Notice of Funding Opportunity

Application due: July 24, 2026

Nonprofit Security Grant Program (NSGP)

Assistance Listing Number: 97.008
Funding Opportunity Number: DHS-26-GPD-008-00-99

Contents

Before you begin 2

Step 1: Review the Opportunity 3

Basic information 4

Eligibility 5

Program Description 8

Step 2: Get Ready to Apply 21

Submission Requirements and Application Deadlines 22

Step 3: Write Your Application 25

Application Contents and Format 26

Step 4: Learn About the Award Review Process 29

Application Review Information 30

Intergovernmental Review 35

Step 5: Learn What Happens After Award 37

Award Notices 38

Post-Award Requirements and Administration 39

Other Information 48

Contacts and Appendices 55

Contacts 56

Appendices 58

Before you begin

If you believe you are a good candidate for this funding opportunity, secure your System for Award Management (SAM.gov) and Grants.gov registrations now. If you are already registered, make sure your registration is active and up-to-date.

(a) SAM.gov registration (this can take several weeks)

You must have an active account with SAM.gov. This includes having a Unique Entity Identifier (UEI).

See Step 2: Get Ready to Apply

(b) Grants.gov registration (this can take several days)

You must have an active Grants.gov registration. Doing so requires a Login.gov registration as well.

See Step 2: Get Ready to Apply

Fraud, waste, abuse, mismanagement, and other criminal or noncriminal misconduct related to this program may be reported to the Office of Inspector General (OIG) Hotline. The toll-free numbers to call are 1-(800)-323-8603 and TTY 1-(844)-889-4357

To help you find what you need, this NOFO uses internal links. In Adobe Reader, you can go back to where you were before clicking an internal link by pressing Alt + Left Arrow (Windows) or Command + Left Arrow (Mac) on your keyboard.

A. Step 1: Review the Opportunity

In this step

Basic information 4

Eligibility 5

Program description 8

1. Basic Information

A. Award Facts

Agency Name: Department of Homeland Security (DHS),Federal Emergency Management Agency (FEMA), Resilience, Grant Programs Directorate, Preparedness Grants Division, Nonprofit Security Grant Program
Assistance Listing Number: 97.008

Notice of Funding Opportunity (NOFO) Title: Fiscal Year (FY) 2026 Nonprofit Security Grant Program (NSGP)

Funding Opportunity Number: DHS-26-GPD-008-00-99

Announcement Type: Initial

Expected Award Range:

- **NSGP - Urban Area (NSGP-UA)**: $269,000 – $32 million
- **NSGP - State (NSGP-S):** $0 or 1.4 million - $5.9 million

Expected Total Funding: $300,000,000

- **Subtotal for NSGP-UA: $150 million**
- **Subtotal for NSGP-S: $150 million**

Anticipated Number of Awards: 56 Awards

Have questions? See Contacts and Support

Key Dates

Projected Application Start Date: June 24, 2026

Projected Application End Date: July 24, 2026

Anticipated Funding Selection Date:
No later than 09/30/2026

Anticipated Award Date:
No later than 09/30/2026

Projected Period of Performance Start Date:
09/1/2026

Projected Period of Performance End Date:
08/31/2029

Budget Period:
09/1/2026 - 08/31/2029

1. Executive Summary

The FY 2026 Nonprofit Security Grant Program (NSGP) enhances the physical/cybersecurity and facility/target hardening of nonprofit organizations' facilities at risk of terrorist or other extremist attacks, ultimately safeguarding the lives and property of the American people.

The State Administrative Agency (SAA) is responsible for administering NSGP funds and coordinating with eligible nonprofit organizations.

In FY 2026, there are two funding sources available for nonprofit organizations:

1. **NSGP - Urban Area (NSGP-UA):** Provides funding to nonprofit organizations located **within** FY 2026 designated high-risk urban areas. Each NSGP-UA recipient will receive an allocation for nonprofit organizations **within** FY 2026 designated high-risk urban areas.
2. **NSGP - State (NSGP-S):** Provides funding to nonprofit organizations located **outside** of a FY 2026 designated high-risk urban area. Each NSGP - S recipient will receive an allocation for nonprofit

organizations in the state located **outside** of FY 2026 designated high-risk urban areas.

2. Eligibility

A. Eligible Entities

Only the following entities or entity types are eligible to apply.

(1) Applicant Eligibility

Note: Throughout this funding notice, the term "applicant" refers to the SAA, and the term "subapplicant" refers to the nonprofit organization. Consistent with the commitment to clarity and transparency, most of this NOFO's information identifies actions for the applicant to take, not the subapplicant. Contact FEMA-NSGP@fema.dhs.gov with questions.

All states, territories and FEMA identified high-risk urban areas SAAs are deemed the only applicants eligible to apply to FEMA for funding. Nonprofit organizations are eligible as subapplicants to SAAs. Nonprofit organizations may NOT apply directly to the Department of Homeland Security (DHS)/FEMA for FY 2026 NSGP funds.

Additional information on the subapplicant processes specific to nonprofit organizations is included in the Subapplicant Eligibility subsection of this funding notice.

SAAs, in coordination with the Urban Area Working Groups (UAWG) or other relevant state partners, are encouraged to notify and actively inform eligible nonprofit organizations of the availability of FY 2026 NSGP funding.

NSGP-UA funds nonprofit organization located **within** the FY 2026 designated high-risk urban area. Under NSGP-UA, each urban area will receive an allocation for nonprofit organizations located within a designated high-risk urban area. See Appendix B for the complete list.

NSGP-S funds nonprofit organizations located **outside** of a FY 2026 designated high-risk urban area. Under NSGP-S, each state will receive an allocation for nonprofit organizations in the state located outside of FY 2026 Designated high-risk urban areas. See Appendix C for the FY 2026 Allocations.

(2) Subapplicant Eligibility

Nonprofit organization subapplicants and subawards are allowed. However, *Nonprofit organizations may* NOT *apply to FEMA directly.*

Nonprofit organizations must apply for the FY 2026 NSGP through their SAA, which is responsible for submitting application information to FEMA. A list of SAA points of contact is available at: State Administrative Agency (SAA) Contacts | FEMA.gov. Subawards are permitted under the NSGP. The SAA receives the award and subsequently distributes funds to nonprofit organizations, which are considered subrecipients. All funds provided to nonprofit organizations are classified as subawards.

Nonprofit organizations eligible to apply as **subapplicants to the SAA** 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 501c3 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 may not require recognition of exemption, if the method chosen is applied consistently.

   Refer to links below for additional information:
   - Exemption Requirements - 501(c)(3) Organizations | Internal Revenue Service (irs.gov)
   - Publication 557 (01/2022), Tax-Exempt Status for Your Organization | Internal Revenue Service (irs.gov)
   - Charities and Nonprofits | Internal Revenue Service (irs.gov)

2. Able to demonstrate, through the application, that the organization is at high risk of a terrorist or other extremist attack; and
3. For NSGP-UA, located within a FY 2026 designated high-risk urban area; or for NSGP-S, located outside of a FY 2026 designated high-risk urban area.

Examples of eligible subapplicant organizations can include houses of worship, museums, educational facilities, senior centers, community centers, and day camps, among many others.

B. Project Type Eligibility

(3) Allowable Project Types

Allowable costs generally must fall into the categories of planning, equipment, training, or exercises.

Please see Appendix A: Allowable Costs for more information on allowable costs.

If there are any questions regarding allowable costs, please contact the appropriate FEMA Headquarters (HQ) Preparedness Officer (or contact fema-nsgp@fema.dhs.gov for information on the designated HQ Preparedness Officer).

(4) Unallowable Project Types

See Program-Specific Unallowable Costs for more information on unallowable project types.

C. Requirements for Personnel, Partners, and Other Parties

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.

Subapplicants/subrecipients should not include foreign nationals or noncitizens. If a subapplicant/subrecipients has foreign nationals, they must be properly vetted and must adhere to all government statues, polices, and procedures including "staff American, stay in America" and security requirements.

Subapplicants/subrecipients must submit short bios and resumes. This should include the type of entity, organizational leadership, and board members along with both the names and addresses of the individuals. Resumes are subject to approval.

D. Maximum Number of Applications

The maximum number of applications that can be submitted is: One (1) per state.

Nonprofit organizations must apply through their respective SAA. See the Eligible Entities section above for more information about the SAA, nonprofit organization, and applicant/subapplicant roles and responsibilities. For NSGP-UA and NSGP-S, consistent with prior years, each nonprofit organization may only represent one site/location/physical address per application. For example, a nonprofit organization with one site may apply for up to $200,000 for that site.

Nonprofit organizations with multiple sites, locations, or physical addresses may apply for funding for up to three sites per funding stream (NSGP-S and NSGP-UA), at a maximum of $200,000 per site, not to exceed $600,000 total per state. Nonprofit organizations with locations in multiple states may apply for up to three sites per funding stream in each state. For example, a nonprofit organization with sites in both NSGP-S and NSGP-UA areas within a state may apply for up to six sites, but the combined award total cannot exceed $600,000 per state.

Appendix B provides a table of eligible Urban Areas for FY 2026 applicable to the NSGP-UA funding stream. Nonprofit organizations located outside of these Urban Areas should apply under the NSGP-S program.

If a nonprofit subapplicant applies for projects at multiple sites, each site's application must include a vulnerability and risk assessment specific to that location, regardless of whether the projects are similar in nature. One vulnerability assessment is required per physical address. Failure to provide a unique assessment for each site may result in the rejection of the application.

E. Additional Restrictions

None

F. References to Other Eligibility Factors

Please see the following other eligibility references provided below:

1. "Threshold Review Criteria" subsection
2. "Financial Integrity Criteria" subsection
3. "Supplemental Financial Integrity Criteria and Review" subsection
4. FEMA may request financial information such as the Employer Identification Number (EIN) and bank information as part of the potential award selection. This will apply to everyone who benefits from the award, including subrecipients.

G. Cost Share Requirements

There is no cost share requirement for the FY 2026 NSGP.

H. Cost Share Description, Type, and Restrictions

Not applicable.

I. Cost Share Example

Not applicable.

J. Required Information for Verifying Cost Share

Not applicable.

(5) Maintenance of Effort

Not applicable.

3. Program Description

A. Program Purpose

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. These grant programs are 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 nonprofit organizations that are at risk of terrorist attack.

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.

NSGP reflects DHS's commitment to risk-informed investment, collaboration, and resilience. To ensure that priorities reflect the current threat environment, FEMA's Preparedness Grant Programs are guided by annually designated National Priority Areas (NPAs).

The FY 2026 NPAs did not change from FY 2025. They are:

1. Enhancing the protection of soft targets and crowded places. (This includes faith-based organizations and election sites)
2. Supporting Homeland Security Task Forces and fusion centers;
3. Enhancing and integrating cybersecurity resiliency;
4. Enhancing election security; and
5. Border Crisis Response and Enforcement Support.

For FY 2026, the Administration encourages applicants to propose innovative solutions that support the broader homeland security mission reflected in the NPAs, as applicable.

The NSGP has significantly contributed to the improvement and increase in the physical/cyber security and facility/target hardening of nonprofit organizations' facilities, ultimately safeguarding the lives and property of the American people. Nonprofit organizations tend to be high-profile and/or visible targets of group- or identity-based attacks because the populations affiliated with these organizations are usually members of a group with a shared identity (religious, ideological, mission-based, etc.). The frequency and severity of attacks – whether they are hate-based, group-based, opportunistic, or random – are increasing. The Federal Bureau of Investigation (FBI) reported more than 11,862 hate or bias-based attacks in 2023, an increase from previous years.

Nonprofit organizations tend to not have the resources, capital, or experience to secure facilities and implement costly and effective (i.e., state-of-the-art) security measures to protect the individuals who use their services or facilities from the increasing acts of violence perpetrated against populations who affiliate with these, often identity-based, nonprofits.

In FY 2025, the types of equipment nonprofit organizations requested and received the most NSGP funding for included:

1) Video assessment and security systems;
2) Impact resistant doors and gates;
3) Physical access control systems;
4) Jersey walls, fences, and other barriers; and
5) Fixed area lighting.

By providing crucial funding to high-risk non-profit organizations, the NSGP supports the ability of non-profit organizations to protect themselves and the individuals targeted by affiliation.

In the history of the program, over $2 billion has been allocated to nonprofit organizations and over 18,000 applications have been awarded. In recent years:

- NSGP emphasized the integration of preparedness activities of nonprofit organizations with broader state and local preparedness efforts.
- Funding priorities evolved to include spending Planning, Organizational, Equipment, Training, and Exercises (POETE) towards addressing the NPAs.

B. Goals and Objectives

This program will improve and increase the physical/cybersecurity and facility/target hardening of nonprofit organizations' facilities at risk of a terrorist of other extremist attack, ultimately safeguarding the lives and property of the American people. 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: NSGP, via SAAs, provides funds to nonprofit organizations that are at high 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.**
    - 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 on FY 2026 NSGP funding priorities.

