on behalf of itself and any number of other consortium member nonprofit organizations. Funding availability for consortia applicants is in addition to the amount of funds indicated in the introduction section. **Nonprofit organizations may not apply both individually and as part of a consortium.** Each consortium member may apply for up to $200,000 for their site with a maximum funding request of $1,000,000 per consortium. If awarded, the lead consortium member will accept the subaward on behalf of the consortium, as well as implement and manage the approved projects/contracts for all consortium member sites throughout the period of performance. This includes ensuring that all terms and conditions of the subaward are met for all consortium members. **Additionally, consortium applicants are required to fill out and submit a Consortium Workbook which captures the necessary data for all participating consortium nonprofit organizations.**

- **Build America, Buy America Act (BABAA)**
  Consortium awards that total over $250,000 must comply with the Build America, Buy America Act: https://www.fema.gov/grants/policy-guidance/buy-america.

Unique Entity Identifier and System for Awards Management
Effective April 4, 2022, the Federal Government transitioned from using the Data Universal Numbering System (DUNS number) to a new, non-proprietary identifier known as a Unique Entity Identifier (UEI). For entities that had an active registration in the System for Award Management

(SAM) prior to this date, the UEI has automatically been assigned and no action is necessary. For all entities filing a new registration in SAM.gov on or after April 4, 2022, the UEI will be assigned to that entity as part of the SAM.gov registration process. Additional information on UEI registration, please refer to GSA.gov's Unique Entity Identifier Update.

Application Requirements:

1. **Investment Justification (IJ)**
   All applicants must submit an Investment Justification (IJ) **utilizing the FFY 2024 NSGP IJ Template.** Application materials, including the IJ, are available on OGR's **NSGP-NSS program page**,.

   Nonprofit organizations with one site may apply for up to $200,000 for that site. Nonprofit organizations (not applying as part of a consortium) with multiple sites may apply for up to $200,000 per site, for up to three sites per funding stream (NSGP-NSS-U or NSGP-NSS-S) for a maximum of $600,000. If a nonprofit organization applies for multiple sites, it must submit one complete IJ for each site. IJs cannot include more than one physical site and must identify the site's physical address (not a PO Box #) to be considered eligible. The nonprofit must occupy the location at the time of application.

   Each IJ must describe how the proposed funding will be used to improve the nonprofit's security against terrorist or extremist attacks. The IJ must address an identified risk, including threat and vulnerability, and how the funds will be used to support at least one of the following capabilities identified in the National Preparedness Goal: prevention, protection, response, recovery, and mitigation.

   For consortia, the lead nonprofit organization must include information in the IJ to that identifies shared threats, vulnerabilities, and consequences of the risk facing all nonprofit organizations within the consortium and demonstrate how the proposed investments prevent, protect, respond to or support the recovery from the identified shared risk of terrorism.

   All proposed projects must be: 1) both feasible and effective at reducing the risks for which the project was designed; and 2) able to be fully completed by **April 30, 2027**.

   Applicants must ensure that their IJ is consistent with all applicable requirements outlined in the FFY 2024 NSGP-NSS Notice of Funding Opportunity (NOFO) available on OGR's **NSGP-NSS program page**, and must support the National Preparedness Goal.

2. **Budget Workbook**
   Each applicant must include with its application this budget summary and detail of allowable costs. Applicants must use the template provided and submit the workbook in Excel format (i.e., do not convert to PDF or another format).

3. **Applicant Signature Page**

Each applicant must include with its application the Signature Page signed by the nonprofit organization's authorized representative.

4. **Vulnerability Assessment**

   To be eligible for this grant funding, each applicant must submit a vulnerability assessment **unique to each site** for which the IJ is being submitted. The vulnerability assessment must be submitted as a separate attachment in a PDF or Word format.

5. **Mission Statement**

   Each applicant must include with its application its Mission Statement in a PDF or Word format. Recognizing the impact an organization's ideology, beliefs, or mission may have on their risk of potential terror threats, OGR will use the Mission Statement along with information provided in the applicant's IJ to validate the organization type identified in the IJ as either 1) Ideology-based/Spiritual/Religious, 2) Educational, 3) Medical, or 4) Other. The organization type is a factor when calculating the final score of the application.

