Nonprofit Security Grant Program

Notice of Funding Opportunity (NOFO) Summary

Delaware Emergency Management Agency

FY2023

This Program Guide summarizes pertinent information from the FY2023 Nonprofit Security Grant Program, Notice of Funding Opportunity and includes Delaware specific application information, such as the Delaware application deadline.

Interested nonprofit organizations should still review the Notice of Funding Opportunity and Preparedness Grants Manual, Appendix C for additional information regarding the FY2023 NSGP.

Program Overview and Objectives

The Nonprofit Security Grant Program (NSGP) is a competitive grant program appropriated annually through DHS and administered by FEMA. It is intended to provide federal funding support for physical and cyber security enhancements and other security-related activities to nonprofit organizations that are at high risk of a terrorist attack. The NSGP also seeks to integrate the preparedness activities of nonprofit organizations with broader state and local preparedness activities.

For FY23, DHS is focused on the importance of information sharing and collaboration to building a national culture of preparedness and protecting against terrorism and other threats to our national security.

2022-2026 FEMA Strategic Plan: The 2022-2026 FEMA Strategic Plan outlines three bold, ambitious goals in order to position FEMA to address the increasing range and complexity of disasters, support the diversity of communities we serve, and complement the nation's growing expectations of the emergency management community. The NSGP supports FEMA's efforts to instill equity as a foundation of emergency management, as well as promote and sustain a ready FEMA and prepared nation. The NSGP program supports the goals of Building a Culture of Preparedness and Readying the Nation for Catastrophic Disasters.

Eligibility

Eligible nonprofit organizations:

- Are described under section 501(c)(3) of the Internal Revenue Code of 1986 (IRC) and exempt from tax under section 501(a) of such code; and
- Demonstrate, through the application, that the organization is at high risk of a terrorist attack.

FEMA requires applicants to obtain a Unique Entity Identifier (UEI) and register in the System for Award Management (SAM.gov).

Each applicant, unless they have a valid exception under 2 CFR 25.110, must:

1) Be registered in SAM.gov before application submission;
2) Provide a valid Unique Entity Identifier (UEI) in its application; and
3) Continue to always maintain an active System for Award Management (SAM) registration with current information during the Federal Award process.

For entities that have an active registration in the SAM.gov, 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 as part of the SAM.gov registration process.

Application Materials and Process

Interested nonprofit organizations must apply through their State Administrative Agency (SAA), who then applies to FEMA on behalf of eligible nonprofit organizations. For Delaware, the Delaware Emergency Management Agency (DEMA) is designated as the SAA.

All application materials must be submitted to Mark Dworkin of DEMA at PreparednessGrants@delaware.gov by 5pm on Monday, April 21, 2023.

For NSGP, nonprofit organizations with one site may apply for up to $150,000 for that site. Nonprofit organizations with multiple sites may apply for up to $150,000 per site for up to three sites, for a maximum of $450,000 per nonprofit. **The maximum award is $150,000.00 per project application.**

If a nonprofit organization applies for projects at multiple sites, regardless of whether the projects are similar in nature, they **must** submit a separate Investment Justification (IJ) and vulnerability assessment **unique to each site**. Failure to do so may be cause for rejection of the application.

Each eligible nonprofit organization must submit the following application materials to their SAA:

1. **Mission Statement**
   - Mission Statement or any mission statement policies or practices that may elevate the organization's risk. A Mission Statement is a formal summary of the aims and values of an organization . It is highly recommended that the Mission Statement is documented on official letterhead.
2. **Vulnerability Assessment**
   - A vulnerability assessment **unique to the site** that addresses the threats, vulnerabilities, and consequences of potential events at the specific location/facility for which the nonprofit organization is applying.
3. **A completed NSGP Investment Justification (IJ)**
   - As part of the NSGP application, eligible 501(c)(3) organizations must develop a formal IJ that addresses each initiative proposed for funding. The IJ should be consistent with the findings of the vulnerability assessment, addresses the proposed projects that are intended to address/mitigate the identified risks and vulnerabilities, and establishes the project timeline, milestones, and key individuals that will be involved in implementing and administering the award.

Completing a vulnerability risk assessment and registering for a Unique Entity ID can take time. It is recommended to begin that part of the application processes as early as possible.

