FY 2025 Nonprofit Security Grant Program (NSGP)

Notice of Funding Opportunity (NOFO)

Grant Issued By:

U.S. Department of Homeland Security (DHS)/Federal Emergency Management Agency (FEMA)/Grant Programs Directorate (GPD)

Grant Issued Through:

Missouri Department of Public Safety (DPS), Office of Homeland Security (OHS)

Assistance Listing:

97.008

Funding Opportunity Title:

FY 2025 Nonprofit Security Grant Program (NSGP)

Overview

The Nonprofit Security Grant Program (NSGP) is one of the grant programs that support DHS/FEMA's focus on enhancing the ability of state, local, tribal, and territorial governments, as well as nonprofits, to prevent, protect against, prepare for, and respond to terrorist or other extremist attacks. This grant program is part of a comprehensive set of measures authorized by Congress and implemented by DHS to help strengthen the nation's communities against potential terrorist or other extremist attacks. The NSGP is a competitive grant program intended to provide federal funding for physical security enhancements and other security-related activities to nonprofit organizations that are at risk of terrorist attack.

In FY 2025, there are two funding sources appropriated for nonprofit organizations:

1) ***Nonprofit Security Grant Program (NSGP) - Urban Area (NSGP-UA):*** NSGP-UA funds nonprofit organizations located **within** FY 2025 Urban Area Security Initiative (UASI)-designated high-risk urban areas. Eligible applicant criteria is listed below under Applicant Eligibility Criteria.

2) ***Nonprofit Security Grant Program (NSGP) - State (NSGP-S):*** NSGP-S funds nonprofit organizations located **outside** of a FY 2025 UASI-designated high-risk urban area. Eligible applicant criteria is listed below under Applicant Eligibility Criteria.

DHS is focused on the criticality of information sharing and collaboration in building a national mindset of preparedness and protecting against terrorism and other threats to our national security. DHS and its homeland security mission were born from the "failures among federal agencies and between the federal agencies and state and local authorities to share critical information related to the threat of terrorism" prior to the September 11, 2001, attacks. However, the threat profile has changed in the past two decades. We now face continuous cyberattacks by sophisticated actors, as well as ongoing threats to soft targets and crowded places, such as schools, churches, synagogues, mosques, and other nonprofit entities. The NSGP reflects DHS's commitment to risk-informed investment, collaboration, and resilience.

Goal, Objectives, and Priorities

Goal: The NSGP will improve and increase the physical/cybersecurity and facility/target hardening of nonprofit organizations' facilities at risk of a terrorist or other extremist attack, ultimately safeguarding the lives and property of the American people. Concurrently, the NSGP will integrate the preparedness activities of nonprofit organizations that are at high risk of a terrorist or other extremist attack with broader state and local preparedness efforts.

Objectives: The NSGP provides funds to nonprofit organizations' facilities at risk of terrorist or other extremist attack to meet the following three objectives throughout the period of performance:

1) Enhance equipment and conduct security-related activities to improve the security posture of nonprofit organizations that are at high risk of a terrorist or other extremist attack.

    a. With this funding, build and sustain core capabilities, as identified in individual nonprofit organization Vulnerability Assessments, of high-risk nonprofit organizations in the annual national priority areas. See the table "FY 2025 NSGP Funding Priorities".

2) Address and close capability gaps that are identified in the individual nonprofit organization Vulnerability Assessments via funding spent on Planning, Equipment, and Training and Exercises that aim to enhance the protection of soft targets and crowded places.

    a. Planning – carrying out risk management for the protection of programs and activities, risk and disaster resilience assessment, threats, and hazard identification, as well as operational coordination.

    b. Equipment – Strengthening security infrastructure, technology, and protective measures.

    c. Training & Exercises – long-term vulnerability reduction via preparedness training, public information and warning enhancement, and threat response exercises.

3) Strengthen relationships across nonprofit organizations, state, local, and territorial homeland security strategy agencies for a whole community approach to preparedness.

    a. Implementing a comprehensive and coordinated (whole of community) approach to preparedness can address enduring security needs, including effective planning, training and awareness campaigns, and exercises. See the table "FY 2025 NSGP Funding Priorities".

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. The FY 2025 National Priority Areas (NPAs) reflect FEMA's broader mission across all preparedness efforts. Applicants should be familiar with these NPAs as they represent DHS's current focus areas and may shape future guidance:

1) Enhancing the Protection of Soft Targets/Crowded Places
2) Supporting Homeland Security Task Forces and Fusion Centers
3) Enhancing Cybersecurity
4) Enhancing Election Security
5) Supporting Border Crisis Response and Enforcement

Enduring needs include:

1) Effective planning
2) Training and awareness campaigns
3) Equipment and capital projects
4) Exercises

The table below provides a breakdown of the NPAs and core capabilities impacted, as well as examples of eligible project types for each area. More information on allowable investments can be found in the Funding Restrictions and Allowable Costs section below.

FY 2025 NSGP Funding Priorities

All priorities in this table concern the Safety and Security Lifelines.