2. **Address and close capability gaps that are identified in 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.**
    - 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.
    - Equipment– Strengthening security infrastructure, technology, and protective measures.
    - 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 agencies for a whole community approach to preparedness.**
    - 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 on FY 2026 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 2026 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:

- Enhancing Protection of Soft Targets/Crowded Places
- Supporting Homeland Security Task Forces and Fusion Centers
- Enhancing Cybersecurity
- Enhancing Election Security
- Supporting Border Crisis Response and Enforcement

Enduring needs include:

- Effective planning
- Training and awareness campaigns
- Equipment and capital projects
- 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 2026 NSGP Funding Priorities

All priorities reflected in this table align with the Safety and Security Lifelines.

Priority Areas	Core Capabilities Enhanced	Example Project Types
National Priorities		
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	▪ Private contracted security guards ▪ Physical security enhancements o Closed circuit television (CCTV) security cameras o Security screening equipment for people and baggage o Access controls ▪ Fencing, gates, barriers, etc. ▪ Card readers, associated hardware/software

Priority Areas	Core Capabilities Enhanced	Example Project Types
	activities ▪ Long-term vulnerability reduction ▪ Situational assessment ▪ Infrastructure systems	
Supporting Homeland Security Task Forces and Fusion Centers	▪ Intelligence and information sharing ▪ Interdiction and disruption ▪ Public information and warning ▪ Operational coordination ▪ Risk management for protection programs and activities	▪ 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 ▪ 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

Priority Areas	Core Capabilities Enhanced	Example Project Types
		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 Cybersecurity	▪ Cybersecurity ▪ Intelligence and Information Sharing ▪ Interdiction and disruption ▪ Long-term vulnerability reduction	▪ Cybersecurity enhancements o Risk-based cybersecurity planning and training o Improving cybersecurity of access control and identify verification systems o Improving cybersecurity of security technologies (e.g., CCTV systems) ▪ Adoption of cybersecurity performance goals (CISA's Cross-Sector Cybersecurity Performance Goals)
Enhancing Election Security	▪ Cybersecurity ▪ Intelligence and information sharing ▪ Planning ▪ Long-term vulnerability reduction ▪ Situational assessment	▪ 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 –

Priority Areas	Core Capabilities Enhanced	Example Project Types
	▪ Infrastructure systems ▪ Operational coordination ▪ Community resilience	e.g., locks, shatter proof glass, alarms, access controls, etc. ▪ General election security navigator support ▪ Cyber and 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 ▪ Public awareness/preparedness campaigns discussing election security and integrity measures ▪ Long-term vulnerability reduction and community resilience
Supporting Border Crisis Response and Enforcement	▪ Training and awareness ▪ 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,

Priority Areas	Core Capabilities Enhanced	Example Project Types
		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		
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: o Security plans and protocols o Emergency/contingency plans o Evacuation/shelter in place plans
Training & Awareness	▪ Long-term vulnerability reduction ▪ Public information and warning	▪ Active shooter training, including integrating the needs of persons with disabilities ▪ Security training for employees ▪ Public awareness/preparedness

Priority Areas	Core Capabilities Enhanced	Example Project Types
		campaigns
Exercises	▪ Long-term vulnerability reduction	▪ Response exercises

C. Performance Measures and Targets

FEMA will calculate and analyze the metrices through a review of recipient Biannual Strategy Implementation Report (BSIR) updates and award monitoring to ensure that the funds are expended for their intended purpose and achieve the stated outcomes in the grant application.

1. **Percentage of agreed-upon security personnel deployed by subrecipients to enhance visible deterrence and reduce threats at high-risk facilities.**

   Target: By 2029, ensure that 100% of agreed-upon contract security personnel hired by high-risk nonprofit subrecipients are using awarded funding.

2. **Percentage of cybersecurity vulnerabilities, equipment, or resources identified that were addressed.**

   Target: By 2029, achieve 100% of identified cybersecurity vulnerabilities, equipment or resource gaps that were successfully addressed by nonprofits organizations using NSGP funds.

3. **Performance Measure: Percentage of identified vulnerabilities addressed by nonprofit recipients through NSGP-funded security and safety projects, as described in vulnerability assessments.**

   Target: By 2029, ensure that 100% of high-risk nonprofits implement security and safety projects through the purchase or installation of equipment and technology to enhance or sustain facility hardening, strengthening their resilience against potential threats.

4. **Performance Measure: Percentage of preparedness activities (e.g. planning, awareness campaign, training, and exercises) implemented by each nonprofit.**

   Target: By 2029, ensure that 100% of nonprofits' preparedness activities outlined in the Investment Justification (IJ) are successfully implemented with annual incremental targets.

D. Federal Assistance Type

Grant

E. Program-Specific 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 Investment Justification (IJ);
- Initiatives in which federal agencies are the beneficiary or that enhance federal property;
- Initiatives which study technology development;
- Proof-of-concept initiatives; and
- Direct or indirect pass-through of benefits to non-eligible entities.

Note: The above list may not be exhaustive. Please consult the applicable terms and conditions and with FEMA for more information.

F. General Funding Requirements

Costs charged to federal awards (including federal and non-federal cost share funds) must comply with applicable statutes, rules and regulations, policies, this NOFO, 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)).

Recipients 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).

G. Prohibition on Covered Equipment or Services

FEMA provides additional resources regarding the prohibition on covered telecommunications equipment and services in its policy titled Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services (FEMA Policy #405-143-1). This policy outlines specific requirements related to the prohibition. Additionally, FEMA's Contract Provisions Guide offers sample language for the required contract provisions.

Recipients, 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. See 2 C.F.R. §§ 200.216, 200.327, 200.471, and Appendix II to 2 C.F.R. Part 200 for more information.

(1) Prohibition on Covered Foreign Unmanned Aircraft Systems (UAS)

Recipients, subrecipients, and their contractors or subcontractors must also comply with Section 1825 of the American Security Drone Act of 2023, enacted as part of the National Defense Authorization Act for Fiscal Year 2024 (Pub. L. No. 118-31 §§ 1821-33, 41 U.S.C. 3901 note prec.). This provision mandates that, beginning December 22, 2025, no federal funds awarded through a contract, grant, or cooperative agreement, or otherwise made available may be used to procure a covered unmanned aircraft system (UAS) that is manufactured or assembled by a covered foreign entity. Significantly, no funds may be used in connection with the operation of such a drone or UAS. For more information, refer to Public Law 118-31 and OMB Memorandum M-26-02, Ensuring Government Use of Secure Unmanned Aircraft Systems and Supporting United States Producers.

H. Beneficiary and Participant Eligibility

(2) Beneficiary

There are no program requirements. See Eligibility for additional information. This NOFO and any subsequent federal awards create no rights or causes of action for any beneficiary.

(3) Participant

There are no program requirements. This NOFO and any subsequent federal awards create no rights or causes of action for any participant.

This NOFO and any subsequent federal awards create no rights or causes of action for any beneficiary or participant. Please consult the DHS Standard Terms and Conditions, your awarding agency's terms and conditions, and your awarding documents for more details.

I. Indirect Costs

Indirect costs (IDC) are allowed for recipients and subrecipients.

IDC are costs incurred for a common or joint purpose benefiting more than one cost objective and not readily assignable to specific cost objectives without disproportionate effort. Applicants with a current negotiated IDC 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 IDC rate agreement. Applicants that are not required to have a 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 FEMA for further instructions. Applicants who wish to use a cost allocation plan in lieu of an IDC rate proposal must reach out to FEMA for further instructions. As it relates to the IDC for subrecipients, a recipient must follow the requirements of 2 C.F.R. §§ 200.332 and 200.414 in approving the IDC rate for subawards.

J. Budget Period

There will be only a single budget period with the same start and end dates as the period of performance.

K. Pre-Award Costs

Recipient (SAA) pre-award costs are allowable only with the prior written approval of DHS/FEMA and as included in the award agreement. To request pre-award costs, a written request must be included with the application signed by the SAA. The letter must outline what the pre-award costs are for, including a detailed budget break-out of pre-award costs from the post-award costs, and a justification for approval. Subrecipients cannot claim pre-award costs. Please contact your SAA should exigent circumstances exist.

L. Management and Administration Costs

Management and Administration (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 because 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.

Note: SAAs must be able to separately account for M&A costs associated with the NSGP-UA award from those associated with the NSGP-S award.

M&A costs are allowed under this program as described below:

1. SAA (Recipient) for NSGP-S and NSGP-UA M&A

The SAA may use and expend up to 5% of their total FY 2026 NSGP-S and NSGP-UA awards for M&A purposes associated with administering the NSGP-S and NSGP-UA awards. SAAs must include the amount they are requesting for NSGP-S and NSGP-UA M&A in the SF-424A form. The amount should be in addition to the total requested by the subapplicant nonprofit organizations but not exceed 5% of the total requested by the subapplicant nonprofit organizations. SAAs must be able to separately account for M&A costs associated with the NSGP-UA award from those associated with the NSGP-S.

2. Nonprofit Organization (subrecipient) for NSGP-S and NSGP-UA M&A

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 receives more than one subaward, they must be able to separately account for M&A costs for each subaward.

M. Authorizing Authority

Section 2009 of the *Homeland Security Act of 2002* (Pub. L. No. 107-296, as amended) (6 U.S.C. § 609a).

N. Appropriation Authority

Homeland Security and Further Additional Continuing Appropriations Act, *2026*, Pub. L. No. 119-86.

B. Step 2: Get Ready to Apply

In this step

Submission Requirements and Application Deadlines 22

1. Submission Requirements and Application Deadlines

A. Registration

You must have an active SAM.gov account which includes having a UEI. SAM.gov registration can take several weeks. Begin that process today.

For more detailed instructions for obtaining a UEI number or to register, go to SAM.gov Entity Registration and click "Get Started." From the same page, you can also click on the Entity Registration Checklist for the information you will need to register.

You must also have an active account with Grants.gov. You can see step-by step instructions see the Quick Start Guide for Applicants.

B. Requesting the Application Package

The application package is accessible in the FEMA Grants Outcomes (FEMA GO) system. To access the system, go to https://go.fema.gov/.

C. Application and Submission Instructions

To apply for an award under this program, all applicants must:

1. Apply for, update, or verify their UEI number and EIN from the Internal Revenue Service;
2. Provide their UEI number in the application;
3. Have an account with login.gov;
4. Register for, update, or verify their SAM.gov account and ensure the account is active before submitting the application;
5. Register in FEMA GO, add the organization to the system, and establish the Authorized Organizational Representative (AOR). The organization's electronic business point of contact (eBiz POC) from the SAM registration may need to be involved in this step. For step-by-step instructions, see the FEMA GO Startup Guide;
6. Submit the complete application in FEMA GO; and
7. Always maintain an active SAM registration with current information during which the applicant has an active federal award, an application, or plan under consideration by a federal awarding agency. As part of this, applicants must also provide information on an applicant's immediate and highest-level owner and subsidiaries, as well as on all predecessors that have been awarded federal contracts or federal financial assistance within the last three years, if applicable.

Per 2 C.F.R. 25.110(a)(2)(iv), if an applicant is experiencing exigent circumstances that prevents it from obtaining an UEI number and completing SAM registration prior to receiving a federal award, the applicant must notify FEMA as soon as possible. Contact fema-grants-news@fema.dhs.gov and provide the details of the exigent circumstances.

D. How to Register to Apply

(1) General Instructions

Registering and applying for an award under this program is a multi-step process and requires time to complete. Below are instructions for registering to apply for FEMA funds. Read the instructions carefully and prepare the requested information before beginning the registration process. Gathering the required information before starting the process will alleviate last-minute searches for required information.

The registration process can take up to four weeks to complete. To ensure an application meets the deadline, applicants are advised to start the required steps well in advance of their submission. Organizations must have a UEI number, EIN, and an active SAM registration.

(2) Obtain a UEI Number

All entities applying for funding, including renewal funding, must have a UEI number.

(3) Obtain Employer Identification Number

In addition to having a UEI number, all entities applying for funding must provide an EIN. The EIN can be obtained from the IRS at Get an employer identification number.

(4) Create a login.gov account

Applicants must have a login.gov account to register with SAM or update their SAM registration. Applicants can create a login.gov account at Create an account.

Applicants only have to create a login.gov account once. For existing SAM users, use the same email address for both login.gov and SAM.gov so that the two accounts can be linked.

For more information on the login.gov requirements for SAM registration, refer to SAM.gov.

(5) Register with SAM.gov

In addition to having a UEI number, all organizations must register with SAM.gov. Failure to register with SAM.gov will prevent your organization from applying through FEMA GO. SAM.gov registration must be renewed annually and must remain active throughout the entire grant life cycle.

For more detailed instructions for registering with SAM.gov, refer to Register with SAM.gov.

Note: per 2 C.F.R. § 25.200 applicants must also provide the applicant's immediate and highest-level owner, subsidiaries, and predecessors that have been awarded federal contracts or federal financial assistance, applicants must also provide the applicant's immediate and highest-level owner, subsidiaries, and predecessors that have been awarded federal contracts or federal financial assistance within the past three years, if applicable.

