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

Federal Fiscal Year 2023
Nonprofit Security Grant Program
Application Instructions

REVISED ON 3/21/23

Maura T. Healey
Governor

Kimberley Driscoll
Lieutenant Governor

Terrence M. Reidy
Secretary

Kevin J. Stanton
Executive Director

Federal Fiscal Year 2023
Notice of Funding Opportunity
Office of Grants and Research

March 15, 2023

Overview
The U.S. Department of Homeland Security's (DHS) Federal Fiscal Year (FFY) 2023 Nonprofit Security Grant Program (NSGP) provides funding support for target hardening and other physical security enhancements to nonprofit organizations that are at high-risk of terrorist attack.

In Fiscal Year (FY) 2023, the **Nonprofit Security Grant Program - Urban Area** (NSGP-UA) will be a competitive grant program that funds nonprofits located in UASI-designated urban areas. *In Massachusetts, the UASI Metro Boston area is Boston, Brookline, Cambridge, Chelsea, Everett, Quincy, Revere, Somerville, and Winthrop.* Under the **Nonprofit Security Grant Program - State** (NSGP-S), each state will receive an allocation for nonprofit organizations located outside of the Urban Area Security Initiative (UASI)-designated urban areas.

As the **State Administrative Agency (SAA)**, the Massachusetts Executive Office of Public Safety and Security's **Office of Grants and Research (OGR)** is the **ONLY** entity in Massachusetts that may submit FFY 2023 NSGP applications (also referred to as Investment Justifications or IJ) directly to the Department of Homeland Security (DHS)/Federal Emergency Management Agency (FEMA). All applications from eligible nonprofits for FFY 2023 NSGP funding must be submitted to OGR. Final award decisions will be made by DHS/FEMA.

Maximum Funding Request for MA Applicants	
Maximum Funding Request for NSGP-UA	**Up to $150,000/applicant**
Maximum Funding Request for NSGP-S	**Up to $150,000/applicant**

Project Period of Performance
The project period of performance will end no later than **December 31, 2025**. Please adhere to this timeframe in the Investment Justification's Milestones section.

Nonprofit Security Grant Program (NSGP) Key Dates:

DATE	**TASK**
March 15, 2023	OGR release of Notice of Funding Opportunity for NSGP
March 22, 2023 at 2pm	Application Assistance Webinar Register below: https://attendee.gotowebinar.com/register/690575095746559833
April 14, 2023	**Deadline to submit Application (IJ), Signature Page, Vulnerability Assessment, Mission Statement, and OGR Risk Assessment by 4:00 p.m.**
Award Notification	**September 2023**
Performance Period	**November 2023-December 2025**

Eligible Applicants:
Nonprofit organizations (as described under section 501(c) (3) of the Internal Revenue Code of 1986) at high-risk of terrorist attacks.

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

- Identification and substantiation (e.g. police reports or insurance claims) of prior threats or attacks (from within

or outside the U.S.) by a terrorist organization, network, or cell against the applicant or closely related organizations;
- Symbolic value of the site(s) as a highly recognized national or historical institution that renders the site as a possible target of terrorism;
- Role of the applicant in responding to or recovering from terrorist attacks;
- Findings from previously conducted risk assessments including threat or vulnerability.

An application submitted by an otherwise eligible non-federal entity (which for this program is the SAA) may be deemed ineligible when the person that submitted the application (for the applicant/SAA) is not: 1) a ***current employee, personnel, official, staff, or leadership*** of the non-federal entity; and 2) ***duly authorized to apply*** for an award on behalf of the non-federal entity at the time of application. Further, the Authorized Organization Representative (AOR) must be a duly authorized current employee, personnel, official, staff or leadership of the recipient and ***provide an email address unique to the recipient (SAA) at the time of application and upon any change in assignment during the period of performance. Consultants or contractors of the recipient are not permitted to be the AOR of the recipient.***

Unique Entity Identifier

Effective April 4, 2022, the Federal Government transitioned from using the Data Universal Numbering System or DUNS number, to a new, non-proprietary identifier known as a Unique Entity Identifier or 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.
UEI registration information is available on GSA.gov at https://www.gsa.gov/about-us/organization/federal-acquisition-service/office-of-systems-management/integrated-award-environment-iae/iae-systems-information-kit/unique-entity-identifier-update.