National Priorities		
Priority Areas	**Core Capabilities**	**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 identify verification
	• Physical protective measures
	• Risk management for protection programs and activities
	• Long-term vulnerability reduction
	• Situational assessment
	• Infrastructure systems
		• Private contracted security guards
		• Physical security enhancements
		  ○ Closed circuit television (CCTV) security cameras
		  ○ Security screening equipment for people and baggage
		  ○ Access Controls
		  ▪ Fencing, gates, barriers, etc.
		  ▪ Card readers, associated hardware/software

Enhancing Cybersecurity	• Cybersecurity
	• Intelligence and information sharing
	• Interdiction and disruption
	• Long-term vulnerability reduction
		• Cybersecurity enhancements
		  ○ Risk-based cybersecurity planning and training
		  ○ Improving cybersecurity of access control and identity verification systems
		  ○ Improving cybersecurity of security technologies (e.g., CCTV systems)
		• Adoption of cybersecurity performance goals (CISA's Cross-Sector Cybersecurity Performance Goals)

Supporting Homeland Security Task Forces and Fusion Centers	• Intelligence and information sharing • Interdiction and disruption • Public information and warning • Operational coordination	• Establishing or enhancing multi-agency Homeland Security Task Forces (HSTFs), including operational coordination centers • Enhancing capabilities and integration with local fusion centers • Procurement of technology or equipment to support surveillance, communications, and data analysis

	• Risk management for protection programs and activities	• Development of standard operating procedures for information sharing, joint operations, and immigration enforcement coordination • Personnel training, credentialing, and certification to improve interoperability and mission alignment • Intelligence analysis, reporting, and suspicious activity monitoring • Exercises and simulations focused on joint operations, intelligence sharing, or interdiction/disruption of criminal or smuggling networks • Community engagement efforts to foster trust and encourage threat reporting • Information sharing with all DHS components; fusion centers; other operational investigative, and analytic entities; and other federal law enforcement and intelligence entities • Cooperation with DHS and other entities in intelligence, threat recognition, assessment, analysis, and mitigation • Identification, assessment, and reporting of threats of violence • Intelligence analysis training, planning, and exercises • Coordinating the intake, triage, analysis, and reporting of tips/leads and suspicious activity, to include coordination with the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI)
Enhancing Election Security	• Cybersecurity • Intelligence and information sharing • Planning • Long-term vulnerability reduction • Situational assessment • Infrastructure systems • Operational coordination • Community resilience	• Prioritize compliance with the VVSG 2.0 established by the U.S. Election Assistance Commission • Complete testing through a VSTL accredited by the U.S. Election Assistance Commission • Physical security planning and exercise support • Physical/site security measures – e.g., locks, shatter proof glass, alarms, access controls, etc. • General election security navigator support • Cybersecurity risk assessments, training, and planning • Projects that address vulnerabilities identified in cybersecurity risk assessments • Iterative backups, encrypted backups, network segmentation, software to monitor/scan, and endpoint protection • Distributed Denial of Service protection • Migrating online services to the ".gov" internet domain • Online harassment and targeting prevention services • Public awareness/preparedness campaigns discussing election security and integrity measures • Long-term vulnerability reduction and community resilience
Supporting Border Crisis Response and Enforcement	• Community resilience • Operational coordination • Risk management for protection programs and activities	• Staffing support to expand 287(g) screening operations within correctional facilities • Operational overtime costs directly tied to 287(g) screening, processing, and enforcement activities • Training programs for state and local law enforcement officers in immigration law, civil rights protections, and 287(g) procedures

		• Development or enhancement of information-sharing platforms between ICE and local agencies • Procurement of screening, detection, and communications technology to support immigration enforcement activities • Establishing secure and dedicated communication networks with ICE Field Offices • Conducting joint training exercises with ICE and local law enforcement to test operational coordination • Support for facilities upgrades, such as creating dedicated interview rooms and secure processing spaces • Community engagement and public briefings to promote transparency and understanding of 287(g) operations and protections
Enduring Needs		
Priority Areas	**Core Capabilities**	**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

Training & Awareness	• Long-term vulnerability reduction • Public information and warning	• Active shooter training, including integrating the needs of person with disabilities • Security training for employees • Public awareness/preparedness campaigns
Exercise	• Long-term vulnerability reduction	• Response exercises

NSGP-UA Maximum Award

St. Louis Urban Area

Applicants located within the St. Louis Urban Area Security Initiative (UASI)-designated urban area (St. Louis City and Missouri counties of St. Charles County, Franklin County, Jefferson County, St. Louis County and Illinois counties of Madison, St. Clair, and Monroe) with one site may apply for up to $200,000 per site. Applicants with multiple sites (multiple locations/physical addresses) may choose to apply for additional sites at up to $200,000 per site, for a maximum of three sites per funding stream, not to exceed $600,000 per **state**. Applicants with locations in multiple states may apply for up to three sites within each state and funding stream (three for NSGP-S and three for NSGP-UA per state). If an applicant applies for projects at multiple sites, regardless of whether the projects are similar in nature, it must include an assessment of the vulnerability and risk unique to each site. That is, one vulnerability assessment per location/physical address. Failure to do so may be cause for rejection of the application. Applicants must apply through the Missouri Department of Public Safety (DPS)/Office of Homeland Security (OHS) using the WebGrants System.