(6) Register in FEMA GO, Add the Organization to the System, and Establish the AOR

Applicants must register in FEMA GO and add their organization to the system. The organization's

electronic business point of contact (eBiz POC) from the SAM.gov registration may need to be involved in this step. For step-by-step instructions, see the FEMA GO Startup Guide.
Note: FEMA GO will support only the most recent major release of the following browsers:

- Google Chrome;
- Mozilla Firefox;
- Apple Safari; and
- Microsoft Edge.

Applicants using tablet type devices or other browsers may encounter issues with using FEMA GO.

E. Submitting the Final Application

Applicants will be prompted to submit the standard application information, and any program-specific information required in FEMA GO.

After submitting the final application, FEMA GO will provide either an error message or send an email to the submitting AOR confirming the transmission was successfully received.

F. Application Deadline

July 24, 2026 11:59 p.m. Eastern Time

G. Pre-Application Requirements Deadline

Not applicable.

H. Post Application Requirements Deadline

Not applicable.

I. Effects of Missing Deadlines

All applications must be completed in FEMA GO by the application deadline. FEMA GO automatically records proof of submission and generates an electronic date/time stamp when FEMA GO successfully receives an application. The submitting AOR will receive an email with an official date/time stamp and a FEMA GO tracking number to serve as proof of timely submission prior to the application deadline.

Applicants experiencing system-related issues have until 3 p.m. ET on the date applications are due to notify FEMA. No new system-related issues will be addressed after this deadline. Applications not received by the application submission deadline will not be accepted.

C. Step 3: Write Your Application

In this step

Application contents and format 26

1. Application Contents and Format

A. Application Requirements

The following forms or information are integrated into the application package in FEMA GO. Applicants should review these forms at SF-424 Family | Grants.gov before applying to ensure they are providing all required information.

1. SF-424, Application for Federal Assistance
2. Grants.gov Lobbying Form, Certification Regarding Lobbying
3. SF-424A, Budget Information (Non-Construction)
   - If construction is permitted under the program, submit SF-424C, Budget Information (Construction), instead of SF-424A
4. SF-424B, Standard Assurances (Non-Construction)
   - If construction is permitted under the program, submit SF-424D, Standard Assurances (Construction), instead of SF-424B
5. SF-LLL, Disclosure of Lobbying Activities

B. Required Documents, Content, and Formatting

Applications must be submitted in FEMA GO by the SAA ONLY. To begin, visit Grants.gov and search for the NSGP posting. Download the necessary documents from the Related Documents tab. Complete all forms accurately and ensure they are clearly labeled. Save the completed forms, then log in to FEMA GO and upload the required documents as part of your application submission.

C. Program-Specific Required Documents and Information

The following program-specific forms or information are required to be submitted in FEMA GO *following award to the applicable SAA and before any subawards are approved/issued*:

- Investment Justifications (IJ) from **ALL** nonprofit subapplicants must be submitted, regardless of whether the SAA recommends them for funding, using the FY 2026 IJ Template (Office of Management and Budget (OMB) Control Number: 1660-0110/FEMA Form FF-207-FY-21-115).
- SAA Prioritization of IJs must be completed using the DHS/FEMA-provided template (OMB Control Number: 1660-0110/FEMA Form FF 207-21-114) available in the Related Documents tab of the Grants.gov posting:
  - SAAs **must** include application details for each nonprofit organization that applied for funding (e.g., nonprofit organization name, IJ title(s), requested amount(s)) on the State Prioritization of IJs, even if the organization is not recommended by the SAA for funding.
  - IJs for applications not recommended for funding must be submitted to FEMA**.**
  - Each nonprofit organization recommended for funding must be scored and assigned a unique rank (one [1] being the highest ranked, continuing sequentially through the total number of applications scored by the SAA).
  - States with multiple FY 2026 designated high-risk urban areas must ensure that nonprofits organizations are ranked separately within each high-risk urban area. For example, if a state has three high-risk urban areas, there should be three distinct groups of rankings.

As part of the FY 2026 NSGP application, each eligible nonprofit subapplicant must submit the following three documents to the SAA by the SAA's established deadline:

1. ***NSGP IJ***
   Nonprofit subapplicants with one site may apply for up to $200,000 for that site. Nonprofit subapplicants with multiple sites may apply for up to $200,000 per site, for up to three sites per funding stream, with a maximum of $600,000 per state. See Eligibility, Section D. for more information about this maximum. If applying for multiple sites, a nonprofit subapplicant must submit a separate, complete IJ for each site. IJs cannot include more than one physical site.

   A fillable IJ form (DHS/FEMA Form FF-207-FY-21-115, OMB Control Number: 1660-0110) is available in the Related Documents tab of the Grants.gov NSGP posting. Each IJ must describe the investment proposed for funding. The investments or projects described in the IJ must:
   - Be for the location(s)/physical address(es) (NOT P.O. Boxes) that the nonprofit occupies at the time of application;
   - Address an identified risk, including threat and vulnerability, regardless of whether similar projects are submitted 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 three-year period of performance; and
   - Be consistent with all applicable requirements outlined in this NOFO and the Preparedness Grants Manual.

   More information about the IJ's content and scoring is listed in Appendix D.

   Nonprofit subapplicants are required to self-identify with one of the following categories in the IJ as part of the application process:
   - Ideology-based/Spiritual/Religious (Houses of Worship, Educational Institutions, Medical Facilities, etc.)
   - Educational (secular)
   - Medical (secular)
   - Other

2. ***Vulnerability/Risk Assessment***
   Each nonprofit subapplicant must include a site-specific vulnerability/risk assessment **unique to the site** for which the IJ is submitted.

3. ***Mission Statement***
   Each nonprofit subapplicant must include its Mission Statement and any mission implementation policies or practices that may elevate the organization's risk. SAAs will use the Mission Statement along with the nonprofit subapplicant's self-identification in the IJ to validate that the organization is one of the following types: 1) Ideology-based/Spiritual/Religious; 2) Educational; 3) Medical; or 4) Other. The organization type is a factor when calculating the final score of the application; see

Application Review Information, subsection “Final Score.”

The Vulnerability/Risk Assessment and Mission Statement are not to be submitted in FEMA GO but should be maintained by the SAA and must be made available to DHS/FEMA upon request.

D. Post-Application Requirements for Successful Applicants

1. **Grant Agreement and Acceptance:** Recipients must review, sign, and return the grant agreement to formalize acceptance of the award and its terms.
2. **Additional Application Material:** With FEMA's approval, applicants may submit certain required information post award. For detailed guidance, please refer to the award letter or contact your assigned FEMA Head Quarters (HQ) Preparedness Officer.
3. **General Information About Post-Federal Award Reporting Requirements:** Award recipients must submit the following reports: quarterly financial reports, semi-annual performance reports and BSIR submissions, final financial and performance reports, and an annual audit report (if required). These must follow the Part 200 Uniform Requirements or specific conditions of the award. If reports are late, future funding or fund access may be delayed, and additional reports may be requested in some cases.

D. Step 4: Learn about the Award Review Process

In this step

Application Review Information 30

Intergovernmental Review 35

1. Application Review Information

A. Threshold Criteria

Subapplicants will be disqualified if they: submit incomplete subapplication packages; are administratively noncompliant (e.g., scanned IJs, incorrect or previous year forms); have a history of poor performance in grant administration; apply for the wrong funding stream; and/or are deemed an ineligible organization.

B. Application Criteria

1. **Programmatic Criteria** (See Appendix D for Evaluation Criteria and Scoring Matrix)
   Nonprofit organizations must submit their FY 2026 NSGP applications to their respective SAA by the deadline established by the SAA. If an SAA has established a deadline that is prior to release of the FY 2026 NSGP funding notice, the SAA is responsible for working with any nonprofits that may need to amend their submissions to account for changes in the FY 2026 NSGP program prior to the start of the SAA application evaluation process. FY 2026 NSGP-S and NSGP-UA 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 FY 2026 NSGP-S and NSGP-UA SAAs will make recommendations to DHS/FEMA based on their allocation and according to the chart listed in the respective process subsection below.

   The following are the FY 2026 NSGP-S and NSGP-UA evaluation process and criteria:
   - For NSGP-UA, state and federal verification that the nonprofit organization is located within one of the FY 2026 Designated high-risk urban areas (contact the appropriate SAA for the UAWG-defined high-risk urban area footprints); and for NSPG-S, verification that the nonprofit is located outside of one of the FY 2026 designated high-risk urban areas;
   - Identification and substantiation of current or persistent threats or attacks (from within or outside the United States) by a terrorist or other extremist organization, network, or cell against the subapplicant based on their ideology, beliefs, and/or mission as: 1) an ideology-based/spiritual/religious; 2) educational; 3) medical; or 4) other nonprofit entity;
   - Symbolic value of the site(s) as a highly recognized regional and/or national or historical institution(s) that renders the site a possible target of terrorist or other extremist attacks;
   - Role of the nonprofit organization in responding to or recovering from terrorist or other extremist attacks;
   - Alignment between the project activities requested within the physical or cyber vulnerabilities identified in the organization's vulnerability assessment;
   - Integration of nonprofit preparedness with broader state and local preparedness efforts;
   - Completed IJ for each site that addresses an identified risk unique to that site, including the assessed threat, vulnerability, and consequence of the risk; and
   - History of prior funding under NSGP. Not having received prior year NSGP funding is a positive factor when calculating the state score of the application; see Application Review Information – Review and Selection Process, for additional information.

   Grant projects must be: 1) both feasible and effective at mitigating the identified vulnerability and

thus reducing the risks for which the project was designed; and 2) able to be fully completed within the three-year period of performance. DHS/FEMA will use the information provided in the application, as well as any supporting documentation, to determine the feasibility and effectiveness of the grant project. Information that would assist in the feasibility and effectiveness determination includes the following:

- Scope of work (purpose and objectives of the project, identification of what is being protected);
- Desired outcomes, including expected long-term impact where applicable;
- Summary of status of planning and design accomplished to date (e.g., included in a capital improvement plan); and
- Project schedule.

Recipients and subrecipients are expected to conform, as applicable, with accepted engineering practices, established codes, standards, modeling techniques, and best practices.

2. **Final Score**

To calculate an application's final score, the subapplicant's SAA score will be multiplied:

- By a factor of three for ideology-based/spiritual/religious entities (Houses of Worship, Educational Institutions, Medical Facilities, etc.);
- By a factor of two for secular medical and educational institutions; and
- By a factor of one for all other nonprofit organizations.

Subapplicants who have never received a NSGP award will have 15 points added to their score.

3. **Security Review**

DHS receives a list of potential NSGP subrecipient organizations, which it reviews against U.S. intelligence community reporting. The security review occurs after the competitive scoring and selection process is complete. The information provided for the security review is limited to the nonprofit organization's name and physical address, as submitted by the nonprofit organization. Any potentially derogatory information, as well as any potentially mitigating information, that could assist in determining whether a security risk exists is sent to FEMA and is used in making final award decisions.

C. Financial Integrity Criteria

Before making an award, the awarding agency is required to review OMB-designated databases for applicants' eligibility and financial integrity information. This is required by the Payment Integrity Information Act of 2019 (Pub. L. No. 116-117, § 2 (2020), 41 U.S.C. § 2313, and the "Do Not Pay Initiative" (31 U.S.C. 3354). For more details, please see 2 C.F.R. § 200.206.

Thus, the Financial Integrity Criteria may include the following risk-based considerations of the applicant:

1. Financial stability.
2. Quality of management systems and ability to meet management standards.

3. History of performance in managing federal award.
4. Reports and findings from audits.
5. Ability to effectively implement statutory, regulatory, or other requirements.

D. Supplemental Financial Integrity Criteria and Risk Review

Before making an award expected to exceed the simplified acquisition threshold, defined at 41 U.S.C. § 134, over the period of performance:

1. The awarding agency is required by 41 U.S.C. § 2313 to review or consider certain information found in SAM.gov. For details, please see 2 C.F.R. § 200.206(a)(2).
2. An applicant may review and comment on any information in the responsibility/qualification records available in SAM.gov.
3. Before making decisions in the risk review required by 2 C.F.R. § 200.206, the awarding agency will consider any comments by the applicant.

E. Reviewer Selection

NSGP subapplications undergo a two-tiered review process. The SAAs review, score, and rank all submitted subapplications. FEMA then reviews all subapplications recommended by the SAA for Federal Review. FEMA's review is conducted by the FEMA Grant Programs Directorate (GPD) Homeland Security Programs Division's Branch Chiefs, Section Chiefs, and Preparedness Officers, who receive comprehensive training on evaluation criteria to ensure consistency and fairness. To uphold impartiality, FEMA enforces strict conflict of interest policies, requiring reviewers to disclose any potential conflicts prior to participation. This rigorous process ensures that funding decisions are thorough and unbiased.

