Commonwealth of Massachusetts
Executive Office of Public Safety and Security
Office of Grants and Research

Federal Fiscal Year 2026
Nonprofit Security Grant Program
Availability of Grant Funds

Maura T. Healey
Governor

Kimberley Driscoll
Lieutenant Governor

Gina K. Kwon
Secretary

Kevin J. Stanton
Executive Director

Federal Fiscal Year 2026
Notice of Availability of Grant Funds
Office of Grants and Research

Deadline: July 10, 2026

Introduction

The Massachusetts **Office of Grants and Research** (OGR) is the State Administering Agency (SAA) for federal funds received from the Department of Homeland Security (DHS) Federal Emergency Management Agency (FEMA), Department of Justice, and the National Highway Traffic Safety Administration. OGR manages more than $300 million in state and federal grants that are distributed to state, municipal, education, nonprofit, and tribal agencies across the Commonwealth.

Overview of Funding Opportunity

FFY2026 Nonprofit Security Grant Program (NSGP) is made available from the DHS/FEMA (Funding Opportunity Number: **DHS-26-GPD-067-00-98** and Assistance Listing Number: **97.008**). NSGP funds are intended to improve the physical/cybersecurity and facility/target hardening of nonprofit organizations 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.

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.

This opportunity is composed of two funding streams based on the location of an applicant:

- **The Nonprofit Security Grant Program - Urban Area (NSGP-UA)** is a competitive opportunity that will fund nonprofits located in a federally designated high-risk Metro Boston urban area. In Massachusetts, the Urban Area Security Initiative (UASI) Metro Boston area includes **Boston, Brookline, Cambridge, Chelsea, Everett, Quincy, Revere, Somerville, and Winthrop**. Massachusetts has received an allocation of **$399,755.00** to support nonprofits located within these nine cities.

- **The Nonprofit Security Grant Program - State (NSGP-S)** is a competitive opportunity that will fund nonprofits located outside the UASI-designated high-risk urban area. Massachusetts has received an allocation of **$3,420,000.00** to support nonprofits located in the other 342 Massachusetts cities and towns not designated as UASI.

All applications must be submitted to OGR for consideration of funding. As the SAA for these funds, OGR is the only entity in Massachusetts that may submit **FFY2026 NSGP** applications directly to DHS/FEMA. Any otherwise eligible application may be deemed ineligible if submitted by a person or entity other than OGR. Final award decisions will be made by DHS/FEMA.

Maximum Funding Request for NSGP-UA: Up to $200,000/applicant per site
Maximum Funding Request for NSGP-S: Up to $200,000/applicant per site

Key Dates

Date	Task
June 26, 2026	OGR release of Notice of Funding Opportunity for NSGP
July 10, 2026, 4:00pm	**Application Submission Deadline**
October 2026	Tentative Award Notification
Contract start date – August 31, 2028	Performance Period Start Date – Performance Period End Date

OGR recognizes that the July 10 deadline offers a brief application period. This timeline is necessitated by the deadline by which OGR must submit all applications to FEMA for review.

Project Period of Performance
The project period of performance will end no later than **August 31, 2028**. Please adhere to this timeframe in the Investment Justification's Milestones section.

Eligible Applicants
Only nonprofit organizations at risk of a terrorist or other extremist attack are eligible to apply for this funding opportunity. Examples of eligible applicant organizations can include houses of worship, museums, educational facilities, senior centers, community centers, and day camps, among many others.

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 or network/cell made against the applicant or closely related organizations (e.g. police reports or insurance claims).
- Symbolic value of the site 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.

Guidance for Applicants of the FFY25 NSGP
FEMA intends to notify OGR later this summer of which nonprofits will receive FFY25 NSGP funding. OGR expects to receive that notification after the FFY26 NSGP deadline of July 10, 2026. FFY25 applicants have two options when applying for the FFY26 NSGP:

1. Submit an application for the same projects included in the FFY25 application. If approved for funding, the nonprofit will only be eligible to receive funds through either the FFY25 program or the FFY26 program, but not both.
2. Request funds for a different project. Applicants that choose to request funds for a different project should not include any of the elements requested in their FFY25 application.