If an applicant applies for multiple sites, it must submit one complete Investment Justification (IJ) for each site. ***Additionally, an application must be submitted in the WebGrants System for each site/IJ. For***

example, if the applicant is applying for three sites/IJs, it MUST submit three separate applications in the WebGrants System to be eligible for funding.

Kansas City Urban Area

Applicants located within the Kansas City Urban Area Security Initiative (UASI)-designated urban area (Missouri counties of Jackson, Cass, Platte, Clay, and Ray and Kansas counties of Leavenworth, Wyandotte, and Johnson) with one site may apply for up to $200,000 per site. Applicants with multiple sites (multiple locations/physical addresses) may choose to apply for additional sites at up to $200,000 per site, for a maximum of three sites per funding stream, not to exceed $600,000 per **state**. Applicants with locations in multiple states may apply for up to three sites within each state and funding stream (three for NSGP-S and three for NSGP-UA per state). If an applicant applies for projects at multiple sites, regardless of whether the projects are similar in nature, it must include an assessment of the vulnerability and risk unique to each site. That is, one vulnerability assessment per location/physical address. Failure to do so may be cause for rejection of the application. Applicants must apply through the Missouri Department of Public Safety (DPS)/Office of Homeland Security (OHS) using the WebGrants System.

If an applicant applies for multiple sites, it must submit one complete Investment Justification (IJ) for each site. ***Additionally, an application must be submitted in the WebGrants System for each site/IJ. For example, if the applicant is applying for three sites/IJs, it MUST submit three separate applications in the WebGrants System to be eligible for funding.***

NSGP-S Maximum Award

Applicants located within the state of Missouri **outside** of the St. Louis and Kansas City Urban Area Security Initiatives with one site may apply for up to $200,000 per site. Applicants with multiple sites (multiple locations/physical addresses) may choose to apply for additional sites at up to $200,000 per site, for a maximum of three sites per funding stream, not to exceed $600,000 per **state**. Applicants with locations in multiple states may apply for up to three sites within each state and funding stream (three for NSGP-S and three for NSGP-UA per state). If an applicant applies for projects at multiple sites, regardless of whether the projects are similar in nature, it must include an assessment of the vulnerability and risk unique to each site. Failure to do so may be cause for rejection of the application. Applicants must apply through the Missouri Department of Public Safety (DPS)/Office of Homeland Security (OHS) using the WebGrants System.

If an applicant applies for multiple sites, it must submit one complete Investment Justification (IJ) for each site. ***Additionally, an application must be submitted in the WebGrants System for each site/IJ. For example, if the applicant is applying for three sites/IJs, it MUST submit three separate applications in the WebGrants System to be eligible for funding.***

Period of Performance: 24 months

Extensions to the period of performance may be allowed. For additional information on period of performance extensions refer to the Missouri Office of Homeland Security, Division of Grants, Administrative Guide.

Projected Period of Performance Start Date(s): September 1, 2025

Projected Period of Performance End Date(s): August 31, 2027

Funding Instrument Type: Grant

Applicant Eligibility Criteria

Eligible nonprofit organizations are those organizations that are:

1. 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. ***This includes entities designated as "private" (e.g., private institutions of higher learning), as private colleges and universities can also be designated as 501 (c)(3) entities.***

   Note: The Internal Revenue Service (IRS) does not require certain organizations such as churches, mosques, and synagogues to apply for and receive a recognition of exemption under section 501(c)(3) of the IRC. Such organizations are automatically exempt if they meet the requirements of section 501(c)(3). These organizations are not required to provide recognition of exemption. For organizations that the IRS requires to apply for and receive a recognition of exemption under section 501(c)(3), the state of Missouri requires recognition of exemption to be submitted with the application.

   Refer to links below for additional information:
   - Exemption Requirements - 501(c)(3) Organizations
   - Tax-Exempt Status for Your Organization
   - Charities and Nonprofits

2. Able to demonstrate, through the application, that the organization is at high risk of a terrorist or other extremist attack

3. NSGP-UA
   a. located **inside** of the FY 2025 St. Louis UASI-designated urban area (St. Louis City and the Missouri Counties of Franklin, Jefferson, St. Charles, and St. Louis and Illinois counties of Madison, St. Clair, and Monroe)
   b. located **inside** of the FY 2025 Kansas City UASI-designated urban area (Missouri Counties of Jackson, Cass, Platte, Clay, and Ray and Kansas counties of Leavenworth, Wyandotte, and Johnson)

4. NSGP-S, located within the State of Missouri **outside** of the FY 2025 St. Louis UASI-designated urban area (St. Louis City and the Missouri Counties of Franklin, Jefferson, St. Charles, and St. Louis) and Kansas City UASI-designated urban area (Missouri Counties of Jackson, Cass, Platte, Clay, and Ray)

The final beneficiary of the NSGP grant award must be an eligible nonprofit organization and cannot be a for-profit/fundraising extension of a nonprofit organization. While these for-profit or fundraising extensions may be associated with the eligible nonprofit organization, NSGP funding cannot be used to benefit those extensions and therefore the will be considered ineligible applications. If the funding being sought is for the benefit of a for-profit/fundraising extension, then that would constitute an ineligible applicant since only nonprofit organizations are eligible applicants.