F. Merit Review Process

In the NSGP Federal Review, the SAAs' score is multiplied by the applicable multiplier and bonus points are added based on first-time status. The scoring matrix the SAAs use is found in Appendix D of this NOFO. IJs are also reviewed to identify any unallowable expenses or projects/activities, with costs disallowed or placed on hold as necessary. Subapplications are selected for funding in descending order, starting with the highest-scored subapplications, until the available funds are allocated. Additional information on this process can be found in the Review and Selection Section of this NOFO. This merit-based selection process ensures that funding is directed to the most promising and highest risk subapplications.

a. Review and Selection Process

1. NSGP-UA Process

Urban Area Review

Application packages are submitted by the nonprofit organization to the SAA based on the established criteria. As part of the review for NSGP-UA, the SAAs must:

- Conduct an eligibility review in coordination with the UAWG;
- Verify that the nonprofit is located within a FY 2026 designated high-risk urban area;
- Review and score only complete application packages (including mission statements and vulnerability assessments) using the NSGP Scoring Criteria provided by DHS/FEMA;

- Validate the self-certified organization type listed in the IJ by assessing the central purpose of the organization described in the mission statement;
- Prioritize all NSGP IJs by ranking each IJ. Each IJ will receive a unique rank (one [1] being the highest ranked, continuing sequentially through the total number of applications scored by the SAA);
- For states with multiple FY 2026 designated high-risk urban areas, each high-risk urban area must be ranked separately;
- Submit the results of the SAA review of complete applications from eligible subapplicants to DHS/FEMA using the SAA Prioritization Tracker;
- Submit nonprofit organization application details for applications received but not recommended for funding (including incomplete applications and ineligible subapplicants), as well as justification as to why they are not being recommended for funding to DHS/FEMA using the SAA Prioritization Tracker;
- Submit IJs that are recommended for funding; SAAs should submit IJs that collectively represent 150% of the state's NSGP-UA allocation; this will allow DHS/FEMA to award the next prioritized IJ in instances when a subapplicant is found to be ineligible or when a significant portion of an IJ includes proposed projects that are unallowable, for example:

NSGP-UA Allocation	Submit IJs That Total This Amount to DHS/FEMA
$1.5 million	$ 2.25 million
$ 2 million	$ 3 million
$ 2.5 million	$ 3.75 million

- Submit IJs received and not recommended for funding, including incomplete IJs and IJs from subapplicants deemed ineligible; and
- Retain the mission statements and vulnerability assessments submitted by each nonprofit organization.

The SAA will base the ranking on the final scores from the Prioritization Tracker as determined by the SAA's subject-matter expertise and discretion with consideration of the following factors:

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

The SAA reviewers will score each question in the IJ according to the scoring matrix in Appendix D.

Federal Review

The highest-ranking IJs received from each high-risk urban area are reviewed by a panel made

up of DHS/FEMA federal staff. As a part of this review, federal staff will also verify that the nonprofit is located within a FY 2026 designated high-risk urban area.

Federal reviewers will review each IJ to check for the following:

- Eligibility (e.g., that a potential subrecipient meets all the criteria for the program);
- Allowability of the proposed project(s); and
- Any derogatory information on the organization applying per Security Review.

2. NSGP-S Process

State Review

Application packages are submitted by the nonprofit organization to the SAA based on the established criteria. The SAA will review applications and recommend to DHS/FEMA which nonprofit organizations should be selected for funding. As part of the state review, the SAAs must:

- Conduct an eligibility review;
- Verify that the nonprofit is located outside a FY 2026 designated high-risk urban area;
- Review and score all complete application packages (including vulnerability assessments and mission statement) using the NSGP Scoring Criteria provided by DHS/FEMA;
- Validate the self-certified organization type listed in the IJ by assessing the central purpose of the organization described in the mission statement;
- Prioritize all NSGP IJs by ranking each IJ. Each IJ will receive a unique rank (one [1] being the highest ranked, continuing sequentially through the total number of applications scored by the SAA);
- Submit the results of the state review along with complete IJs from eligible subapplicants to DHS/FEMA using the SAA Prioritization Tracker;
- Submit nonprofit organization application details for applications received but not recommended for funding (including incomplete and ineligible subapplicants), as well as justification as to why they are not being recommended for funding to DHS/FEMA using the SAA Prioritization Tracker;
- Submit IJs that are recommended for funding; SAAs should submit IJs that collectively represent 150% of the state's NSGP-S allocation; this will allow DHS/FEMA to award the next prioritized IJ in instances when a subapplicant is found to be ineligible or when a significant portion of an IJ includes proposed projects that are unallowable, for example:

NSGP-S Allocation	Submit IJs That Total This Amount to DHS/FEMA
$1.5 million	$ 2.25 million
$ 2 million	$ 3 million
$ 2.5 million	$ 3.75 million

- Submit IJs received and not recommended for funding, including incomplete IJs and IJs from subapplicants deemed ineligible.
- Retain the mission statements and vulnerability assessments submitted by each nonprofit

organization.

The SAA will base the ranking on the final scores from the Prioritization Tracker as determined by the SAA's subject-matter expertise and discretion with consideration of the following factors:

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

The SAA reviewers will score each question in the IJ according to the scoring matrix in Appendix D.

Federal Review

The IJs submitted by each SAA will be reviewed by DHS/FEMA federal staff. Federal staff will also verify that the nonprofit organization is located outside of a FY 2026 designated high-risk urban area. Federal reviewers will review each IJ to check for the following:

- Eligibility (e.g., that a potential subrecipient meets all the criteria for the program);
- Allowability of the proposed project(s); and
- Any derogatory information on the organization applying per Security Review.

G. Final Selection

For NSGP, the determination is made using Final Score (SAA Score * Multiplier + Bonus Points). In both NSGP-S and NSGP-UA, subapplications are compared to those within the same State or Territory. The highest scored subapplication in a State and UA is selected for funding first and selection proceeds in descending order until the state reaches its allocation. In the event of a tie, preference is given to first-time recipients, followed by the SAA ranking.

Subapplicants will be selected from highest to lowest scored within their respective state/territory or urban area until the available state/urban area allocation has been exhausted. In the event of a tie during the funding determination process, priority will be given to nonprofit organizations that have not received prior year funding, and then those prioritized highest by their SAA. Should a state/territory fail to meet their published allocation, the remaining balance will not be reallocated.

DHS/FEMA will use the results to make funding recommendations for subawards to the Secretary of Homeland Security. All final funding determinations for subawards will be made by the Secretary of Homeland Security, who retains the discretion to consider other factors and information in addition to DHS/FEMA's funding recommendations.

2. Intergovernmental Review

A. Requirement Description and State Single Point of Contact

An intergovernmental review may be required. Applicants must contact their state's Single Point of Contact (SPOC) to comply with the state's process under Executive Order 12372. No further action is

needed if you do not find a contact for your state in the latest version of the SPOC list.

Note: This requirement does not apply to tribal governments.

E. Step 5: Learn What Happens After Award

In this step

Award Notices 38

Post-award requirements and administration 39

Other 48

1. Award Notices

A. Notice of Award

The AOR should carefully read the federal award package before accepting the federal award. The federal award package includes instructions on administering the federal award as well as terms and conditions for the award.

By applying, applicants agree to comply with the prerequisites stated in this NOFO and the material terms and conditions of the federal award, should they receive an award.

FEMA will provide the federal award package to the applicant electronically in FEMA GO. Award packages include an Award Letter, Summary Award Memo, Agreement Articles, and Obligating Document. An award package notification email is sent by the grant application system to the submitting AOR.

Recipients must accept their awards no later than 60 days from the award date. Recipients shall notify FEMA of their intent to accept the award and proceed with work in the FEMA GO system.

Funds will remain on hold until the recipient accepts the award in FEMA GO and all other conditions of the award have been satisfied, or until the award is otherwise rescinded. Failure to accept a grant award within the specified timeframe may result in a loss of funds.

B. Pass-Through Requirements

Pass-through funding is required under this program. For more information, please see the Preparedness Grants Manual.

C. Note Regarding Pre-Award Costs

Even if pre-award costs are allowed, beginning performance prior to award is at the applicant or sub-applicant's own risk.

D. Obligation of Funds

The grant funds are obligated in accordance with applicable laws, and no later than upon award.

E. Notification to Unsuccessful Applicants

SAAs are required to inform nonprofit organization subapplicants of their non-selection. FEMA will provide an optional template that SAAs can use; however, SAAs can modify this template as needed. SAAs are required to inform subapplicants of their non-selection no later than 90 days from the date they accept their NSGP award.

2. Post-Award Requirements and Administration

A. Administrative and National Policy Requirements

(1) Presidential Executive Orders

Recipients 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.

Pursuant to the preliminary injunction order issued on November 21, 2025, in County of Santa Clara et al. v. Noem, et al., No. 25-cv-08330-WHO (N.D. Cal.), this requirement does not apply to awards or subawards issued to any of the plaintiffs subject to the preliminary injunction order while the order remains in effect. If the preliminary injunction is extended to cover additional plaintiffs, this provision will also not apply to any awards or subawards issued to those plaintiffs. If the preliminary injunction is stayed, vacated, or extinguished, this requirement will immediately become effective. Also, pursuant to the preliminary injunction order issued on November 21, 2025, in City of Chicago et al. v. Noem, et al., No. 25-CV-12765 (N.D. Ill.), this requirement does not apply to awards or subawards issued to any of the plaintiffs subject to the preliminary injunction order while the order remains in effect. If the preliminary injunction is extended to cover additional plaintiffs, this provision will also not apply to any awards or subawards issued to those plaintiffs. If the preliminary injunction is stayed, vacated, or extinguished, this requirement will immediately become effective.

In accordance with Executive Order 14305, Restoring American Airspace Sovereignty (June 6, 2025), and to the extent allowed by law, eligible state, local, tribal, and territorial grant recipients under this NOFO are permitted to purchase unmanned aircraft systems, otherwise known as drones, or equipment or services for the detection, tracking, or identification of drones and drone signals, consistent with the legal authorities of state, local, tribal, and territorial agencies. Recipients must comply with all applicable federal, state, and local laws and regulations, and adhere to any statutory requirements on the use of federal funds for such unmanned aircraft systems, equipment, or services.

(2) Subrecipient Monitoring and Management

Pass-through entities must comply with the requirements for subrecipient monitoring and management as set forth in 2 C.F.R. §§ 200.331-333.

(3) Termination of a Federal Award

1. The termination condition below applies to the grant award and the “Termination of a Federal Award” term and condition in the FY 2026 DHS Standard Terms and Conditions does not.

2. Termination of the federal award by FEMA
   FEMA, in its sole discretion, may terminate the federal award in whole or in part for one of the following reasons consistent with 2 C.F.R. § 200.340:

a. If the recipient or subrecipient fails to comply with the terms and conditions of the federal award.
b. With the consent of the recipient, in which case FEMA and the recipient must agree upon the termination conditions. These conditions include the effective date and, in the case of partial termination, the portion to be terminated.
c. If the federal award no longer effectuates the program goals or agency priorities. Under this provision, FEMA may terminate the award for these purposes if any of the following reasons apply:
    i. FEMA determines that a specific award objective is ineffective at achieving program goals as described in this NOFO;
    ii. FEMA determines that an objective of the award as described in this NOFO will be ineffective at achieving program goals or agency priorities;
    iii. FEMA determines that the design of the grant program is flawed relative to program goals or agency priorities;
    iv. FEMA determines that the grant program is not aligned to either the DHS Strategic Plan, the FEMA Strategic Plan, or successor policies or documents;
    v. FEMA changes or re-evaluates the goals or priorities of the grant program and determines that the award will be ineffective at achieving the updated program goals or agency priorities; or
    vi. For other reasons based on program goals or agency priorities described in the termination notice provided to the recipient pursuant to 2 C.F.R. § 200.341.
d. For convenience, including if the award no longer advances the national interest. Termination for convenience only applies to discretionary awards, as that term is defined at 2 C.F.R. § 200.1. The term "discretionary award" does not include grants where legislation establishes an entitlement to the funds on the part of the recipient, such as block grants or those awarded based on a statutory formula.

3. Termination of a Subaward by the Pass-Through Entity
    a. The pass-through entity may terminate a subaward in whole or in part for one of the following reasons identified in 2 C.F.R. § 200.340:
        i. If the subrecipient fails to comply with the terms and conditions of the federal award.
        ii. With the consent of the subrecipient, in which case the pass-through entity and the subrecipient must agree upon the termination conditions. These conditions include the effective date and, in the case of partial termination, the portion to be terminated.
    b. If the pass-through entity's award has been terminated the pass-through entity must terminate its subawards.

4. Termination by the Recipient or Subrecipient
The recipient or subrecipient may terminate the federal award in whole or in part as identified in 2 C.F.R. § 200.340 upon sending FEMA or pass-through entity a written notification of the reasons for such termination, the effective date, and, in the case of partial termination, the portion to be terminated. However, if FEMA or pass-through entity determines that the remaining portion of the federal award will not accomplish the purposes for which the federal award was made, FEMA or pass-through entity may terminate the federal award in its entirety.

5. Impacts of Termination
   a. When FEMA terminates the federal award in whole or in part before the end of the period of performance due to the recipient's or subrecipient's material failure to comply with the terms and conditions of the federal award, FEMA will report the termination in SAM.gov in the manner described at 2 C.F.R. § 200.340(c).
   b. When the federal award is terminated in part or its entirety, FEMA or pass-through entity and recipient or subrecipient remain responsible for compliance with the requirements in 2 C.F.R. §§ 200.344 and 200.345.