Unique Entity Identifier (UEI) and System for Awards Management (SAM)
Entities are not required to have a UEI at the time they submit an application for this opportunity, but they must have a valid UEI in order to receive funds. Applicants who do not currently have a UEI number should begin the SAM.gov registration process at the earliest opportunity. Additional information on UEI registration, please refer to GSA.gov's Unique Entity Identifier Update.

Application Requirements

1. **Investment Justification (IJ)**

To apply for FFY2026 NSGP funds, applicants must submit an Investment Justification (IJ) form **utilizing the FFY 2026 NSGP IJ Template** developed by FEMA. Application materials, including the IJ, are available on OGR's **NSGP program page.**

Nonprofit organizations with one site may apply for up to $200,000 for that site. Nonprofit organizations with multiple sites may apply for up to $200,000 per site, for up to three sites per funding stream (NSGP- UA or NSGP-S) for a maximum of $600,000. If a nonprofit organization applies for multiple sites, it must submit one completed IJ for each site through a separate application submission. Each IJ/application 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. The IJ must demonstrate the ability to provide enhancements consistent with the purpose of the NSGP program and guidance provided by DHS/FEMA. NSGP 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 **August 31, 2028**.

IJ Section I – Applicant Information

- Legal Name of the Organization/Physical Address of the Facility/County
- Owning vs. Leasing/Renting and Permission to Make Enhancements
- Active Operation at the Listed Location (i.e., fully operational at the time of application)
- Other Organizations in the Facility
- Mission Statement Summary
- 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
- Organization Function
- Organization's Affiliation
    1. The nonprofit must apply on their own behalf, NOT on behalf of other entities, including government or for-profit entities
- 501(c)(3) Tax-Exempt Designation
- Unique Entity Identifier (UEI) obtained via SAM.gov
    1. Entities are not required to have a UEI at the time the application is submitted, but they must have a valid UEI in order to receive funds
- Funding stream, either:
    1. Designated high-risk urban area (NSGP-UA) or
    2. Outside the high-risk urban area (NSGP -S)
- List all prior federal or state nonprofit security grant award(s), including program name, year, award amount, and most recent spending status
- Federal Funding Request (total estimated cost of projects/activities)
    1. The total amount will auto-populate in the IJ form

IJ Section II – Background (5 possible points out of 40)

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

IJ Section III – Risk (15 possible points out of 40)

- 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.
- 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.
- 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.

IJ Section IV – Facility Hardening (9 possible points out of 40)

- 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 derived from the Vulnerability Assessment.
- Describe how the proposed activities focus on the prevention of and/or protection against a terrorist or other extremist attack.
- Confirm that the proposed projects are allowable and in accordance with the priorities of the NSGP.
- 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.
- Contract security or any hiring outside of the nonprofit organization cannot be sole sourced.
- Nonprofit organizations must always abide by federal and state procurement guidance.

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

- 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.
- NOTE: Activities involving modifications to a building or site will likely require Environmental and Historic Preservation (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.

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

- 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.

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

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

2. Budget Worksheet

Each applicant must include a completed 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). For each cost category that has an associated funding request in the Budget Excel Worksheet, 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.

3. OGR Risk Assessment Form

Federal regulations included in 2 CFR §200.331 require OGR to evaluate each subrecipient's risk of noncompliance with Federal statutes, regulations, and the terms and conditions of the subaward for purposes of determining the appropriate subrecipient monitoring. NSGP applicants must complete this form and submit it with the application.

4. Vulnerability Assessment

In order to be eligible for this grant funding, each applicant must submit with its application a Vulnerability Assessment **unique to the site** for which the IJ is being submitted. The Vulnerability Assessment must be submitted as a separate attachment in a PDF or Word format. Failure to submit a Vulnerability Assessment will **automatically disqualify** an application.

5. Mission Statement

Each applicant must include its Mission Statement (on the organization's letterhead) 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.

Allowable Costs

Funds must be spent in compliance with applicable rules and regulations noted in the FFY 2026 NSGP NOFO.

1. 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 from CISA and related Cybersecurity and Infrastructure Security Agency (CISA) resources. Examples of planning activities allowable under this program include:

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

Please be advised that planning costs incurred before grant awards are made cannot be paid with this grant. Any related planning costs incurred must be after the award is made and fully executed.