An application submitted by an otherwise eligible non-federal entity (i.e., the applicant) may be deemed ineligible when the person that submitted the application 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)/Authorized Official must be a duly authorized current employee, personnel,*

official, or leadership of the recipient and provide an email address unique to the recipient at the time of application and upon any change in assignment during the period of performance. ***Consultants or contractors of the subrecipient are not permitted to be the AOR/Authorized Official of the subrecipient.***

Application and Submission Information

1. Key Dates and Times

a. Application Start Date: November 3, 2025

b. Application Submission Deadline: December 1, 2025, 5:00 p.m. CST

2. Agreeing to Terms and Conditions of the Award

By submitting an application, applicants agree to comply with the requirements of this NOFO and the terms and conditions of the award, should they receive an award.

Nonprofit Organization Specific Application Instructions

Applications will only be accepted through the Missouri Department of Public Safety (DPS) online WebGrants System.

Applicants must designate the NSGP funding source they are applying for in the WebGrants System. Applicants should review the NSGP Funding Source Map in WebGrants to determine which program to apply for based on the physical location of the facility for the project. **If the incorrect funding source is chosen, the application will be ineligible for funding**.

- NSGP – S
- NSGP – UA St. Louis
- NSGP – UA Kansas City

A PowerPoint presentation with instructions on how to apply through the WebGrants System will be available on the DPS website under Grant Applications and Forms, FY 2025 Nonprofit Security Grant Program (NSGP).

As part of the FY 2025 NSGP application, each eligible nonprofit applicant must submit the following documents:

1. NSGP Investment Justification (IJ)

Applicants with one site may apply for up to $200,000 for that site. Applicants with multiple sites may apply for up to $200,000 per site, for up to three sites per funding stream for a maximum of $600,000 per applicant. If an applicant applies for multiple sites, it **must submit one complete IJ for each site**. IJ's **CANNOT** include more than one physical site. A fillable IJ form is available on the DPS website under Grant Applications and Forms, FY 2025 Nonprofit Security Grant Program (NSGP). The IJ form will also be linked in the WebGrants System.

The IJ must describe each investment proposed for funding. The investments or projects described in the IJ must:

- Be for the location(s)/physical address (no P.O. Boxes) that the nonprofit occupies at the time of application
- Address an identified risk, including threat and vulnerability, regardless of whether it is submitting for similar projects at multiple sites
- Demonstrate the ability to provide enhancements consistent with the purpose of the program and guidance provided by DHS/FEMA
- Be both feasible and effective at reducing the risks for which the project was designed
- Be able to be fully completed within the two-year period of performance
- Be consistent with all applicable requirements outlined in this NOFO and the Preparedness Grants Manual.

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

The **fillable version of the FY 2025 IJ** must be submitted as an attachment to the application through the WebGrants System. Older versions and those that are not fillable will **NOT** be accepted and the application will be deemed **INELIGIBLE**.

Additionally, an application must be submitted in the WebGrants System for each site/IJ. For example, if the applicant is applying for three sites/IJs, it MUST submit three separate applications in the WebGrants System to be eligible for funding.

2. Vulnerability/Risk Assessment

Each applicant must include a vulnerability/risk assessment **unique to the site** the IJ is being submitted for. Activities requested for funding in the Investment Justification (IJ) **MUST** directly align to the Vulnerability/Risk Assessment.

The Vulnerability/Risk Assessment must be submitted as an attachment to the application through the WebGrants System.

3. Mission Statement

Each applicant must include its Mission Statement and any mission implementation policies or practices that may elevate the organization's risk.

The Mission Statement must be submitted as an attachment to the application through the WebGrants System.

4. Audit

Each applicant must provide the agency's most recent audit. If the applicant does not have a completed audit or the audit is more than three years old, the agency must provide their most recent annual financial statement.

The audit/financial statement must be submitted as an attachment to the application through the WebGrants System.

5. 501(c)(3) Documentation

Applicants, that are required by the IRS to apply for and receive a recognition of exemption under section 501 (c)(3), must submit recognition of exemption as an attachment to the application through the WebGrants System.

Funding Restrictions and Allowable Costs

Costs charged to federal awards (including federal and non-federal cost share funds) must comply with applicable statutes, rules, regulations, policies, this NOFO, the Preparedness Grants Manual, and the terms and conditions of the federal award. This includes, among other requirements, that costs must be incurred, and products and services must be delivered, within the budget period. See 2 C.F.R. § 200.403(h)

Subrecipients may not use federal funds or any cost share funds for the following activities:

1) Matching or cost sharing requirements for other federal grants and cooperative agreements (see 2 C.F.R. § 200.306)
2) Lobbying or other prohibited activities under 18 U.S.C. § 1913 or 2 C.F.R. § 200.450.
3) Prosecuting claims against the federal government or any other government entity (see 2 C.F.R. § 200.435).

See the Preparedness Grants Manual for more information on funding restrictions and allowable costs.

1. Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services

Subrecipients and their contractors or subcontractors must comply with the prohibitions set forth in Section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019, which restrict the purchase of covered telecommunications and surveillance equipment and services. Please see 2 C.F.R. §§ 200.216, 200.327, 200.471, and Appendix II to 2 C.F.R. Part 200, and FEMA Policy #405-143-1 – Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services for more information.

2. Pre-Award Costs

Subrecipients cannot claim pre-award costs.

3. Management and Administration (M&A) Costs

M&A costs are allowed.

M&A costs are not operational costs but are necessary costs incurred in direct support of the federal award or as a consequence of it, such as travel, meeting-related expenses, and salaries of full/part-time staff in direct support of the program. As such, M&A costs can be itemized in financial reports. Other M&A costs examples include preparing and submitting required programmatic and financial reports, establishing and/or maintaining equipment inventory, documenting operational and equipment expenditures for financial accounting purposes, and responding to official informational requests from state and federal oversight authorities.

Nonprofit organizations that receive a subaward under the NSGP may use and expend up to 5% of each subaward for M&A purposes associated with that subaward. If an organization is receiving more than one subaward, they must be able to separately account for M&A costs for each subaward.

4. Indirect Costs

Indirect costs are allowed for subrecipients.

Indirect costs (IDC) are costs incurred for a common or joint purpose benefitting more than one cost objective and not readily assignable to a specific cost objective without disproportionate effort. Applicants with a current negotiated indirect cost rate agreement who desire to charge indirect costs to a federal award must provide a copy of their IDC rate agreement with their applications. Not all applicants are required to have a current negotiated indirect cost rate agreement. Applicants that are not required to have a negotiated IDC rate agreement. Applicants that are not required to have a current negotiated IDC rate agreement, but are required to develop an IDC rate proposal, must provide a copy of their proposal with their applications. Applicants without a current negotiated IDC rate agreement (including a provisional rate) and wish to charge the de minimis rate must reach out to DPS/OHS for further instructions. Applicants who wish to use a cost allocation plan in lieu of an IDC rate proposal must reach out to the DPS/OHS for further instructions. See the Preparedness Grants Manual for information on establishing indirect cost rates.

5. Other Direct Costs

a. 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 and should include consideration of 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 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
- Other project planning activities with prior approval from FEMA

b. Organization

Organization costs are not allowed under this program.

c. Equipment

Allowable costs are focused on facility hardening and physical security enhancements. 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 or other extremist attack. This equipment is **limited to select items** on the Authorized Equipment List (AEL). These items are as follows:

AEL Code	Title	Description
03OE-03-MEGA	System, Public Address, Handheld or Mobile	Systems for mass audio notification, including vehicle-mounted high powered speaker systems, or battery powered megaphone/public address systems with corded microphone.
03OE-03-SIGN	Signs	Restricted access and caution warning signs that preprinted or field printable and can be various colors, sizes, and shapes. Examples can include traffic cones, other free-standing signage, mountable items, and signs and devices for individuals with disabilities and others with access and functional needs (e.g., programmable audible caution cones and scrolling marquis signs).
04AP-05-CRED	System, Credentialing	Software application and associated hardware and material for creating site/event credential badges and controlling scene access. Although some hardware may be required, functionality may also be obtainable via subscription as a cloud-based service, as opposed to purchasing software.
04-AP-06-VIDA	Software, Video Analytics	Software, either local or cloud-based, that analyzes video input to detect/determine temporal and spatial events, either in real time or using archival video. Analytical priorities might include recognition or patterns (movement or arrangement or persons, vehicles, or other objects). For the NSGP, license plate reader and facial recognition software are not allowed but software to detect weapons through video analysis is allowed.
04AP-09-ALRT	Systems, Public Notification and Warning	Systems used to alert the public of protective actions or provide warning to the public in the event of an incident, such as sirens, the Emergency Alert System (EAS), the Integrated Public Alert and Warning System (IPAWS), and Wireless Emergency Alerts (WEA).

04AP-11-SAAS	Applications, Software as a Service	Sometimes referred to as "on-demand software," this application runs on the provider's servers, delivering functionality via the internet to any device having connectivity and the required browser or interface. Access to the application is obtained via a service subscription rather than outright purchase, with all updates and configuration requirements handled by the service provider. This item is limited to those services that support security systems such as access controls, camera networks, cybersecurity services, or other critical infrastructure security.
05AU-00-TOKN	System, Remote Authentication	Systems used to provide enhanced remote authentication, often consisting of a server or synchronization scheme and a device, token, or smartphone application.
05EN-00-ECRP	Software, Encryption	Encryption software used to protect stored data files or email messages.
05HS-00-MALW	Software, Malware/Anti-Virus Protection	Software for protection against viruses, spyware, and malicious code. May be obtained for individual hosts or for entire network segments.
05HS-00-PFWL	System, Personal Firewall	Personal firewall for operation on individual workstations. This item is usually a software solution, but appliances are also available. See also: 05NP-00-FWAL.
05NP-00-FWAL	Firewall, Network	Firewall (software or standalone appliance) for use in protecting networks. See also 05HS-00-PFWL.
05NP-00-IDPS	System, Intrusion Detection/Prevention	Intrusion Detection and/or Prevention System deployed at either host or network level to detect and/or prevent unauthorized or aberrant (i.e., abnormal) behavior on the network.
06CP-01-PORT	Radio, Portable	Individual/portable radio transceivers, for notifications and alerts.
06CP-01-REPT	Repeater	Electronic device that receives a weak or low-level signal and retransmits that signal to extend usable range.
06CC-02-PAGE	Services/Systems, Paging	Paging services/systems/applications; one-way text messaging for notifications or alerts.
06CP-03-ICOM	Intercom/Intercom System	Communication system for a limited number of personnel in close proximity to receive alerts or notifications.
06CP-03-PRAC	Accessories, Portable Radio	Speaker/microphone extensions to portable radios.
10GE-00-GENR	Generators	Generators (gasoline, diesel, propane, natural gas, etc.) and their required installation materials, including 10PE-00-PTSW (a power switch) if not already included, to support a