6. Notification requirements
   FEMA or the pass-through entity must provide written notice of the termination in a manner consistent with 2 C.F.R. § 200.341. The federal award will be terminated on the date of the notification unless stated otherwise in the notification.

7. Opportunities to Object and Appeals
   Where applicable, when FEMA terminates the federal award, the written notification of termination will provide the opportunity and describe the process to object and provide information challenging the action, pursuant to 2 C.F.R. § 200.342.

8. Effects of Suspension and Termination
   The allowability of costs to the recipient or subrecipient resulting from financial obligations incurred by the recipient or subrecipient during a suspension or after the termination of a federal award are subject to 2 C.F.R. § 200.343.

B. DHS Standard Terms and Conditions

A recipient under this funding opportunity must comply with the DHS Standard Terms and Conditions in effect as of the federal award, unless a term and condition specifically indicates otherwise. The DHS Standard Terms and Conditions are available online and can be found at DHS Standard Terms and Conditions | Homeland Security. For continuation awards, the terms and conditions for the initial federal award will apply unless otherwise specified in the terms and conditions of the continuation award. The specific version of the DHS Standard Terms and Conditions applicable to the federal award will be in the federal award package.

A recipient under this funding opportunity must comply with the FY 2026 Department of Homeland Security Standard Terms and Conditions, with the following exceptions. The term titled "Communication and Cooperation with the Department of Homeland Security and Immigration Officials" and paragraph (2)(a)(ii) of the term titled "Federal Anti-Discrimination Laws Material to the Government's Payment Decisions Under the False Claims Act" do not apply to any federal award under this funding opportunity.

Pursuant to the preliminary injunction order issued on November 21, 2025, in County of Santa Clara et al. v. Noem, et al., No. 25-cv-08330-WHO (N.D. Cal.), the following terms and conditions do not apply to awards or subawards issued to any of the plaintiffs subject to the preliminary injunction order while the order remains in effect: (1) The DHS Standard Term and Condition titled " Federal Anti-Discrimination Laws Material to the Government's Payment Decisions Under the False Claims Act "; and (2) the DHS Standard Term and Condition titled "All Executive Orders Related to Grants". If the

preliminary injunction is extended to cover additional plaintiffs, this provision will also not apply to any awards or subawards issued to those plaintiffs. If the preliminary injunction is stayed, vacated, or extinguished, both terms will immediately become effective. As stated above, Paragraph (2)(a)(ii) of the DHS Standard Term and Condition titled "Federal Anti-Discrimination Laws Material to the Government's Payment Decisions Under the False Claims Act" will not apply even if the preliminary injunction is stayed, vacated, or extinguished.

Pursuant to the preliminary injunction order issued on November 21, 2025, in City of Chicago et al. v. Noem, et al., No. 25-CV-12765 (N.D. Ill.), the following terms and conditions do not apply to awards or subawards issued to any of the plaintiffs subject to the preliminary injunction order while the order remains in effect: (1) the DHS Standard Term and Condition titled " Federal Anti-Discrimination Laws Material to the Government's Payment Decisions Under the False Claims Act"; and (2) the DHS Standard Term and Condition titled " All Executive Orders Related to Grants". If the preliminary injunction is extended to cover additional plaintiffs, this provision will also not apply to any awards or subawards issued to those plaintiffs. If the preliminary injunction is stayed, vacated, or extinguished, both terms will immediately become effective. As stated above, paragraph (2)(a)(ii) of the DHS Standard Term and Condition titled "Federal Anti-Discrimination Laws Material to the Government's Payment Decisions Under the False Claims Act" will not apply even if the preliminary injunction is stayed, vacated, or extinguished.

Pursuant to the preliminary injunction order issued on October 31, 2025, in City of Seattle v. Trump, et al., No. 2:25-cv-01435-BJR (W.D. Wa.), the following terms and conditions do not apply to awards or subawards issued to any of the plaintiffs subject to the preliminary injunction order while the order remains in effect: the DHS Standard Term and Condition titled " Federal Anti-Discrimination Laws Material to the Government's Payment Decisions Under the False Claims Act ". If the preliminary injunction is extended to cover additional plaintiffs, this provision will also not apply to any awards or subawards issued to those plaintiffs. If the preliminary injunction is stayed, vacated, or extinguished, the term will immediately become effective. As stated above, paragraph (2)(a)(ii) the DHS Standard Term and Condition titled "Federal Anti-Discrimination Laws Material to the Government's Payment Decisions Under the False Claims Act" will not apply even if the preliminary injunction is stayed, vacated, or extinguished.

Note: While not a requirement in the DHS Standard Terms and Conditions, as a best practice, entities receiving funds through this program should ensure that cybersecurity is integrated into the design, development, operation, and maintenance of investments that impact information technology (IT) and/ or operational technology (OT) systems.

Additionally, the recipient and subrecipient must take reasonable cybersecurity and other measures to safeguard information including protected personally identifiable information (PII) and other types of information per 2 C.F.R. § 200.303(e).

C. Financial Reporting Requirements

Recipients must report obligations and expenditures through a federal financial report. The Federal Financial Report (FFR) form, also known as SF-425, is integrated in FEMA GO but, for reference, is available online at Post-Award Reporting Forms.

Recipients must submit the FFR quarterly, throughout the period of performance (POP) as detailed below:

Reporting Period	Report Due Date
October 01 – December 31	January 30
January 01 – March 31	April 30
April 01 – June 30	July 30
July 01 – September 30	October 30

The final FFR is due within 120 calendar days after the end of the POP.

FEMA may withhold future federal awards and cash payments if FFRs are not timely, complete, detailed, and accurate. FFRs showing inadequate progress may also cause future federal awards and cash payments to be withheld.

D. Programmatic Performance Reporting Requirements

As of FY 2024, recipients are only responsible for completing and submitting the now referenced Biannual Strategy Implementation Report (BSIR) Snapshot through FEMA GO on a bi-annual basis. The former Performance Progress Report (PPR) is no longer required. The FEMA GO system is configured to allow the entry and updating of project-level details throughout the life of an award. The FEMA GO system automatically generates the BSIR on January 1 and July 1 of each year. The BSIR provides a snapshot of project-level details entered and approved in FEMA GO as of December 30 and June 30 of the previous reporting period.

The BSIR Snapshot is due within 30 days after the end of the reporting period: July 30 for the reporting period of Jan. 1 through June 30 (summer BSIR report); and Jan. 30 for the reporting period of July 1 through December 31 (winter BSIR report). All required attributes of each project must be included. Updated obligations, expenditures, and significant developments must be provided within the BSIR Snapshot to show the progress of implementation for every project as well as how expenditures support Planning, Organization, Equipment, Training, and Exercises.

1. A Performance Report must be submitted bi-annually throughout the POP.
2. A Performance Report must include updated obligations, expenditures, and significant developments to show the progress of implementation for every project as well as how expenditures support Planning, Organization, Equipment, Training, and Exercises.
3. The Progress Report must be submitted through FEMA GO.
4. Performance Report Due Dates are as detailed below:

Reporting Period	Report Due Date
January 01 - December 31	January 30

E. Closeout Reporting Requirements

Within 120 days after the end of the period of performance, or after an amendment has been issued to close out a federal award, recipients must submit the following:

1. The final request for payment, if applicable.
2. The final FFR.
3. The final progress report detailing all accomplishments.
4. A qualitative narrative summary of the impact of those accomplishments throughout the period of performance.
5. Other documents required by this NOFO, terms and conditions of the federal award, or other DHS Component guidance.

After the awarding agency approves these reports, it will issue a closeout notice. The notice will indicate the period of performance as closed, list any remaining funds to be de-obligated, and address the record maintenance requirement. Unless a longer period applies, such as due to an audit or litigation, for equipment or real property used beyond the period of performance, or due to other circumstances outlined in 2 C.F.R. § 200.334, this maintenance requirement is three years from the date of the final FFR.

Also, pass-through entities are responsible for closing out those subawards as described in 2 C.F.R. § 200.344(e); subrecipients are still required to submit closeout materials within 90 calendar days of the subaward period of performance end date. When a subrecipient completes all closeout requirements, pass-through entities must promptly complete all closeout actions in time for the recipient to submit all necessary documentation and information to the awarding agency during the closeout of their prime award.

The recipient is responsible for returning any balances of unobligated or unliquidated funds that have been drawn down that are not authorized to be retained per 2 C.F.R. § 200.344(e).

(4) Administrative Closeout

Administrative closeout is a mechanism for FEMA to unilaterally execute closeout of an award. FEMA will use available award information in lieu of final recipient reports, per 2 C.F.R. § 200.344(h)-(i). It is an activity of last resort, and if FEMA administratively closes an award, this may negatively impact a recipient's ability to obtain future funding.

F. Additional Reporting Requirements

Anytime there is a change in personnel for any of the awardees or if applicable, subrecipients, their information needs to be submitted for approval (all the previous personal information identified).

G. Disclosing Information per 2 C.F.R. § 180.335

Before entering into a federal award, the applicant must notify the awarding agency if it knows that the applicant or any of the principals (as defined by 2 C.F.R. § 180.995) for the federal award:

1. Are presently excluded or disqualified;
2. Have been convicted within the preceding three years of any of the offenses listed in § 180.800(a) or had a civil judgment rendered against you for one of those offenses within that time period;

3. Are presently indicted for or otherwise criminally or civilly charged by a governmental entity (federal, state, or local) with the commission of any of the offenses listed in 2 C.F.R. § 180.800(a); or
4. Have had one or more public transactions (federal, state, or local) terminated within the preceding three years for cause or default.

This requirement is fully described in 2 C.F.R. § 180.335. Additionally, 2 C.F.R. § 180.350 requires recipients to provide immediate notice to the awarding agency at any time after entering into a federal award if:

1. The recipient learns that either it failed to earlier disclose information as required by 2 C.F.R. §180.335;
2. Due to changed circumstances, the applicant or any of the principals for the federal award now meet the criteria at 2 C.F.R. §180.335 listed above.

H. Reporting of Matters Related to Recipient Integrity and Performance

Appendix XII to 2 C.F.R. Part 200 states the terms and conditions for recipient integrity and performance matters used for this funding opportunity.

If the total value of all active federal grants, cooperative agreements, and procurement contracts for a recipient exceeds $10 million at any time during the period of performance:

1. The recipient must maintain the currency of information reported in SAM.gov about civil, criminal, or administrative proceedings described in paragraph (b) of Appendix XII;
2. The required reporting frequency is described in paragraph (d) of Appendix XII.

I. Single Audit Reports

A recipient expending $1 million or more in federal awards (as defined by 2 C.F.R. § 200.1) during its fiscal year must undergo an audit. This may be either a single audit complying with 2 C.F.R. § 200.514 or a program-specific audit complying with 2 C.F.R. §§ 200.501 and 200.507. Audits must follow 2 C.F.R. Part 200, Subpart F, 2 C.F.R. § 200.501, and the U.S. Government Accountability Office (GAO) Generally Accepted Government Auditing Standards.

J. 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 recipient or 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 recipient's or 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 conduct desk reviews and make site visits to review and evaluate project accomplishments and management control systems as well as provide any required technical assistance. Recipients and subrecipients must respond in a timely and accurate manner to DHS requests for information relating to a federal award.

K. Program Evaluation

Title I of the Foundations for Evidence-Based Policymaking Act of 2018 (Evidence Act), Pub. L. No. 115-435 (2019), urges federal agencies to use program evaluation as a critical tool to learn, improve delivery, and elevate program service and delivery across the program lifecycle. Evaluation means "an assessment using systematic data collection and analysis of one or more programs, policies, and organizations intended to assess their effectiveness and efficiency." Evidence Act, § 101 (codified at 5 U.S.C. § 311). OMB A-11, Section 290 (Evaluation and Evidence-Building Activities) further outlines the standards and practices for evaluation activities. Federal agencies are required to specify any requirements for recipient participation in program evaluation activities (2 C.F.R. § 200.301). Program evaluation activities incorporated from the outset in the NOFO, and program design and implementation allow recipients and agencies to meaningfully document and measure progress and achievement towards program goals and objectives, and identify program outcomes and lessons learned, as part of demonstrating recipient performance (2 C.F.R. § 200.301).

As such, recipients and subrecipients are required to participate in a Program Office (PO) or a DHS Component-led evaluation, if selected. This may be carried out by a third party on behalf of the PO or the DHS Component. Such an evaluation may involve information collections including, but not limited to, records of the recipients; surveys, interviews, or discussions with individuals who benefit from the federal award, program operating personnel, and award recipients; and site visits or other observation of recipient activities, as specified in a DHS Component or PO-approved evaluation plan. More details about evaluation requirements may be provided in the federal award, if available at that time, or following the award as evaluation requirements are finalized. Evaluation costs incurred during the period of performance are allowable costs (either as direct or indirect) in accordance with 2 C.F.R. § 200.413.

Recipients and subrecipients are also encouraged, but not required, to participate in any additional evaluations after the period of performance ends, although any costs incurred to participate in such evaluations are not allowed and may not be charged to the federal award.