6. **OGR Risk Assessment Form**

   Federal regulations require OGR to evaluate each sub-recipient's risk of noncompliance with Federal statutes, regulations, and the terms and conditions of the sub-award in order to determine appropriate sub-recipient monitoring. NSGP applicants must complete this form and submit it with the application.

Consortia Application Requirements

The consortia's lead nonprofit organization is required to self-identify with one of the following categories in the IJ as part of the application process: 1. Ideology-based/Spiritual/Religious (Houses of Worship, Educational Institutions, Medical Facilities, etc.); 2. Educational (secular); 3. Medical (secular); or 4. Other.

Consortia are required to fill out and submit the following forms:

1. **Investment Justification (IJ)**
   o Part 1, Nonprofit Organization Sub-Applicant Information – The lead nonprofit organization of the consortium must fill out the required fields based solely on the lead nonprofit organization's information.
   o Part 2, Background Information – The lead nonprofit organization must summarize the shared background information of all nonprofit organizations within the consortium.
   o Part 3, Risk – The lead nonprofit organization must summarize the threats, vulnerabilities, and potential consequences facing <u>all</u> nonprofit organizations within the consortium. Additional space for further detail and more information is available in the Consortium Workbook.
   o Part 4, Facility Hardening – The lead nonprofit organization must summarize how the proposed activities or investments of the consortium address the shared vulnerabilities identified in Part 3. For Section IV-B, the lead organization must input the total funding requested for all nonprofit organizations within the consortium under each allowable category.
   o Part 5, Milestones – The lead nonprofit organization must provide the key milestones

for the proposed activities of all nonprofit organizations within the consortium.
- o Part 6, Project Management – An individual from the lead nonprofit organization must be identified to oversee the projects carried out by the nonprofit organizations in the consortium and assess their plans.
- o Part 7, Impact – The lead nonprofit organization must describe the key measurable outputs and outcomes for all nonprofit organizations within the consortium.
- o In Funding History and the Nonprofit Sub-applicant Contact Information sections, the lead nonprofit organization must fill out the required fields based solely on the lead nonprofit organization's information.

2. **Consortium Workbook**
   - o Instructions can be found in the instructions tab of the Consortium Workbook. The Consortium Workbook must expand upon the information provided in the consortium lead nonprofit organization's IJ. The Consortium Workbook must contain the number of nonprofit organizations within the consortium and the following information for each nonprofit:
     - Identifying information, including the nonprofit's name, physical 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.
     - Additional narrative information, including how each nonprofit organization's proposed projects address the objective of the consortium application as outlined in the lead nonprofit organization's IJ.

3. **Vulnerability/Risk Assessments**
   - o 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.

4. **Mission Statement**
   - o A consortium must submit Mission Statements for each participating nonprofit organizations and any mission implementation policies or practices that may elevate the organization's risk.

Allowable Costs
Funds must be spent in compliance with applicable rules and regulations. NSGP-NSS allowable costs are focused on security-related activities. Funding can be used for contracted security personnel; security-related planning, exercises, and training; and the acquisition and installation of security equipment (including improvements to current equipment) and cybersecurity measures on real property (including buildings) owned or leased by the nonprofit organization at the time of application. Applicants should indicate in their budget narrative if a cost includes shipping. It is not required to break the costs out as separate from the relevant purchase(s).