		redundant power supply for security systems, alarms, lighting, and other physical security/cybersecurity infrastructure or systems.
10PE-00-UPS	Supply, Uninterruptible Power (UPS)	Systems that compensate for power loss to serviced equipment (e.g., short-duration battery devices, standby generator devices for longer duration).
13IT-00-ALRT	System, Alert/Notification	Alert/notification software that allows for real-time dissemination of information for situational awareness or alerts among a group via means such as smartphones, landlines, pagers, etc. This item may also be a subscription cloud-based service using a web browser interface or a mobile application instead of a software.
14CI-00-COOP	System, Information Technology Contingency Operations	Back-up computer hardware, operating systems, data storage, and application software necessary to provide a working environment for contingency operations. May be a purchased as a remote service or a dedicated alternate operating site.
14EX-00-BCAN	Receptables, Trash, Blast-Resistant	Blast-resistant trash receptacles.
14EX-00-BSIR	Systems, Building, Blast/Shock/Impact Resistant	Systems to mitigate damage from blasts, shocks, or impacts, such as column and surface wraps, wall coverings, portable or fix ballistic boards/barriers, breakage/shatter resistant glass, window wraps/films/velums, etc.
14SW-01-ALRM	Systems, Sensors, Alarm	Systems and standalone sensors designed to detect access violations or intrusions using sensors such as door/window switches, motion sensors, acoustic sensors, seismic sensors, and thermal sensors. May also include temperature sensors for critical areas.
14SW-01-ASTN	Network, Acoustic Sensor Triangulation	Network of deployed acoustic sensors and one or more processing nodes for data integration and analysis. Such networks can be set to one or more ranges of frequencies to detect sounds such as gunshots, heavy weapons discharge, explosions, man-portable air defense system launches, vehicle noises, etc., and utilize acoustic triangulation to provide accurate location data. Such networks can be wired, wireless, or hybrid, and are capable of operation near critical infrastructure assets or in wide areas.
14SW-01-DOOR	Doors and Gates, Impact Resistant	Reinforced doors and gates with increased resistance to external impact for increased physical security.

14SW-01-LITE	Lighting, Area, Fixed	Fixed high-intensity lighting systems for improved visibility in areas such as building perimeters, parking lots, and other critical zones to increase physical security.
14SW-01-PACS	System, Physical Access Control	Locking devices and entry systems for control of physical access to facilities.
14SW-01-SIDP	Systems, Personnel Identification	Systems for positive identification of personnel as a prerequisite for entering restricted areas or accessing information systems.
14SW-01-SIDV	Systems, Vehicle Identification	Systems for identification of vehicles, ranging from decals to radio frequency identification or other transponder devices. (License plate reader and facial recognition software are NOT allowed.)
14SW-01-SNSR	Sensors/Alarms, System and Infrastructure Monitoring, Standalone	Standalone sensors/alarms for use on critical systems or infrastructure items (e.g., security systems, power supplies, etc.) to provide warning when these systems fail or are near failure.
14SW-01-VIDA	Systems, Video Assessment, Security	Camera-based security systems utilizing standard, low light, or infrared technology. (License plate reader and facial recognition software are NOT allowed.)
14SW-01-WALL	Barriers: Fences; Jersey Walls	Obstacles designed to channel or halt pedestrian or vehicle-borne traffic to protect a physical asset or facility such as barriers, bollards, planters, benches etc. (Earthen barriers, berms, trees, or other botanical obstacles are NOT allowed.)
15SC-00-PPSS	Systems, Personnel/Package Screening	Hand-held or fixed systems such as walk-through magnetometers used to screen personnel and packages for hazardous materials/devices.
21GN-00-INST	Installation	Installation costs for authorized equipment purchased through FEMA grants.
21GN-00-TRNG	Training and Awareness	

****Note: Radios purchased with NSGP funding will not be permitted to operate on the Missouri Statewide Interoperability Network (MOSWIN). ****

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. In addition, subrecipients will be responsible for obtaining and maintaining all necessary certifications and licenses for the requested equipment, whether with NSGP funding or other sources of funds.

Subrecipients may purchase equipment not listed on the AEL, but **only** if they first seek and obtain **prior approval** from FEMA. Contact DPS/OHS for further instructions on prior approval requirements.