L. Payment Information

Recipients will submit payment requests in FEMA GO under this program.

(5) Instructions to Grant Recipients Pursuing Payments

FEMA is instituting additional reviews on all grant payments and obligations to ensure allowability in accordance with 2 C.F.R. § 200.305. These measures will ensure funds are disbursed appropriately while continuing to support and prioritize communities who rely on FEMA for assistance. Once a recipient submits a payment request, FEMA will review the request. If FEMA approves a payment, recipients will be notified by FEMA GO and the payment will be delivered pursuant to the recipient's SAM.gov financial information. If FEMA disapproves of payment, FEMA will inform the recipient.

(6) Processing and Payment Timeline

FEMA must comply with regulations governing payments to grant recipients per 2 C.F.R. § 200.305. For grant recipients other than States, 2 C.F.R. § 200.305(b)(3) stipulates that FEMA is to make payments on a reimbursement basis within 30 days after receipt of the payment request, unless FEMA reasonably believes the request to be improper. For state recipients, 2 C.F.R. § 200.305(a)

instructs that federal grant payments are governed by Treasury-State Cash Management Improvement Act (CMIA) agreement ("Treasury-State agreement") and default procedures codified at 31 C.F.R. part 205 and Treasury Financial Manual 4A-200, "Overall Disbursing Rules for All Federal Agencies."

Treasury-State agreements generally apply to "major federal assistance programs" that are governed by 31 C.F.R. part 205, subpart A and are identified in the Treasury-State agreement in 31 C.F.R. §§ 205.2, 205.6. Where a federal assistance (grant) program is not governed by subpart A, payment and funds transfers from FEMA to the state are subject to 31 C.F.R. part 205, subpart B. Subpart B requires FEMA to "limit a funds transfer to a state to the minimum amounts needed by the state and must time the disbursement to be in accord with the actual, immediate cash requirements of the state in carrying out a federal assistance program or project. The timing and amount of funds transfers must be as close as is administratively feasible to a state's actual cash outlay for direct program costs and the proportionate share of any allowable indirect costs" per 31 C.F.R. § 205.33(a). Nearly all FEMA grants are not "major federal assistance programs." As a result, payments to states for those grants are subject to the "default" rules of 31 C.F.R. part 205, subpart B.

If additional information is needed, a request for information will be issued by FEMA to the recipient; recipients are strongly encouraged to respond to any additional FEMA request for information inquiries within three business days. If an adequate response is not received, the request may be denied, and the entity may need to submit a new reimbursement request; this will re-start the 30-day timeline.

(7) Submission Process

All non-disaster grant program reimbursement requests must be reviewed and approved by FEMA prior to drawdowns.

For all non-disaster reimbursement requests (regardless of system), please ensure submitting the following information:

1. Grant ID / Award Number
2. Total amount requested for drawdown
3. Purpose of drawdown and timeframe covered (must be within the award performance period)
4. Subrecipient Funding Details (if applicable).
    - Is funding provided directly or indirectly to a subrecipient?
        - If **no**, include statement "This grant funding is not being directed to a subrecipient."
        - If **yes**, provide the following details:
            - The name, mission statement, and purpose of each subrecipient receiving funds, along with the amount allocated and the specific role or activity being reimbursed.
            - Whether the subrecipient's work or mission involves supporting aliens, regardless of whether FEMA funds support such activities.
            - Whether the payment request includes an activity involving support to aliens.

- Whether the subrecipient has any diversity, equity, and inclusion practices.[1]

5. Supporting documentation to demonstrate that expenses are allowable, allocable, reasonable, and necessary under 2 C.F.R. part 200 and in compliance with the grant's NOFO, award terms, and applicable federal regulations.

M. Immigration Conditions

The term titled "Communication and Cooperation with the Department of Homeland Security and Immigration Officials" and paragraph (2)(a)(ii) of the term titled "Federal Anti-Discrimination Laws Material to the Government's Payment Decisions Under the False Claims Act" in the FY 2026 DHS Standard Terms and Conditions do not apply to any federal award under this funding opportunity.

3. Other Information

A. Period of Performance Extension

Extensions to the period of performance are allowed.

Recipients should consult with their FEMA point of contact for requirements related to performance period extensions.

See the Preparedness Grants Manual for more information on period of performance extensions.

B. Environmental Planning and Historic Preservation (EHP) Compliance

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

Recipients and subrecipients proposing projects with the potential to impact the environment or cultural resources, such as the modification or renovation of existing buildings, structures, and

[1] Pursuant to the preliminary injunction order issued on November 21, 2025, in *County of Santa Clara et al. v. Noem, et al.*, No. 25-cv-08330-WHO (N.D. Cal.), the DHS Standard Term and Condition titled "Federal Anti-Discrimination Laws Material to the Government's Payment Decisions Under the False Claims Act" does not apply to awards or subawards issued to any of the plaintiffs subject to the preliminary injunction order while the order remains in effect. If the preliminary injunction is extended to cover additional plaintiffs, this provision will also not apply to any awards or subawards issued to those plaintiffs. If the preliminary injunction is stayed, vacated, or extinguished, the term will immediately become effective.

Pursuant to the preliminary injunction order issued on November 21, 2025, in *City of Chicago et al. v. Noem, et al.*, No. 25-CV-12765 (N.D. Ill.), the DHS Standard Term and Condition titled "Federal Anti-Discrimination Laws Material to the Government's Payment Decisions Under the False Claims Act" does not apply to awards or subawards issued to any of the plaintiffs subject to the preliminary injunction order while the order remains in effect. If the preliminary injunction is extended to cover additional plaintiffs, this provision will also not apply to any awards or subawards issued to those plaintiffs. If the preliminary injunction is stayed, vacated, or extinguished, the term will immediately become effective.

Pursuant to the preliminary injunction order issued on October 31, 2025, in *City of Seattle v. Trump, et al.*, No. 2:25-cv-01435-BJR (W.D. Wa.), the DHS Standard Term and Condition titled "Federal Anti-Discrimination Laws Material to the Government's Payment Decisions Under the False Claims Act " does not apply to awards or subawards issued to any of the plaintiffs subject to the preliminary injunction order while the order remains in effect. If the preliminary injunction is extended to cover additional plaintiffs, this provision will also not apply to any awards or subawards issued to those plaintiffs. If the preliminary injunction is stayed, vacated, or extinguished, the term will immediately become effective.

As stated above, Paragraph(2)(a)(ii) of the DHS Standard Term and Condition titled "Federal Anti-Discrimination Laws Material to the Government's Payment Decisions Under the False Claims Act" will not apply even if any of these preliminary injunctions are stayed, vacated, or extinguished.

facilities, either new construction 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, and historic properties; 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, alternative courses of action, or both that may lessen impacts to those resources.

FEMA is sometimes required to consult with other regulatory agencies and the public 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, alternative courses of action, or both to lessen impacts to EHP resources and bring the project into EHP compliance. If a proposed project has been evaluated by another federal agency, FEMA may be able to streamline portions of the EHP review by adopting or supplementing previous analyses performed under the National Environmental Policy Act. If a proposed project has previously been reviewed by another federal agency, please provide those documents for FEMA's consideration.

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 found in the EHP Directive & 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.

The EHP screening form is available at Environmental & Historic Preservation Grant Preparation Resources.

C. Procurement Compliance

When purchasing under a FEMA award, recipients and subrecipients must comply with the federal procurement standards in 2 C.F.R. §§ 200.317-200.327. To assist with determining whether an action is a procurement or instead a subaward, please consult 2 C.F.R. § 200.331.

For detailed guidance on the federal procurement standards, recipients and subrecipients should refer to various materials issued by FEMA's Procurement Disaster Assistance Team (PDAT). The Procurement Under Grants Policy Guide (PUGPG) and additional resources can be found on the PDAT website at Procurement and Contracting.

When conducting procurement transactions under a federal award, states, Tribal Nations, the District of Columbia, U.S. territories, and their agencies must follow their own documented procurement policies and procedures as outlined in 2 C.F.R. § 200.317. They are also required to comply with rules

for domestic preferences (2 C.F.R. § 200.322), the use of recovered materials (2 C.F.R. § 200.323), and ensure all necessary contract provisions are included (2 C.F.R. § 200.327). If these entities do not have documented procurement policies or procedures, they must follow the federal procurement rules listed in 2 C.F.R. §§ 200.318–200.327.

Note: Tribal Nations are exempt from the recovered materials requirements in 2 C.F.R. § 200.323.

Local government and nonprofit recipients or subrecipients must have and use their own documented procurement procedures that reflect applicable state, local, tribal, and territorial (SLTT) laws and regulations, provided that the procurements conform to applicable federal law and the standards identified in 2 C.F.R. §§ 200.318–200.327.

(1) Important Changes to Procurement Standards in 2 C.F.R. Part 200

On April 22, 2024, OMB updated various parts of Title 2 of the Code of Federal Regulations, among them the procurement standards. These revisions apply to all FEMA awards with a federal award date or disaster declaration date on or after October 1, 2024, unless specified otherwise. The changes include updates to the Federal Procurement Standards, which govern how FEMA award recipients and subrecipients must purchase under a FEMA award.

More information on OMB's revisions to the Federal Procurement Standards can be found in Purchasing Under a FEMA Award: 2024 OMB Revisions Fact Sheet.

(2) Threshold Increases Effective October 1, 2025

Effective October 1, 2025, the United States Office of Management and Budget increased the Federal micro-purchase threshold from $10,000 to $15,000 and the Federal simplified acquisition threshold from $250,000 to $350,000. These updated thresholds now apply to recipient and subrecipient activities under 2 C.F.R. Part 200, including procurements and budget approval requests executed on or after October 1, 2025, for all open financial assistance awards.

(3) Procurement Standards: Competition and Conflict of Interest

All procurement transactions under a federal award must provide for full and open competition. To ensure compliance, recipients and subrecipients must avoid practices that restrict competition. Examples of restrictive practices include, but are not limited to:

- Placing unreasonable requirements on firms to qualify to do business;
- Requiring unnecessary experience or excessive bonding;
- Engaging in noncompetitive pricing practices between firms or affiliated companies;
- Awarding noncompetitive contracts to consultants on retainer;
- Specifying only a "brand name" product instead of allowing "an equal" product to be offered; and
- Taking arbitrary actions during the procurement process.

(4) Real Conflict of Interest

Under 2 C.F.R. § 200.318(c)(1), local government and nonprofit recipients or subrecipients must maintain written standards of conduct to address conflicts of interest. Employees, officers, or agents

involved in the selection, award, or administration of contracts are prohibited from participating if they have a real or apparent conflict of interest. A conflict arises when the individual, their immediate family, partner, or an organization they are affiliated with has a financial or other interest in, or stands to benefit from, a firm considered for a contract.

Additionally, officers, employees, and agents may not solicit or accept gratuities, favors, or anything of monetary value from contractors or subcontractors. However, recipients or subrecipients may establish standards for situations where the financial interest is not substantial, or the gift is an unsolicited item of nominal value. Violations of these standards must result in disciplinary actions as outlined in the recipient's or subrecipient's policies.

(5) Organizational Conflict of Interest

Under 2 C.F.R. § 200.318(c)(2), recipients or subrecipients with a parent, affiliate, or subsidiary organization that is not a state, local, tribal, or territorial (SLTT) government must maintain written standards of conduct to address organizational conflicts of interest. An organizational conflict of interest occurs when a relationship with a parent company, affiliate, or subsidiary compromises, or appears to compromise, the recipient's or subrecipient's impartiality in conducting a procurement action.

Recipients or subrecipients must disclose any potential organizational conflicts of interest in writing to FEMA or the pass-through entity, as required by FEMA policy.

(6) Contractors Drafting Requirements

Per 2 C.F.R. § 200.319(b), contractors that develop or draft specifications, statements of work, invitations for bids, or requests for proposals are prohibited from competing for those procurements. FEMA considers this an organizational conflict of interest and extends this restriction to contractors who assist recipients or subrecipients in developing grant applications, project plans, or budgets.

This prohibition also applies to former employees who worked on such activities while employed by the recipient or subrecipient. Unless the recipient or subrecipient solicits and awards a contract that explicitly includes both the development and execution of specifications (or similar elements), and the contract was procured in compliance with 2 C.F.R. §§ 200.317–200.327, federal funds cannot be used to pay the contractor to perform the work. This rule applies to all contracts funded with federal grant funds, including pre-award costs (e.g., grant writer fees) and post-award costs (e.g., grant management fees).

(7) Supply Schedules and Purchasing Programs

Generally, a recipient or subrecipient may seek to procure goods or services from a federal supply schedule, state supply schedule, or group purchasing agreement.

Information on General Services Administration programs, including multiple award schedules, for states, Tribal Nations, and local governments, and their instrumentalities, can be found in Purchasing Resource and Support for State and Local Government.

(8) Procurement Documentation

Per 2 C.F. R. § 200.318(i), local government and nonprofit recipients or subrecipients are required to maintain and retain records sufficient to detail the history of procurement. These records must include, but are not limited to, the rationale for the procurement method, selection of contract type, contractor selection or rejection, and the basis for the contract price. States and Tribal Nations are reminded that in order for any cost to be allowable, it must be adequately documented per 2 CFR §200.403(g).