Allowable Budget Cost Categories	Description
Planning	Funding may be used for security or emergency planning expenses and the materials required to conduct planning activities. Planning must be related to the protection of the facility and the people within the facility; this should include those with access and functional needs as well as those with limited English proficiency. Planning efforts can also include conducting risk and resilience assessments on increasingly connected cyber and physical systems, on which security depends, using the Resilience Planning Program | CISA and related CISA resources. Examples of planning activities allowable under this program include: • Development and enhancement of security plans and protocols. • Development or further strengthening of security assessments. • Emergency contingency plans. • Evacuation/Shelter-in-place plans. • Coordination and information-sharing with fusion centers; and • Other project planning activities with prior approval from FEMA. • Please be advised that pre-award planning costs are not allowable. Any related planning costs incurred must be after the award is made and fully executed.
Equipment	Funding may be used for the acquisition and installation of security equipment on real property owned or leased by the nonprofit organization, specifically to prevent or protect against a terrorist attack. Unless otherwise stated, equipment must meet all mandatory statutory, regulatory, and FEMA-adopted standards to be eligible for purchase using these funds, including the Americans with Disabilities Act. Equipment is limited to select items per FEMA. (See appendix.)
Maintenance and Sustainment	Maintenance and sustainment costs, such as maintenance contracts, warranties, repair or replacement costs, upgrades, and user fees are allowable. For additional information, see the Preparedness Grants Manual.
Training/Exercises	Nonprofit organization security personnel and staff may use these funds to attend security-related training courses, exercises, and programs in the United States. Allowable training-related costs under NSGP-NSS are limited to attendance fees for the training and related expenses, such as materials, supplies, and/or equipment. Nonprofit organizations may also use NSGP-NSS award funds to provide on-site security training for employees, members, and congregants. Overtime, backfill, and/or travel expenses are not allowable costs. Allowable training topics are limited to the protection of critical infrastructure key resources, including physical and cybersecurity, facility hardening, and terrorism/other extremism awareness/employee preparedness such as Community Emergency Response Team (CERT) training, indicators and behaviors indicative of terrorist/other extremist threats, Active Shooter training, and emergency first aid training. Additional examples of allowable training courses include: "Stop the Bleed" training, kits/equipment, and training aids; First Aid and other novice level "you are the help until help arrives" training, kits/equipment, and training aids; and Automatic External Defibrillator (AED) and AED/Basic Life Support training, kits/equipment, and training aids. Training conducted using these funds must address a specific threat and/or vulnerability, as identified in the application Investment Justification (IJ). Training should provide the opportunity to demonstrate and validate skills learned as well as to identify any gaps in these skills. Proposed attendance at training courses and all associated costs using the NSGP-NSS must be

Allowable Budget Cost Categories	Description
	included in the IJ. The Homeland Security Exercise and Evaluation Program (HSEEP) provides a set of guiding principles for exercise programs, as well as a common approach to exercise program management, design, and development, conduct, evaluation, and improvement planning.
Personnel	List each position by title and name of employee, if available. Show the annual salary rate and the percentage of time to be devoted to the project. Compensation paid for employees engaged in grant activities must be consistent with that paid for similar work within the applicant organization. In the budget narrative, include a description of the responsibilities and duties of each position in relationship to fulfilling the project goals and objectives. Nonprofit organizations and consortia of nonprofit organizations that receive a subaward may use and expend up to 5% of each subaward for M&A purposes associated with that subaward. If the applicant is receiving more than one award, they must be able to separately account for M&A costs for each subaward. M&A costs are for activities directly related to the management and administration of the award, such as financial management and monitoring, submitting required programmatic and financial reports, and establishing and maintaining equipment inventory. All M&A costs must be broken down and identifiable on the Excel Budget Worksheet.
Indirect (Facilities & Administrative [F&A]) Costs	Indirect costs (IDC) mean those costs incurred for a common or joint purpose benefitting more than one cost objective and not readily assignable to the cost objectives specifically benefitted, without effort disproportionate to the results achieved. IDC are allowable as described in 2 C.F.R. Part 200, including 2 C.F.R. § 200.414. Except for recipients who have never received a negotiated indirect cost rate as described in 2 C.F.R. § 200.414(f), **recipients must utilize their approved indirect cost rate agreement with their cognizant federal** agency to charge indirect costs to this award or, recipients without an IDC rate agreement may elect to use the 15 percent de minimis indirect cost rate for any award executed on or after October 1, 2024. All Federal agencies must honor the new de minimis rate after this date unless a different rate is required by law (such as Federal statute or regulation) or otherwise allowed by 2 CFR part 200.
Construction and Renovation	Any applicant considering submitting an application that involves construction and renovation cost must contact OGR prior to submission. All recipients of these funds must request and receive approval before any funds are used for construction or renovation.
Contracted Security	The recipient must be able to sustain this capability in future years without this funding, and a sustainment plan will be part of the closeout package for any award funding this capability. Funding may not be used to purchase equipment for contracted security. Contracted security costs described in the IJ should include the hourly/daily rate, the number of personnel, and anticipated number of hours/days the personnel will work over the course of the period of performance. **Additionally, recipients and subrecipients may not use more than 50% of their award to pay for personnel activities unless a waiver is approved by FEMA.**
Fringe Benefits	Fringe benefits should be based on actual known costs or an approved negotiated rate by a federal agency. If not based on an approved negotiated rate, list the composition of the fringe benefit package. Fringe benefits are for the personnel listed in the budget category (A) and only for the percentage of time devoted to the project. Actual know costs must be