Applicants should analyze the costs and benefits of purchasing versus leasing equipment, especially high cost items and those subject to rapid technical advances. Large equipment purchases must be identified and explained. For more information regarding property management standards for equipment, please reference 2 C.F.R. Part 200, including but not limited to 2 C.F.R. §§ 200.310, 200.313, and 200.316. Also see 2 C.F.R. §§ 200.216, 200.471, and FEMA Policy #405-143-1, Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services, regarding prohibitions on covered telecommunications equipment or services. Additionally, subrecipients 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. This SAFECOM Guidance can be found at SAFECOM Funding and Sustainment.

The installation of certain equipment may trigger Environmental Planning and Historic Preservation (EHP) requirements. Please reference the EHP section in the NOFO and the Preparedness Grants Manual for more information.

d. Training and Exercises

Subrecipients may use NSGP funds for the following training-related costs:

- Employed or volunteer security staff to attend security-related training within the United States
- Employed or volunteer staff to attend security-related training within the United States with the intent of training other employees or members/congregants upon completing the training (i.e., "train-the-trainer" type courses)
- Nonprofit organization's employees, or members/congregants to receive on-site security training

Allowable training-related costs under NSGP are limited to attendance fees for training and related expenses, such as materials, supplies, and/or equipment. Overtime, backfill, and 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 the 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 NSGP funds must address a specific threat and/or vulnerability, as identified in the nonprofit organization's Investment Justification. 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 associated costs using the NSGP must be included in the nonprofit organization's IJ.

Funding may be used to conduct security-related exercises. This includes costs related to planning, meeting space and other meeting costs, facilitation costs, materials and supplies, and documentation. Exercises afford organizations the opportunity to validate plans and procedures, evaluate capabilities, and assess progress toward meeting capability targets in a controlled, low risk setting. All shortcomings or gaps – including those identified for children and individuals with access and functional needs – should be identified in an improvement plan. Improvement plans should be dynamic documents with corrective actions continually monitored and implemented as part of improving preparedness through the exercise cycle.

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 Homeland Security Exercise and Evaluation Program. In accordance with HSEEP guidance, subrecipients are reminded of the importance of implementing corrective actions iteratively throughout the progressive exercise cycle. This link provides access to a sample After Action Report (AAR)/Improvement Plan (IP) template: Improvement Planning – HSEEP Resources – Preparedness Toolkit.

e. Maintenance and Sustainment

Maintenance and sustainment costs, such as maintenance contracts, warranties, repair or replacement costs, upgrades, and user fees are allowable. Warranty and sustainment coverage may exceed the period of performance (POP) if purchased as part of the original purchase of the system or equipment if the original purchase of the system or equipment is consistent with that which is typically provided for, or available through, these types of agreements, warranties, or contracts. When purchasing a stand-alone warranty or extending an existing maintenance contract on an already-owned piece of equipment system, coverage purchased may not exceed the POP of the award used to purchase the maintenance agreement or warranty. As with warranties and maintenance agreements, this extends to licenses and user fees as well.

f. Construction and Renovation

NSGP funding may not be used for construction and renovation projects without prior written approval from FEMA. In some cases, the installation of equipment may constitute construction and/or renovation. If you have any questions regarding whether an equipment installation project could be considered construction or renovation, please contact the DPS/OHS. The total cost of any construction or renovation paid for using NSGP funds may not exceed 15% of the NSGP award.

g. Contracted Security Personnel

Contracted security personnel are allowed under this program only as described in this NOFO and must comply with guidance set forth in Information Bulletin 421b and Information Bulletin 441. NSGP funds may not be used to purchase equipment for contracted security.

Unallowable Costs

The following projects and costs are considered **ineligible** for award consideration:

- Organization costs, and operational overtime costs
- Hiring of public safety personnel (excluding off duty law enforcement personnel in the capacity of contract security)
- General-use expenditures
- Overtime and backfill
- 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 IJ
- Initiatives in which federal agencies are the beneficiary or that enhance federal property
- Initiatives which study technology development
- Proof-of-concept initiatives
- Direct or indirect pass-through of benefits to non-eligible entities

Administrative and National Policy Requirements

1. Presidential Executive Orders

Subrecipients must comply with the requirements of Presidential Executive Orders related to grants (also known as federal assistance and financial assistance), the full text of which are incorporated by reference.

2. DHS Standard Terms and Conditions

A subrecipient under this funding opportunity must comply with the DHS Standard Terms and Conditions in effect as of the date of the federal award. The DHS Standard Terms and Conditions are available online: DHS Standard Terms and Conditions. The specific version of the DHS Standard Terms and Conditions applicable to the federal award will be in the federal award package.

3. Environmental Planning and Historic Preservation (EHP) Compliance

FEMA is required to consider the effects of its actions on the environment and historic properties to ensure that all activities, grants, and programs funded by FEMA, comply with federal Environmental Planning and Historic Preservation (EHP) laws, Executive Orders (EO), regulations, and policies.

Subrecipients proposing projects with the potential to impact the environment or cultural resources, such as the modification or renovation of existing buildings, structures and facilities, and/or new construction and/or replacement of buildings, structures, and facilities must participate in the FEMA EHP review process. This includes conducting early engagement to help identify EHP resources, such as threatened or endangered species, historic properties, or communities with environmental concerns; submitting a detailed project description with supporting documentation to determine whether the proposed project has the potential to impact EHP resources; and identifying mitigation measures and/or alternative courses of action that may lessen impacts to those resources.