2. Equipment

Funding may be used for the acquisition and installation of security equipment on real property owned or leased by the nonprofit organization, specifically in prevention of and/or protection against the risk of a terrorist or other extremist attack. Equipment is limited to select items on the Authorized Equipment List (AEL):

- 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, recipients that are using NSGP funds to support emergency communications equipment activities must comply with the SAFECOM Guidance on Emergency Communications Grants, including provisions on technical standards that ensure and enhance interoperable communications.

3. **Maintenance and Sustainment**
   Funding may be used for maintenance contracts, warranties, repair or replacement costs, upgrades, and user fees as described in DHS/FEMA Policy FP 205-402-125-1.

4. **Training/Exercises**
   Nonprofit organization security personnel may use NSGP funds to attend security-related training courses, exercises, and programs in the United States. Allowable training-related costs under NSGP are limited to attendance fees for the training and related expenses, such as materials, supplies, and/or equipment. Overtime, backfill, and/or travel expenses are **not** allowable costs. Allowable training topics are limited to the protection of Critical Infrastructure/Key Resources (CI/KR), including physical and cyber security, target hardening, and terrorism awareness/employee preparedness programs such as Community Emergency Response Team (CERT) training, Active Shooter training, and emergency first aid.

   Training conducted using NSGP funds must address a specific threat, vulnerability, and/or consequence as identified in the nonprofit's IJ. Proposed attendance at training courses or exercises and all associated costs leveraging the FFY2026 NSGP must be included in the nonprofit organization's 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.

5. **Management and Administration (M&A)**
   Nonprofit organizations that receive an award under this program may use and expend up to 5% of their FFY2026 NSGP funds for M&A purposes. M&A refers to the cost of 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.

6. **Indirect (Facilities & Administrative [F&A]) Costs**
   Indirect costs are allowable under this program as described in 2 C.F.R. § 200.414. With the exception of recipients who have never received a negotiated indirect cost rate as described in 2 C.F.R. § 200.414(f), recipients must have an approved indirect cost rate agreement with their cognizant federal agency to charge indirect costs to this award.

7. **Construction and Renovation**
   Any applicant considering submitting an application that involves construction and renovation costs must contact OGR prior to submission. All recipients of NSGP funds must request and receive approval from DHS/FEMA before any funds are used for construction or renovation.

8. **Contracted Security**
   The recipient must be able to sustain this capability in future years without NSGP funding, and a sustainment plan will be part of the closeout package for any award funding contracted security. NSGP

funds 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.

Unallowable Costs:
Examples of unallowable costs include:

- Organizational operating expenses.
- Hiring of public safety personnel. NSGP 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, or licensing fees.
- Overtime and backfill.
- Weapons, weapons systems and accessories, ammunition, or weapons-related training.
- Initiatives that do not address the implementation of programs/initiatives to build prevention and protection-focused capabilities directed at identified facilities and/or the surrounding communities.
- The development of risk/vulnerability assessment models.
- Initiatives that fund risk or vulnerability security assessments or the development of the Investment Justification.
- Initiatives in which Federal agencies are the beneficiary or that enhance Federal property.
- Initiatives that study technology development.
- Proof-of-concept initiatives.
- Initiatives that duplicate capabilities being provided by the Federal government.
- Reimbursement of pre-award security expenses.
- Law enforcement related equipment such as cameras for facial recognition, license plate readers/license plate reader software, unmanned aerial vehicles such as drones and the like.
- Knox Boxes.

Prohibitions on Expending Grant or Cooperative Agreement Funds for Certain Telecommunications and Video Surveillance Services or Equipment
Recipients and subrecipients of FEMA federal financial assistance are subject to the prohibitions described in section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (FY 2019 NDAA), Pub. L. No. 115-232 (2018) and 2 C.F.R. §§ 200.216, 200.327, 200.471, and Appendix II to 2 C.F.R. Part 200. Beginning August 13, 2020, the statute – as it applies to FEMA recipients, subrecipients, and their contractors and subcontractors – prohibits obligating or expending federal award funds on certain telecommunications and video surveillance products and contracting with certain entities for national security reasons. 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.