Allowable Budget Cost Categories	Description
	itemized by type and include rate computation. Include a copy of approved rate agreement. All requested information must be included in the budget detail worksheet and budget narrative.
Contractor and Consultants	Consultant Fees: For each consultant enter the name, if known, service to be provided, hourly or daily fee (8-hour day), and estimated time on the project. maximum rate for an 8-hour day (currently $650) requires additional justification and prior approval. All requested information must be included in the budget detail worksheet and budget narrative.
Travel	Travel directly related to the purpose of the grant. In-state travel costs associated with the grant shall include mileage rates not to exceed $0.62 per mile, as well as the actual costs of tolls and parking. Note that no grant funds may be spent for out-of-state conference fees, out-of-state travel or out-of-state lodging without prior written approval from OGR.

Unallowable Costs

Award funds may not be used as matching funds for any other federal awards, lobbying, or intervention in federal regulatory or adjudicatory proceedings. In addition, federal funds may not be used to sue the Federal Government or any other government entity. Examples of unallowable costs include:

- **Hiring of public safety personnel**. Funds may not be used to support sworn public safety officers for the purposes of fulfilling traditional public safety duties or to supplant traditional public safety positions and responsibilities.
- **General-use expenditures**. Expenditures for items such as general-use software (word processing, spreadsheet, graphics, etc.), general-use computers and related equipment (other than for allowable M&A activities, or otherwise associated preparedness functions), general-use vehicles, speed bumps, or licensing fees.
- **Overtime and backfill personnel costs**.
- **Supplanting organizational operating expenses.** Grant funds may not be used to pay for existing organizational costs.
- **Weapons.** Including weapons systems and accessories, ammunition, or weapons-related training.
- Initiatives that fund the development or completion of risk or vulnerability security assessments or Investment Justifications.
- Initiatives that benefit Federal agencies or that enhance Federal property.
- Initiatives that study technology development or proof-of-concept initiatives.
- Initiatives that duplicate capabilities being provided by the Federal government.
- Reimbursement of application activities and security or project expenses incurred prior to receipt of a fully executed contract.
- **Law Enforcement Equipment**. For example, license plate readers/license plate reader software, facial recognition cameras, bulletproof vests, electronic control weapons (i.e., tasers), and the like.
- Knox Boxes (a small wall mounted safe that holds keys for emergency responders).

Prohibitions on Expending Grant or Cooperative Agreement Funds for Certain Telecommunications and Video Surveillance Services or Equipment

Recipients and subrecipients of FEMA funding are subject to the prohibitions described in section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (FY 2019 NDAA), Pub. L. No. 115-232 (2018) and 2 C.F.R. §§ 200.216, 200.327, 200.471, and Appendix II to 2 C.F.R. Part 200.