Examples of the types of documents that would cover this information include but are not limited to:

- Solicitation documentation, such as requests for quotes, invitations for bids, or requests for proposals;
- Responses to solicitations, such as quotes, bids, or proposals;
- Pre-solicitation independent cost estimates and post-solicitation cost/price analyses on file for review by federal personnel, if applicable;
- Contract documents and amendments, including required contract provisions; and
- Other documents required by federal regulations applicable at the time a grant is awarded to a recipient.

D. Buy America Preference Requirements 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 project are produced in the United States.

Recipients and subrecipients provided funds under this program for an infrastructure project must comply with FEMA's implementation requirements of the Build America, Buy America Act, as detailed in FEMA's Buy America Preference Policy. 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.

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.

For more information about FEMA's implementation of the Buy America Preference, please visit FEMA's Buy America Preference webpage at Programs and Definitions: Build America, Buy America Act | FEMA.gov.

(9) Waivers

When necessary, recipients (and subrecipients through their pass-through entity) may apply for a waiver from these requirements.

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

- Applying the domestic content procurement preference would be inconsistent with the public interest, or
- 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 satisfactory quality, or
- 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 | FEMA.gov.

(10) Definitions

For definitions of the key terms of the Build America, Buy America Act, please visit Programs and Definitions: Build America, Buy America Act | FEMA.gov.

E. Mandatory Disclosures

The non-federal entity or applicant for a federal award must disclose, in a timely manner, in writing to the federal awarding agency or pass-through entity all violations of federal criminal law involving fraud, bribery, or gratuity violations potentially affecting the federal award, 2 C.F.R. § 200.113.

F. Adaptive Support

Pursuant to Section 504, of the Rehabilitation Act of 1973, recipients of FEMA financial assistance must ensure that their programs and activities do not discriminate against qualified individuals with disabilities.

G. Record Retention

(11) Record Retention Period

Financial records, supporting documents, statistical records, and all other non-federal entity records pertinent to a federal award generally must be maintained for at least three years from the date the final FFR is submitted per 2 C.F.R. §200.334. Further, if the recipient does not submit a final FFR and the award is administratively closed, FEMA uses the date of administrative closeout as the start of the general record retention period.

The record retention period may be longer than three years or have a different start date in certain cases.

(12) Types of Records to Retain

FEMA requires that recipients and subrecipients maintain the following documentation for federally funded purchases:

- Specifications
- Solicitations
- Competitive quotes or proposals
- Basis for selection decisions
- Purchase orders
- Contracts
- Invoices
- Cancelled checks

H. Actions to Address Noncompliance

Non-federal entities receiving financial assistance funding from FEMA are required to comply with requirements in the terms and conditions of their awards or subawards, including the terms set forth in applicable federal statutes, regulations, NOFOs, and policies. Throughout the award lifecycle or even after an award has been closed, FEMA or the pass-through entity may discover potential or actual noncompliance on the part of a recipient or subrecipient.

In the case of any potential or actual noncompliance, FEMA may place special conditions on an award per 2 C.F.R.§ 200.208 and 2 C.F.R.§ 200.339. FEMA may place a hold on funds until the matter is corrected, or additional information is provided per 2 C.F.R.§ 200.339. or it may do both. Similar remedies for noncompliance with certain federal civil rights laws are authorized pursuant to 44 C.F.R. Part 7 and 44 C.F.R. Part 19 or other applicable regulations.

If the noncompliance is not able to be corrected by imposing additional conditions or the recipient or subrecipient refuses to correct the matter, FEMA may take other remedies allowed under 2 C.F.R. § 200.339.

I. Audits

FEMA grant recipients are subject to audit oversight from multiple entities including the DHS Office of Inspector General (OIG), the GAO, the pass-through entity, or independent auditing firms for single audits, and may cover activities and costs incurred under the award. Auditing agencies such as the DHS OIG, the GAO, and the pass-through entity (if applicable), and FEMA in its oversight capacity, must have access to records pertaining to the FEMA award.

F. Contacts and Appendices

Contacts 56

Appendices 56

1. Contacts

A. Program Office

FEMA has assigned state-specific Preparedness Officers for the NSGP. If you do not know your Preparedness Officer, please contact NSGP by E-mail at fema-nsgp@fema.dhs.gov.

B. FEMA Grants News

FEMA Grants News provides general information on all FEMA grant programs and maintains a comprehensive database containing key personnel contact information at the federal, state, and local levels. FEMA Grants News is reachable at fema-grants-news@fema.dhs.gov or (800) 368-6498, Monday through Friday, 9 a.m. – 5 p.m. ET.

C. Award Administration Division

GPD's Award Administration Division (AAD) provides support regarding financial matters and budgetary technical assistance. AAD can be contacted at ASK-GMD@fema.dhs.gov.

D. Procurement Under Grants Division

The Procurement Disaster Assistance Team (PDAT) and Buy America Branch (BAB) within GPD's Procurement Under Grants Division offer technical support to ensure compliance with federal procurement and domestic preference standards for FEMA awards. You can reach PDAT at fema-gpd-pdat@fema.dhs.gov and BAB at fema-grants-buyamerica@fema.dhs.gov. When reaching out, please include your FEMA grant program point of contact for reference.

E. FEMA Regional Offices

FEMA Regional Offices also may provide fiscal support, including pre- and post-award administration and technical assistance. FEMA Regional Office contact information is available at Regions, States and Territories.

F. Civil Rights

Consistent with Executive Order 14173, Ending Illegal Discrimination & Restoring Merit-Based Opportunity, the FEMA Integration and Coordination Division (ICD) is responsible for ensuring compliance with and enforcement of federal civil rights obligations in connection with programs and services conducted by FEMA. They are reachable at fema-ocr@fema.dhs.gov.

G. Environmental Planning and Historic Preservation

The FEMA Office of Environmental Planning and Historic Preservation (OEHP) provides guidance and information about the EHP review process to FEMA programs and recipients and subrecipients. Send any inquiries regarding compliance for FEMA grant projects under this NOFO to FEMA-OEHP-NOFOQuestions@fema.dhs.gov.

H. Payment and Reporting

FEMA uses FEMA GO for financial reporting, invoicing, and tracking payments. The Direct Deposit/Electronic Funds Transfer (DD/EFT) method of payment is used for recipients. For any

questions about the system, contact the FEMA GO Helpdesk at femago@fema.dhs.gov or (877) 585-3242, Monday through Friday, 9 a.m. – 6 p.m. ET.

I. FEMA GO

For technical assistance with the FEMA GO system, please contact the FEMA GO Helpdesk at femago@fema.dhs.gov or (877) 585-3242, Monday through Friday, 9 a.m. – 6 p.m. ET.

J. FEMA Preparedness Toolkit

The FEMA Preparedness Toolkit (PrepToolkit) provides access to tools and resources needed to implement the National Preparedness System and provide a collaborative space for communities completing the Unified Reporting Tool (URT). Recipients complete and submit their Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR), and other required assessments using the PrepToolkit. For assistance, contact support@preptoolkit.fema.dhs.gov.

K. Preparedness Grants Manual

Recipients seeking guidance on policies and procedures for managing preparedness grants should reference the Preparedness Grants Manual.

2. Appendices

Appendix A: Allowable Costs

A. Planning

Planning costs are allowed under this program only as described in this funding notice and the Preparedness Grants Manual.

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

1. Development and enhancement of security plans and protocols;
2. Development or further strengthening of security assessments;
3. Emergency contingency plans;
4. Evacuation/Shelter-in-place plans;
5. Coordination and information sharing with fusion centers; and,
6. Other project planning activities with prior approval from FEMA.

B. Organization

Organization costs are not allowed under this program.

C. Equipment

Equipment costs are allowed under this program only as described in this funding notice and the Preparedness Grants Manual.

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, including the item's plain-language description *specific to the NSGP*, 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.
04AP-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 to 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).

AEL Code	Title	Description
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-	Repeater	Electronic device that receives a weak or low-

AEL Code	Title	Description
REPT		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.
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.
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).
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	Receptacles, Trash, Blast-Resistant	Blast-resistant trash receptacles.

AEL Code	Title	Description
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

AEL Code	Title	Description
		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	See Appendix A, Training and Exercises

Additional dropdowns in Section IV-B of the IJ, while not part of the AEL, include the following:

–Code	Title	Description
Contract Security	Private Contact Security Personnel/Guards	See Appendix A, Contracted Security Personnel
M&A	Management and Administration (M&A)	See Management and Administration (M&A)

–Code	Title	Description
PLANNING	Planning	See Appendix A, Planning
EXERCISE	Exercise	See Appendix A, Training and Exercises

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, recipients 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 (see the Maintenance and Sustainment section below for more information).

Recipients and subrecipients must obtain prior approval from FEMA to purchase equipment not listed on the AEL. Note: Subapplicants budget narratives should indicate costs that include shipping and/or tax, as applicable. It is not required to itemize these costs separately from the relevant purchases.

Applicants and subapplicants should analyze the cost 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, 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. This SAFECOM Guidance can be found at the Funding and Sustainment page on CISA.gov.

The installation of certain equipment may trigger EHP requirements. Please refer to the EHP sections in this NOFO and the Preparedness Grants Manual for more information. Additionally, some equipment installation may constitute construction or renovation. Please see the Construction and Renovation subsection for additional information.

D. Training and Exercises

Training and exercise costs are allowed under this program only as described in this funding notice and the Preparedness Grants Manual.

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

1. Employed or volunteer security staff to attend security-related training within the United States;

2. 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); and

3. Nonprofit organization’s employees, or members/congregants to receive on-site security training.

Allowable training-related costs under the 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 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 subapplicant's IJ. Training should provide the opportunity to demonstrate and validate skills learned as well as to identify any gaps in these skills. ***Proposed attendance at training courses and all associated costs using the NSGP must be included in the subapplicant'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 | FEMA.gov. 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 (fema.gov). Recipients are encouraged to enter their exercise data and AAR/IP in the Preparedness Toolkit.

Note: Subapplicants budget narratives should indicate costs that includes shipping and/or tax, as applicable. It is not required to break the costs out as separate from the relevant purchase(s).

E. Maintenance and Sustainment

Maintenance and sustainment costs, such as maintenance contracts, warranties, repair or replacement costs, upgrades, and user fees are allowable. For additional information, see the Preparedness Grants Manual.

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 your Preparedness Officer. All recipients of NSGP funds must request and receive prior approval from FEMA before any NSGP funds are used for any construction or renovation. Additionally, recipients are required to submit a SF-424C Budget and budget detail citing the project costs and an SF-424D Form for

standard assurances for the construction project. The total cost of any construction or renovation paid for using NSGP funds may not exceed the greater amount of $1 million or 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 441. Subrecipients may use 100% of the NSGP funds awarded for contracted security personnel. NSGP funds may not be used to purchase equipment for contracted security.

Appendix B: FY2026 NSGP-UA Eligible High Risk Urban Areas Allocations

State/Territory	Funded Urban Area	NSGP-UA Actual Allocation	5% M&A	NSGP-UA Total Allocation (Actual + M&A)
Arizona	Phoenix Area	$3,094,415	$162,864	$3,257,279
California	Anaheim/Santa Ana Area	$1,042,557	$54,871	$1,097,428
	Bay Area	$10,597,377	$557,757	$11,155,134
	Los Angeles/Long Beach Area	$7,880,378	$414,757	$8,295,135
	Riverside Area	$783,586	$41,241	$824,827
	Sacramento Area	$1,631,025	$85,843	$1,716,868
	San Diego Area	$1,084,768	$57,093	$1,141,861
Colorado	Colorado Springs Area	$255,715	$13,459	$269,174
	Denver Area	$2,227,856	$117,256	$2,345,112
District of Columbia	National Capital Region	$6,740,564	$354,767	$7,095,331
Florida	Jacksonville Area	$578,934	$30,470	$609,404
	Miami/Fort Lauderdale Area	$8,233,906	$433,363	$8,667,269
	Orlando Area	$966,950	$50,892	$1,017,842
	Tampa Area	$1,521,981	$80,104	$1,602,085
Georgia	Atlanta Area	$2,615,446	$137,655	$2,753,101
Hawaii	Honolulu Area	$328,425	$17,286	$345,711
Illinois	Chicago Area	$6,526,053	$343,476	$6,869,529
Indiana	Indianapolis Area	$447,656	$23,561	$471,217
Louisiana	New Orleans Area	$281,822	$14,833	$296,655
Maryland	Baltimore Area	$1,857,628	$97,770	$1,955,398
Massachusetts	Boston Area	$399,755	$21,040	$420,795
Michigan	Detroit Area	$3,075,383	$161,862	$3,237,245
Minnesota	Twin Cities Area	$1,119,687	$58,931	$1,178,618
Missouri	Kansas City Area	$711,312	$37,437	$748,749
	St. Louis Area	$849,922	$44,733	$894,655