Applications will be reviewed through a two-phase, State and Federal review process for completeness, adherence to programmatic guidelines, feasibility, and IJ relevance to identified risk(s). The SAA will conduct an eligibility review, prioritize the projects, and submit applications to the Department of Homeland Security/Federal Emergency Management Agency (DHS/FEMA) Headquarters' Program Analysts to review the recommendations by the SAA to ensure they are allowable.

Ranking Considerations: DEMA will rank projects based on need and impacts.

- **Need:** The relative need for the nonprofit organization compared to the other applicants; and
- **Impact:** The feasibility of the proposed project and how effectively the proposed project addresses the identified need.

Funding Guidelines and Restrictions

All costs charged to awards covered by this funding notice must comply with the Uniform Administrative Requirements, Cost Principles, and Audit Requirements at 2 C.F.R. Part 200, unless otherwise indicated in the funding notice, the terms and conditions of the award, or the Preparedness Grants Manual. This includes, among other requirements, that costs must be incurred, and products and services must be delivered, within the period of performance of the award. See 2 C.F.R. § 200.403(h) (referring to budget periods, which for FEMA awards under this program is the same as the period of performance). Any costs or project work obligated, initiated, or incurred outside of the period of performance will be ineligible for reimbursement.

Allowable costs are focused on target hardening and physical and cyber security enhancements and other security-related activities. Funding can be used for the acquisition and installation of security equipment on real property (including buildings and improvements) owned or leased by the nonprofit organization, specifically in prevention of and/or protection against the risk of a terrorist attack. This equipment is limited to select items on FEMA's Authorized Equipment List, located at http://www.fema.gov/authorized-equipment-list.

The Authorized Equipment List (AEL) is a list of approved equipment types allowed under FEMA's preparedness grants programs. Approved AEL equipment types allowable for NSGP are listed starting on page C-3 in the NSGP Appendix of the Preparedness Grant Manual.

Federal funds made available through this award may be used for the purpose set forth in the NOFO, the Preparedness Grants Manual, and the terms and conditions of the award and must be consistent with the statutory authority for the award. Approved allowable costs are outlined in the NOFO, Section D, subsection 13: *Funding Restrictions and Allowable Costs* starting on page 21 and in the Preparedness Grants Manual in the NSGP Appendix starting on page C-1. Unallowable costs ineligible for award consideration can be found in the Preparedness Grants Manual on page C-7.

Reference both the NOFO and Preparedness Grants Manual, NSGP Appendix to ensure project costs are approved and allowable expenses under this grant program.

There is no cost share requirement for the FY 2023 NSGP. Applicants that propose a cost share will not receive additional consideration in the scoring. Additionally, NSGP is a pass-through reimbursement grant program. Federal funds will be subgranted through DEMA to those nonprofits/projects that are awarded funding. Nonprofits will incur project costs within the period of performance and submit documentation to DEMA for reimbursement of those allowable expenses.

Key Dates

- Federal Grant Release: **February 27, 2023**
- DEMA Informational Webinar: **March 17, 2023 at 10:00 AM**
- State Application Submission Deadline: **April 21, 2023 by 5:00 PM**
- Federal Application Submission Deadline: **May 18, 2023 by 5:00 PM**
- Period of Performance: **Thirty-six (36) months**
- Performance Period Start Date: **September 1, 2023**
- Performance Period End Date: **August 31, 2026**

Outreach Series

The Federal Emergency Management Agency's (FEMA) Grant Programs Directorate invites all potential NSGP applicants and sub-applicants to participate in one of the upcoming outreach calls regarding the fiscal year (FY) 2023 NSGP.

Date	Time (ET)	Adobe Connect Registration Link
03/30/2023	3 PM	https://fema.connectsolutions.com/e74ri6jsemnb/event/registration.html
04/04/2023	2 PM	https://fema.connectsolutions.com/ezrhgk10r3uz/event/registration.html
04/25/2023	3 PM	https://fema.connectsolutions.com/ecqkgfqfajjp/event/registration.html
05/04/2023	2 PM	https://fema.connectsolutions.com/en4bo833pqur/event/registration.html
Note: Following registration, you will receive a calendar invitation for the webinar. The link to join the webinar is contained in that calendar event email. It may take time for this email to arrive – please wait following registration and be sure to check your junk/spam folders.		

DEMA will be hosting a webinar on Friday, March 17th, 2023 at 10am to provide general guidance and overview of the FY2023 NSGP to all potential Delaware NSGP applicants.