Beginning August 13, 2020, the statute prohibits FEMA recipients, subrecipients, and their contractors and subcontractors from obligating or expending federal award funds on certain telecommunications and video surveillance products and contracting with certain entities for national security reasons. Guidance is available in *FEMA Policy #405-143-1, Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services* issued May 10, 2022. Additional guidance is available at Contract Provisions Guide: Navigating Appendix II to Part 200 - Contract Provisions for Non-Federal Entity Contracts Under Federal Awards.

For information on restrictions, see the full FEMA FFY 2024 NSGP-NSS NOFO.

Environmental Planning and Historic Preservation Compliance

DHS/FEMA is required to consider the potential impacts to the human and natural environment of projects proposed for DHS/FEMA funding. DHS/FEMA, through its Environmental and Historic Preservation (EHP) Program, engages in a review process to ensure that funded activities comply with various federal laws. A grant subrecipient shall provide any information requested by DHS/FEMA to ensure compliance with applicable EHP requirements. An EHP review will be coordinated through OGR and must be completed **before** any grant-funded purchases may be made.

OGR will work with grant subrecipients on the completion and submission of EHP forms if completion of forms is deemed necessary. The EHP forms are **not** due with the application but must be completed and submitted to OGR by the award subrecipient and approved by FEMA before beginning any grant funded activity.

Other Grant Requirements

During their active contract period, subrecipients will be required to submit quarterly financial and progress reports to OGR. OGR and DHS/FEMA reserve the right to conduct programmatic and financial site visits with subrecipients during and after the contract period.

Sub-grant conditions: Subrecipients will be required to sign the OGR General Subrecipient Grant Conditions. Applicable sections of this document will be reviewed with subrecipients at the beginning of the contract period.

Application/Investment Justification Submission Information

Electronic applications are **due no later than 4:00 pm on Tuesday, December 17, 2024,** and must be submitted via OGR's Online application form.

If you have any issues accessing the online application or submitting the form, please contact Sarah Malloy at sarah.a.malloy@mass.gov.

Late or incomplete applications will not be accepted.

Do not include letters of support with your application. They will not be reviewed or considered.

Application Review Information and Award Announcements
Applications will be reviewed for completeness, adherence to programmatic guidelines, feasibility, and how well the IJ (project description and justification) addresses the identified risk(s). To advance equity in awarding grant funding, OGR will consider an organization's location within a disadvantaged community and how an organization demonstrates they serve a disadvantaged community or population.

Eligible applications will be reviewed and scored by three peer reviewers. Reviewers are responsible for ensuring all stated rules and regulations are adhered to, such as application completeness, answering questions posed, ensuring the application has a homeland security nexus, etc.
The Executive Director of OGR and Public Safety and Security Secretary have final discretion on all recommendations being put forward to FEMA for consideration. FEMA will review all recommendations and inform OGR of award decisions by Spring of 2025.

Nonprofit organizations must fully answer each question in all the sections of their Investment Justification for the form to be considered complete.

I.   **Section I – Applicant Information (2 possible points out of 40)**
    a. Legal Name of the Organization/Physical Address of the Facility/County
    b. Owning vs. Leasing/Renting and Permission to Make Enhancements
    c. Active Operation at the Listed Location (i.e., fully operational at the time of application)
    d. Other Organizations in the Facility
    e. Mission Statement Summary
    f. Organization Type
        1. Applicants are required to self-identify with one of the following categories in the IJ as part of the application process: 1. Ideology-based/Spiritual/Religious (Houses of Worship, Educational Institutions, Medical Facilities, etc.) 2. Educational (secular) 3. Medical (secular) 4. Other
    g. Organization Function
    h. Organization's Affiliation
        1. The nonprofit must apply on their own behalf, NOT on behalf of other entities, including government or for-profit entities.
    i. 501(c)(3) Tax-Exempt Designation
    j. Unique Entity Identifier (UEI) obtained via SAM.gov
        1. Entities are not required to have a UEI at the time of application but must have a valid UEI in order to receive funds.
    k. Funding stream, either:
        1. Designated high-risk urban area (NSGP-NSS-UA) or
        2. Outside the high-risk urban area (NSGP-NSS-S)
    l. List all prior federal or state nonprofit security grant award(s), including program name, year, award amount, and most recent spending status.
    m. Federal Funding Request (total estimated cost of projects/activities)

1. The total amount will auto-populate in the IJ form.

II. Section II – Background (3 possible points out of 40)
   a. 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.
   b. 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.
   c. Describe any heightened threat faced as a result from the Israel-Hamas war.