Effective August 13, 2020, FEMA recipients and subrecipients **may not** use any FEMA funds under open or new awards to:
(1) Procure or obtain any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology of any system;
(2) Enter into, extend, or renew a contract to procure or obtain any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology of any system; or

(3) Enter into, extend, or renew contracts with entities that use covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system.

Definitions
Per section 889(f)(2)-(3) of the FY 2019 NDAA and 2 C.F.R. § 200.216, covered telecommunications equipment or services means:
i. Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation, (or any subsidiary or affiliate of such entities);
ii. For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);
iii. Telecommunications or video surveillance services provided by such entities or using such equipment; or
iv. Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the People's Republic of China.

Examples of the types of products covered by this prohibition include phones, internet, video surveillance, and cloud servers when produced, provided, or used by the entities listed in the definition of "covered telecommunications equipment or services." See 2 C.F.R. § 200.471.

For information on other restrictions, see the full FEMA FFY2026 NSGP 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 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, approved by FEMA **before** any grant-funded purchases/equipment installations may be made.

OGR will work with those awarded grants on the completion and submission of EHP forms (if completion of forms is deemed necessary). These forms are **not** due with the application.

Other Grant Requirements
During their active contract period, subrecipients of FFY2026 NSGP funding 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.

Subgrant conditions: Subrecipients will be required to sign OGR General Subrecipient Grant Conditions. Key applicable elements of this document will be reviewed with recipients at the beginning of contract activity.

DHS Standard Terms and Conditions: Subrecipients will also be required to comply with all relevant DHS Standard Terms and Conditions.

Application Submission
Electronic applications are due no later than **4:00 pm on Friday, July 10, 2026,** and must be submitted via the **FFY26 NSGP Online Application**

Late applications will not be accepted.

Application documents must use the following file naming convention:

- **For NSGP-UA:** Investment Justifications: FY2026_NSGP_UA <MA> <Metro Boston> <Nonprofit Name>
- **For NSGP-S:** Investment Justifications: FY2026_NSGP_S <MA> <Nonprofit Name>

The application **must** include the following attachments:

- completed IJ
- completed Budget Worksheet (submitted as an Excel document),
- organization's mission statement,
- vulnerability assessment,
- OGR risk assessment,
- indirect cost rate agreement (if applicable).

With the exception of the Budget Worksheet, each of these documents must be submitted in Word or PDF format. The Budget Worksheet must be submitted as an Excel document.

Verify Prior to Submission:

- Application package is complete. OGR will not recommend funding for incomplete application packages.
- All proposed projects/activities are allowable per this AGF.
- IJ's content and project goals are logical and reasonable.
- 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).
- IJ is unique to the nonprofit organization, physical location/site/address, and vulnerabilities listed.

Application Assistance

Written questions on general application process matters may be sent to brian.p.nichols@mass.gov. As this is a competitive grant process, questions specific to the merits of a proposal, etc., will not be answered.

Application Review Information

The following are the FFY2026 NSGP-S and NSGP-UA evaluation process and criteria:

- For NSGP-UA, state and federal verification that the nonprofit organization is located within one of the FFY2026 designated high-risk urban areas; for NSPG-S, verification that the nonprofit is located outside of one of the FFY2026 designated high-risk urban areas;
- Identification and substantiation of current or persistent threats or attacks (from within or outside the United States) by a terrorist or other extremist organization, network, or cell against the applicant based on the applicant's ideology, beliefs, and/or mission as: 1) an ideology-based/spiritual/religious; 2) educational; 3) medical; or 4) other nonprofit entity;
- Symbolic value of the site as a highly recognized regional and/or national or historical institution(s) that renders the site a possible target of terrorist or other extremist attack;
- Role of the nonprofit organization in responding to or recovering from terrorist or other extremist attacks;
- Alignment between the project activities with the physical or cyber vulnerabilities identified in the organization's Vulnerability Assessment;
- Integration of nonprofit preparedness with broader state and local preparedness efforts;
- Completed IJ for each site that addresses an identified risk unique to that site, including the assessed threat, vulnerability, and consequence of the risk; and

- History of prior funding under NSGP.

With the assistance of peer reviewers, OGR will review and score all applications received by the above deadline and then submit eligible applications to DHS/FEMA for validation. DHS/FEMA will inform OGR of any awards. Upon receipt of this information, OGR will notify all applicants.