FEMA is sometimes required to consult with other regulatory agencies and the public in order to complete the review process. Federal law requires EHP review to be completed before federal funds are released to carry out proposed projects. FEMA may not be able to fund projects that are not in compliance with applicable EHP laws, Executive Orders, regulations, and policies. FEMA may recommend mitigation measures and/or alternative courses of action to lessen impacts to EHP resources and bring the project into EHP compliance.

EHP guidance is found at Environmental Planning and Historic Preservation. The site contains links to documents identifying agency EHP responsibilities and program requirements, such as implementation of the National Environmental Policy Act and other EHP laws, regulations, and Executive Orders. DHS and FEMA EHP policy is also fund in the EHP Directive and Instruction.

All FEMA actions, including grants, must comply with National Flood Insurance Program (NFIP) criteria or any more restrictive federal, state, or local floodplain management standards or building code (44 C.F.R. § 9.11(d)(6)). For actions located within or that may affect a floodplain or wetland, the following alternatives must be considered: a) no action; b) alternative locations; and c) alternative actions, including alternative actions that use natural features or nature-based solutions. Where possible, natural features and nature-based solutions shall be used. If not practicable as an alternative on their own, natural features, and nature-based solutions may be incorporated into actions as minimization measures.

The GPD EHP screening form is located on FEMA's website. The form should be submitted to the DPS/OHS.

4. Monitoring and Oversight

Per 2 C.F.R. § 200.337, DHS and its authorized representatives have the right of access to any records of the subrecipient pertinent to a Federal award to perform audits, site visits, and any other official use. The right also includes timely and reasonable access to the subrecipient's personnel for the purpose of interview and discussion related to such documents or the Federal award in general. Pursuant to this right and per 2 C.F.R. § 200.329, DHS may con project accomplishments and management control systems as well as provide any required technical assistance. Subrecipients must respond in a timely and accurate manner to DHS/DPS/OHS requests for information relating to a federal award.

5. Build America, Buy America Act

Subrecipients must comply with FEMA's implementation requirements of the Build America, Buy America Act (BABAA), which was enacted as part of the Infrastructure Investment and Jobs Act §§ 70901-70927, Pub. L. No. 117-58 (2021); and Executive Order 14005, Ensuring the Future is Made in All of America by All of America's Workers. See also 2 C.F.R. Part 184, Buy America Preferences for Infrastructure Projects and Office of Management and Budget (OMB) Memorandum M-24-02, Implementation Guidance on Application of Buy America Preference in Federal Financial Assistance Programs for Infrastructure.

None of the funds provided under this program may be used for a project for infrastructure unless the iron and steel, manufactured products, and construction materials used in that infrastructure are produced in the United States.

The Buy America preference only applies to articles, materials, and supplies that are consumed in, incorporated into, or affixed to an infrastructure project. As such, it does not apply to tools, equipment, and supplies, such as temporary scaffolding, brought to the construction site and removed at or before the completion of the infrastructure project. Nor does a Buy America preference apply to equipment and

furnishings, such as movable chairs, desks, and portable computer equipment, that are used at or within the finished infrastructure project but are not an integral part of the structure or permanently affixed to the infrastructure project.
To see whether a particular FEMA federal financial assistance program is considered an infrastructure program and thus required to implement FEMA's Build America, Buy America requirements, please see Programs and Definitions: Build America, Buy America Act.

a. Waivers

When necessary, subrecipients may apply for, and FEMA may grant, a waiver from these requirements.

A waiver of the domestic content procurement preference may be granted by the agency awarding official if FEMA determines that:

- Applying the domestic content procurement preference would be inconsistent with the public interest
- The types of iron, steel, manufactured products, or construction materials are not produced in the United States in sufficient and reasonably available quantities or of a satisfactorily quality
- The inclusion of iron, steel, manufactured products, or construction materials produced in the United States will increase the cost of the overall project by more than 25%

The process for requesting a waiver from the Buy America preference requirements can be found on FEMA's website at: "Buy America" Preference in FEMA Financial Assistance Programs for Infrastructure.

The Missouri Department of Public Safety is an equal opportunity employer and agency. Those with limited English proficiency or who need auxiliary aids or other services, can contact dpsinfo@dps.mo.gov. For Relay Missouri, please dial 711. For TTY/TDD, please dial 800-735-2966.

Contact Information:

Additional information and resources on the FY 2025 NSGP grant opportunity can be located on the Missouri Department of Public Safety (DPS)/Office of Homeland Security (OHS) website in the Grant Applications and Forms section.

Applications must be submitted through the WebGrants System.

Missouri Department of Public Safety (DPS)/Office of Homeland Security (OHS):

Joanne Talleur
Grants Specialist
(573) 522-2851
Joanne.Talleur@dps.mo.gov

Chelsey Call
Grants Supervisor
(573) 526-9203
Chelsey.Call@dps.mo.gov

Joni McCarter
Program Manager
(573) 526-9020
Joni.McCarter@dps.mo.gov