III. Section III – Risk (15 possible points out of 40)
   a. Threat: Describe the specific threats, incidents, or attacks against the nonprofit organization or a closely related organization. Provide support to substantiate the risk, such as police reports, insurance claims, internet threats, etc. Threats/risks must have a terrorism/other extremism nexus.
   b. 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 must be accurate and based on the Vulnerability Assessment submitted to the SAA. Failure to submit a Vulnerability Assessment will automatically disqualify an application.
   c. 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.

IV. Section IV – Facility Hardening (9 possible points out of 40)
   a. 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. Threats/risks must be linked to existing physical vulnerabilities. Funding requests must relate to the information provided from the Vulnerability Assessment.
   b. Describe how the proposed activities focus on the prevention of and/or protection against the risk/threat of a terrorist or other extremist attack.
   c. Confirm that the proposed projects are allowable in accordance with the priorities of the NSGP-NSS.
   d. Confirm that the proposed projects and milestones are feasible, meaning there is a reasonable expectation that all tasks, projects and/or activities can be completed within the subaward period of performance.
   e. Application may not present any actual or perceived conflict between grant writers/consultants and contractors/vendors sourced for projects.
   f. Contract security/any hiring outside of the nonprofit organization is explicitly written to not be sole sourced.
   g. Nonprofit organizations must always abide by federal and state procurement guidance.

V. Section V – Milestones (5 possible points out of 40)

a. Describe any key activities that will lead to milestones in the program/project and grants management over the course of the grant award period of performance.

b. NOTE: Activities involving modifications to a building or site will likely require EHP review. If such projects are proposed, EHP review should be one of the first milestones listed. For more information about the NSGP's EHP process, see [FEMA Policy: Grant Programs Directorate Environmental Planning and Historic Preservation](#).

VI. Section VI – Project Management (2 possible points out of 40)

a. Describe the proposed management team's roles, responsibilities, and governance structure to support the implementation of the projects/activities.

b. Assess the project management plan/approach.

VII. Section VII – Impact (4 possible points out of 40)

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

VIII. Section VIII – Budget Worksheet

a. For each cost category that has an associated funding request in the Budget Excel Worksheet (Attachment B), please provide an overall description and justification. The budget detail should describe the budget items, why the items in that category are needed, and how the budgeted amount was determined.

IX. Overall Verification: Prior to Submission

a. Application package is complete. OGR will reject incomplete application packages.

b. All proposed projects/activities are allowable per this AGF.

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

d. FEMA-provided IJ form is submitted and signed by the nonprofit organization's point of contact, *not by an external party or contractor (e.g., contracted grant writer or grant manager).*

e. IJ is unique to the nonprofit organization, physical location/site/address, and vulnerabilities listed.

Application Assistance

General questions on the application process may be sent in writing to sarah.a.malloy@mass.gov. As this is a competitive grant process, questions on specific review processes, etc., will not be answered. These questions and corresponding answers will be posted as available on OGR's website.

OGR will offer a webinar about this funding opportunity to review changes/highlights, eligibility, allowable costs, an overview of the Investment Justification as well as Q&A session. Please [register here](#) for Federal Fiscal Year 2024 Nonprofit Security Grant Program – National Security Supplemental Application Assistance Webinar on **December 9, 2024, at 11:00 AM EDT**. After registering, you will receive a confirmation email containing information about joining the webinar.

Equipment Appendix

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

Additionally, subrecipients that are using these funds to support emergency communications equipment activities must comply with the SAFECOM Guidance including provisions on technical standards that ensure and enhance interoperable communications This SAFECOM Guidance can be found at the Funding and Sustainment page on CISA.gov Funding Resources