Application Requirements:

1. **Investment Justification (IJ)**
   To apply for FFY2023 NSGP funds, applicants must submit an Investment Justification (IJ) **utilizing the FFY 2023 NSGP IJ Template** available at https://www.mass.gov/how-to/apply-for-a-nonprofit-security-grant.

   Only one IJ is permitted per site, for no more than 3 sites in either NSGP-UA or NSGP-S for a **maximum of $150,000** per location. The site must have a physical address (not a PO Box #) to be considered eligible. The nonprofit must occupy the location at the time of application.

   Each applicant must develop an IJ that addresses the investments it will make with the proposed funding. The IJ must address an identified risk, including threat and vulnerability, and build or sustain a core capability identified in the National Preparedness Goal. 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 **December 31, 2025**.

   Applicants must ensure that their IJ is consistent with all applicable requirements outlined in the FFY 2023 NSGP Notice of Funding Opportunity (NOFO) available at https://www.mass.gov/how-to/apply-for-a-nonprofit-security-grant as well as support the National Preparedness Goal available at https://www.fema.gov/emergency-managers/national-preparedness/goal

2. **Budget Worksheet**
   Each applicant must include with its application this budget summary and detail of allowable costs available at https://www.mass.gov/how-to/apply-for-a-nonprofit-security-grant

3. **Applicant Signature Page**
   Each applicant must include with its application the Signature Page signed by the nonprofit organization's authorized representative and emailed to the NSGP program coordinator.

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.

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, the SAA will use the Mission Statement along with information provided in the applicant's IJ to validate the organization type. The central purpose of the organization described in the Mission Statement will be used to validate the organization's type identified in the IJ as either 1) Ideology-based/Spiritual/Religious, 2) Educational, 3) Medica,; or 4) Other. The organization type is a factor when calculating the final score of the application.

6. **Sub-grantee Risk Assessment Form**
   Federal regulations included in 2 CFR §200.331 require OGR to evaluate each sub-recipient's risk of noncompliance with Federal statutes, regulations, and the terms and conditions of the sub- award for purposes of determining the appropriate sub-recipient monitoring. NSGP applicants must complete this form and submit it with the application. The form may be downloaded from https://www.mass.gov/how-to/apply-for-a-nonprofit-security-grant.

7. **Applicant Information Form**
   This form is not due with the application, it is an online form that is filled out with your organization's contact information that generates a spreadsheet for the program coordinator. The form is available from https://www.mass.gov/how-to/apply-for-a-nonprofit-security-grant

Allowable Costs
Funds must be spent in compliance with applicable rules and regulations noted in the FFY 2023 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.

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 to prevent or protect against a terrorist attack. Equipment is limited to select items on the Authorized Equipment List (AEL):

   - 03OE-03-MEGASystem, Public Address, Handheld or Mobile
   - 04AP-05-CREDSystem, Credentialing
   - 04AP-09-ALRTSystems, Public Notification and Warning
   - 04AP-11-SAASApplications, Software as a Service

- 05AU-00-TOKNSystem, Remote Authentication
- 05EN-00-ECRPSoftware, Encryption
- 05HS-00-MALWSoftware, Malware/Anti-Virus Protection
- 05HS-00-PFWLSystem, Personal Firewall
- 05NP-00-FWALFirewall, Network
- 05NP-00-IDPSSystem, Intrusion Detection/Prevention
- 06CP-01-PORTRadio, Portable
- 06CC-02-PAGEServices/Systems, Paging
- 06CP-03-ICOMIntercom
- 06CP-03-PRACAccessories, Portable Radio
- 10GE-00-GENRGenerators
- 13IT-00-ALRTSystem, Alert/Notification
- 14CI-00-COOPSystem, Information Technology Contingency Operations
- 14EX-00-BCANReceptacles, Trash, Blast-Resistant
- 14EX-00-BSIRSystems, Building, Blast/Shock/Impact Resistant
- 14SW-01-ALRMSystems/Sensors, Alarm
- 14SW-01-DOORDoors and Gates, Impact Resistant
- 14SW-01-LITELighting, Area, Fixed
- 14SW-01-PACSSystem, Physical Access Control
- 14SW-01-SIDPSystems, Personnel Identification
- 14SW-01-SIDV Systems, Vehicle Identification
- 14SW-01-SNSRSensors/Alarms, System and Infrastructure Monitoring, Standalone
- 14SW-01-VIDASystems, Video Assessment, Security
- 14SW-01-WALLBarriers: Fences; Jersey Walls
- 15SC-00-PPSSSystems, Personnel/Package Screening
- 21GN-00-INSTInstallation
- 21GN-00-TRNGTraining 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 Investment Justification. Proposed attendance at training courses and all associated

costs leveraging the FFY 2023 NSGP must be included in the nonprofit organization's Investment Justification. Proposed attendance at training/exercises and all associated costs using NSGP must be 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. For additional information on HSEEP refer to https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep.