March 17, 2023	**Microsoft Teams meeting** Join on your computer, mobile app or room device • Click here to join the meeting • Meeting ID: 248 099 025 062 • Passcode: MvyP7S Or call in (audio only) • +1 302-504-8986,,647708069# United States, Wilmington • Phone Conference ID: 647 708 069#

For questions regarding the DEMA webinar on the FY2023 NSGP, please contact Mark Dworkin at PreparednessGrants@delaware.gov.

Program Priorities

Given the evolving threat landscape, it is incumbent upon DHS/FEMA to continuously evaluate the national risk profile and set priorities that help ensure appropriate allocation of scarce security dollars. In assessing the national risk profile for FY2023, enhancing the protection of soft targets and crowded places attracts the most concern.

Additionally, there are several enduring security needs that crosscut the homeland security enterprise. The following are enduring security priority areas that help recipients implement a comprehensive approach to securing communities:

- Effective Planning
- Training and awareness campaigns
- Exercises

The table below provides a breakdown of these priority areas for FY23 NSGP, showing both the core capabilities enhanced and lifelines supported, as well as examples of eligible project types for each area.

National Priorities		
Priority Areas	**Core Capabilities Enhanced**	**Example Project Types**

Enhancing the Protection of Soft Targets/Crowded Places	• Planning
	• Operational coordination
	• Public information and warning
	• Intelligence and Information Sharing
	• Interdiction and disruption
	• Screening, search, and detection
	• Access control and identity verification
	• Physical protective measures
	• Risk management for protection
	• programs and activities
	• Cybersecurity
	• Long-term vulnerability reduction
	• Situational assessment
	• Infrastructure systems
		<u>Private contracted security guards</u>
		<u>Physical security enhancements</u>
		• Closed circuit television (CCTV) security cameras
		• Security screening equipment for people and baggage
		• Access controls
		  • Fencing, gates, barriers, etc.
		  • Card readers, associated hardware/software
		<u>Cybersecurity Enhancements</u>
		• Risk-based cybersecurity planning and training
		• Improving cybersecurity of access control and identify verification systems
		• Improving cybersecurity of security technologies (e.g., CCTV systems)
		• Adoption of cybersecurity performance goals (https://www.cisa.gov/cpg)

Enduring Needs		
Priority Areas	**Core Capabilities Enhanced**	**Example Project Types**

Planning	• Planning
	• Risk management for protection programs and activities
	• Risk and disaster resilience assessment
	• Threats and hazards identification
	• Operational coordination
		• Conduct or enhancement of security risk assessments
		• Development of:
		  ○ security plans and protocols
		  ○ emergency contingency plans
		  ○ evacuation/shelter in place plans
		• Assessment of capabilities and gaps in planning for the needs of persons with disabilities and others with access and functional needs

Training and Awareness	• Long-term vulnerability reduction • Public information and warning	• Active shooter training • Security training for employees • Public awareness/preparedness campaigns
Exercises	• Long-term vulnerability reduction	• Response exercises

Risk Assessments

- **Violent Intruder Toolkit Self-Assessment:** The Delaware Information and Analysis Center (DIAC) has created a quick reference guide to help organizations further enhance their security posture. This guide contains instructions and template for a Self-Assessment/Security Risk Assessment to identify vulnerabilities at an organization's facility.
  - Link to DIAC Self-Assessment:
    - https://dediac.org/files/DDF/SELF-ASSESSMENT%20FORM.docx
- **Faith-Based Organizations:** The Cybersecurity & Infrastructure Security Agency (CISA) has created a tool designed to guide personnel at houses of worship through a security-focused self-assessment to understand potential vulnerabilities and identify options for consideration in mitigating those vulnerabilities. This self-assessment is a first step in building an effective security program; it is not intended to be an in-depth security assessment. After completing this process and addressing preliminary findings, houses of worship personnel may consider pursuing more detailed security assessments to explore specific issues in greater detail.
  - CISA Security Resources: Faith Based Organizations and Houses of Worship

Resource Links

- The **FY2023 NSGP NOFO** is located online at www.fema.gov/grants as well as on www.grants.gov.
- The **FY2023 FEMA Preparedness Grants Manual** is located online at www.fema.gov/grants.
- Delaware specific NSGP information and resources are available under the Nonprofit Security Grant Program in the resources tab on DEMA's website at: https://dema.delaware.gov/.
- Additional information and resources can be found on FEMA's website at: https://www.fema.gov/grants/preparedness/nonprofit-security.