5. **Nonprofit Management and Administration (M&A)**
   Nonprofit organizations that receive an award under this program may use and expend up to five percent (5%) of their FFY 2023 NSGP funds for M&A purposes. 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, 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 cost 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 this capability. 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.

   Additionally, NSGP recipients and subrecipients may not use more than 50% of their award to pay for personnel activities unless a waiver is approved by FEMA.

Unallowable Costs:
Examples of unallowable costs are listed below:

- 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, 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.
- Organizational operating expenses.
- Reimbursement of pre-award security expenses.
- Cameras for license plate readers/license plate reader software.
- Cameras for facial recognition.
- 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.

See full FFY 2023 NSGP NOFO for other restrictions at https://www.fema.gov/grants/preparedness/nonprofit-security#nofos.

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 **before** any grant-funded purchases 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
Subrecipients of FFY 2023 NSGP funding will be required, during their active contract periods, 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 also be required to sign OGR General Subrecipient Grant Conditions. Key applicable elements of this document will be reviewed with sub-recipients at the beginning of contract activity.

Application/Investment Justification Submission Information
Electronic applications are **due no later than 4:00 pm on April 14th, 2023** and must be submitted to brian.p.nichols@mass.gov with the subject line:

- FY 2023 UASI NSGP_UA <Nonprofit Name>."
- FY 2023 STATE NSGP_S <Nonprofit Name>."

Late applications will not be accepted.
Application documents must use the following file naming convention:

- **For NSGP-UA:** Investment Justifications: FY2023_NSGP_UA <MA> <Metro Boston> <Nonprofit Name>
- **For NSGP-S:** Investment Justifications: FY2023_NSGP_S <MA> <Nonprofit Name>

An application must be in the form of the FFY 2023 NSGP Investment Justification Template, available at https://www.mass.gov/how-to/apply-for-a-nonprofit-security-grant.

The application **must** be accompanied by a copy of the organization's mission statement, vulnerability assessment, OGR risk assessment, applicant signature page, and an indirect cost rate agreement (if applicable). These documents must be submitted in Word or PDF format.

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

Application Review Information and Award Announcements
FFY 2023 NSGP applications will be reviewed through a two-phase state and federal review process for completeness, adherence to programmatic guidelines, feasibility, and how well the IJ (project description and justification) addresses the identified risk(s). For FFY 2023 NSGP-S, the state will make recommendations to DHS/FEMA based on their target allocation of $3,600,000. Priority will be given to nonprofit organizations that have not received prior NSGP funding.

With the assistance of outside reviewers, OGR will review all applications received by the above deadline and then submit eligible applications to DHS/FEMA for final review and award decisions. DHS/FEMA will inform OGR of any awards by late summer 2023**.** Upon receipt of this information, OGR will notify all applicants. DHS/FEMA will award OGR any NSGP funding by **October 2023**. OGR will aim to enter into contracts with successful applicants by **November 2023,** contingent upon awardees providing all necessary, signed contract documentation back to OGR in a timely manner.

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 on specific review processes, etc., will not be answered. The deadline for questions is **April 7,**

2023. These questions and corresponding answers will be posted as available at https://www.mass.gov/how-to/apply-for-a-nonprofit-security-grant.

OGR is pleased to announce a webinar for the FFY 2023 NSGP to review changes/highlights, eligibility, allowable costs, an overview of the Investment Justification and a Q&A session on **Wednesday, March 22, 2023, at 2pm**. See registration below:
Please register for the FFY 2023 Nonprofit Security Grant Program Applicant Information Session on Wednesday, March 22, 2023, at 2:00pm

https://attendee.gotowebinar.com/register/6905750957465598 33

After registering you will receive a confirmation email containing information about joining the webinar.