State/Territory	Funded Urban Area	NSGP-UA Actual Allocation	5% M&A	NSGP-UA Total Allocation (Actual + M&A)
Nevada	Las Vegas Area	$788,838	$41,518	$830,356
New Jersey	Jersey City/Newark Area	$25,716,583	$1,353,504	$27,070,087
New York	New York City Area	$31,083,641	$1,635,981	$32,719,622
North Carolina	Charlotte Area	$820,435	$43,181	$863,616
Ohio	Cincinnati Area	$275,355	$14,492	$289,847
	Cleveland Area	$407,954	$21,471	$429,425
	Columbus Area	$455,006	$23,948	$478,954
Oregon	Portland Area	$793,931	$41,786	$835,717
Pennsylvania	Philadelphia Area	$1,397,185	$73,536	$1,470,721
	Pittsburgh Area	$955,827	$50,307	$1,006,134
Tennessee	Nashville Area	$586,845	$30,887	$617,732
Texas	Austin Area	$783,710	$41,248	$824,958
	Dallas/Fort Worth/Arlington Area	$4,759,793	$250,515	$5,010,308
	Houston Area	$4,964,987	$261,315	$5,226,302
	San Antonio Area	$947,145	$49,850	$996,995
Virginia	Hampton Roads Area	$578,171	$30,430	$608,601
	Richmond Area	$450,561	$23,714	$474,275
Washington	Seattle Area	$1,363,193	$71,747	$1,434,940
Wisconsin	Milwaukee Area	$517,739	$27,249	$544,988
Total		**$142,500,000**	**$7,500,000**	**$150,000,000**

Appendix C: FY2026 NSGP-S Allocations

State/Territory	NSGP-S Actual Allocation	5% M&A	FY26 NSGP-S Total Allocation (Actual + M&A)	State/Territory	NSGP-S Actual Allocation	5% M&A	FY26 NSGP-S Total Allocation (Actual + M&A)
Alabama	$3,135,000	$165,000	$3,300,000	Nevada	$1,710,000	$90,000	$1,800,000
Alaska	$1,710,000	$90,000	$1,800,000	New Hampshire	$1,852,500	$97,500	$1,950,000
Arizona	$2,422,500	$127,500	$2,550,000	New Jersey	$2,280,000	$120,000	$2,400,000
Arkansas	$2,422,500	$127,500	$2,550,000	New Mexico	$2,137,500	$112,500	$2,250,000
California	$5,913,750	$311,250	$6,225,000	New York	$3,990,000	$210,000	$4,200,000
Colorado	$1,995,000	$105,000	$2,100,000	North Carolina	$4,275,000	$225,000	$4,500,000
Connecticut	$2,707,500	$142,500	$2,850,000	North Dakota	$1,710,000	$90,000	$1,800,000
Delaware	$1,710,000	$90,000	$1,800,000	Ohio	$4,275,000	$225,000	$4,500,000
District of Columbia	$0	$0	$0	Oklahoma	$2,850,000	$150,000	$3,000,000
Florida	$3,990,000	$210,000	$4,200,000	Oregon	$2,280,000	$120,000	$2,400,000

State/Territory	NSGP-S Actual Allocation	5% M&A	FY26 NSGP-S Total Allocation (Actual + M&A)	State/Territory	NSGP-S Actual Allocation	5% M&A	FY26 NSGP-S Total Allocation (Actual + M&A)
Georgia	$3,847,500	$202,500	$4,050,000	Pennsylvania	$3,420,000	$180,000	$3,600,000
Hawaii	$1,567,500	$82,500	$1,650,000	Rhode Island	$1,852,500	$97,500	$1,950,000
Idaho	$2,137,500	$112,500	$2,250,000	South Carolina	$3,277,500	$172,500	$3,450,000
Illinois	$3,705,000	$195,000	$3,900,000	South Dakota	$1,710,000	$90,000	$1,800,000
Indiana	$3,277,500	$172,500	$3,450,000	Tennessee	$3,277,500	$172,500	$3,450,000
Iowa	$2,565,000	$135,000	$2,700,000	Texas	$5,201,250	$273,750	$5,475,000
Kansas	$2,137,500	$112,500	$2,250,000	Utah	$2,565,000	$135,000	$2,700,000
Kentucky	$2,992,500	$157,500	$3,150,000	Vermont	$1,710,000	$90,000	$1,800,000
Louisiana	$2,707,500	$142,500	$2,850,000	Virginia	$2,422,500	$127,500	$2,550,000
Maine	$1,852,500	$97,500	$1,950,000	Washington	$2,565,000	$135,000	$2,700,000
Maryland	$1,852,500	$97,500	$1,950,000	West Virginia	$1,995,000	$105,000	$2,100,000
Massachusetts	$3,420,000	$180,000	$3,600,000	Wisconsin	$2,850,000	$150,000	$3,000,000
Michigan	$3,277,500	$172,500	$3,450,000	Wyoming	$1,567,500	$82,500	$1,650,000
Minnesota	$2,280,000	$120,000	$2,400,000	Puerto Rico	$2,565,000	$135,000	$2,700,000
Mississippi	$2,422,500	$127,500	$2,550,000	U.S. Virgin Islands	$1,425,000	$75,000	$1,500,000
Missouri	$2,422,500	$127,500	$2,550,000	American Samoa	$1,425,000	$75,000	$1,500,000
Montana	$1,852,500	$97,500	$1,950,000	Guam	$1,425,000	$75,000	$1,500,000
Nebraska	$2,137,500	$112,500	$2,250,000	Northern Mariana Islands	$1,425,000	$75,000	$1,500,000
NSGP-S Actual Allocation				**$142,500,000**			
5% M&A				**$7,500,000**			
NSGP-S Total Allocation				**$150,000,000**			

Appendix D: FY2026 Evaluation Criteria and Scoring Matrix

SAA Reviewers will score applications based on specific criteria aligned to the NSGP's intent. The table below details the specific criteria aligned to each of the IJ requirements, and the maximum number of points an application can receive for each criterion. The SAA Reviewers will score applications based on specific criteria aligned to the IJ requirements. Each question will be scored based on the complexity within the requirement.

Investment Justification Requirement	Criteria	Score	Explanation
Applicant Information Section			
Did the subapplicant provide all the required information in the Applicant Information Section?	The subapplicant should provide all information as it is applicable in the informational section.	Yes	The subapplicant **did** provide all the required information.
		No	The subapplicant **did not** provide all the required information.
Background Information Section			
Did the subapplicant provide a description of their nonprofit organization to include symbolic value of the site as a highly recognized national or historical institution or significant institution within the community that renders the site as a possible target of terrorism and other extremist attacks?	Subapplicants must describe their organization, its mission/purpose, the symbolic value of the building/organization, and how these factors may make it the target of an attack.	0	The subapplicant **did not provide a description** of the organization including the symbolic value of the site as a highly recognized institution that renders the site a possible target of terrorism or other extremist attacks.
		1	The subapplicant **provided a poor description** of the organization including the symbolic value of the site as a highly recognized institution that renders the site a possible target of terrorism or other extremist attacks.
		2	The subapplicant **provided an adequate description** of the organization including the symbolic value of the site as a highly recognized institution that renders the site a possible target of terrorism or other extremist attacks.
		3	The subapplicant **provided a full, clear, and effective description** of the organization including the symbolic value of the site as a highly recognized institution that renders the site a possible target of terrorism or other extremist attacks.

Investment Justification Requirement	Criteria	Score	Explanation
Did the subapplicant provide a description of their nonprofit organization to include any role in responding to or recovering from events that integrate nonprofit preparedness with broader state/local preparedness efforts?	Subapplicants must clearly describe their individual organization's previous or existing role in response to or in recovery efforts to terrorist or other extremist attacks. This should tie into the broader preparedness efforts of state and/or local government.	0	The subapplicant **did not provide a description** of the organization that included any role in responding to or recovering from events that integrate nonprofit preparedness with broader state/local efforts.
		1	The subapplicant **provided some description** of the organization that included any role in responding to or recovering from events that integrate nonprofit preparedness with broader state/local efforts.
		2	The subapplicant **provides a full, clear, and effective description** of the organization that included any role in responding to or recovering from events that integrate nonprofit preparedness with broader state/local efforts.
Risk			
Did the subapplicant discuss specific threats or attacks against the nonprofit organization or closely related organization?	To substantiate the subapplicant's risk to a terrorist or other extremist attack, subapplicants may describe incidents that have occurred at or threats that have been made to their organization. Subapplicants may also draw from incidents that have occurred at closely related/similar organizations either domestically or internationally; the	0	The subapplicant **does not discuss specific** threats or attacks against the organization or a closely related organization.

Investment Justification Requirement	Criteria	Score	Explanation
	subapplicant should make the connection that they are at risk for the same reasons. Local crimes such as burglary, theft, or vandalism without a terrorism, extremism, or hate-related nexus may provide contextual justification for NSGP funding.		
		1	The subapplicant **provided minimal discussion** of threats or attacks against the organization or a closely related organization.
		2	The subapplicant **provided poor discussion** of threats or attacks against the organization or a closely related organization.
		3	The subapplicant **provided adequate discussion** of threats or attacks against the organization or a closely related organization.
		4	The subapplicant **provided good discussion** of threats or attacks against the organization or a closely related organization.
		5	The subapplicant **provided multiple, detailed, and specific** threats or attacks against the organization or a closely related organization.
In considering the vulnerabilities, how	Subapplicants must provide a clear	0	The subapplicant **did not discuss or describe** the organization's susceptibility to attack.

Investment Justification Requirement	Criteria	Score	Explanation
well did the subapplicant describe the organization's susceptibility to destruction, incapacitation, or exploitation by a terrorist or other extremist attack?	description of findings from a completed vulnerability assessment.	1	The subapplicant **provided minimal description** of the organization's susceptibility to attack.
		2	The subapplicant **provided poor description** of the organization's susceptibility to attack.
		3	The subapplicant **provided adequate description** of the organization's susceptibility to attack.
		4	The subapplicant **provided good description** of the organization's susceptibility to attack.
		5	The subapplicant **provided clear, relevant, and compelling description** of the organization's susceptibility.
In considering potential consequences, how well did the subapplicant address potential negative effects on the organization's asset, system, and/or network if damaged, destroyed, or disrupted by a terrorist or other extremist attack?	Subapplicants should describe how an attack would impact them, the community served, and if possible/applicable, beyond the immediate individuals served (nearby critical infrastructure, businesses, transportation, schools, etc.).	0	The subapplicant **did not discuss or describe** the potential negative consequences the organization may face.
		1	The subapplicant **provided minimal description** of the potential negative consequences the organization may face.
		2	The subapplicant **provided poor description** of the potential negative consequences the organization may face.
		3	The subapplicant **provided adequate description** of the potential negative consequences the organization may face.
		4	The subapplicant **provided good description** of the potential negative consequences the

Investment Justification Requirement	Criteria	Score	Explanation
			organization may face.
		5	The subapplicant **provided a clear, relevant, and compelling description** of the potential negative consequences the organization may face.
Facility Hardening			
How well does the subapplicant describe the proposed facility hardening activities, projects, and/or equipment and relate their proposals to the vulnerabilities described in the "Risk" Section?	In narrative form, subapplicants must clearly explain what the proposed activities, projects, and/or equipment are, identify their estimated cost, and describe how they will mitigate, or address vulnerabilities identified in their vulnerability assessment.	0	The subapplicant **does not propose** facility hardening or the proposals do not mitigate identified risk(s) and/or vulnerabilities.
		1	Proposed activities, projects, or equipment **may provide minimal** facility hardening **or are only minimally related** to some of the identified risk(s) and/or vulnerabilities.
		2	Proposed facility hardening activities, projects, or equipment **would likely mitigate** identified risk(s) and/or vulnerabilities.
		3	Proposed facility hardening activities, projects, or equipment are **clearly aligned with and effectively mitigate** the identified risk(s) and/or vulnerabilities.
Did the subapplicant's proposed facility hardening activity focus on the prevention of and/or protection against the risk of a terrorist or	The proposed activities, projects, and equipment should directly tie to the prevention of and/or protection against the risk of terrorist or other extremist attacks.	0	The proposed facility hardening activities **do not focus** on the prevention of and/or protection against the risk of terrorist or other extremist attacks.
		1	The proposed facility hardening activities **are somewhat focused** on the prevention of and/or protection against the risk of terrorist or other

Investment Justification Requirement	Criteria	Score	Explanation
other extremist attack?			extremist attacks.
		2	The proposed facility hardening activities **are adequately focused** on the prevention of and/or protection against the risk of terrorist or other extremist attacks.
		3	The proposed facility hardening activities **are clearly and effectively focused** on the prevention of and/or protection against the risk of terrorist or other extremist attacks.
Are all proposed equipment, activities, and/or projects tied to a vulnerability that it could reasonably address/mitigate?	The proposed equipment, activities, and/or projects should mitigate/address the vulnerability tied to it.	0	**No vulnerabilities are listed** and/or the proposed equipment, activities, or projects **do not address listed vulnerabilities**.
		1	The proposed equipment/activities/projects **are somewhat reasonable** to address the listed vulnerability.
		2	The proposed equipment/activities/projects **are mostly reasonable** to address the listed vulnerability.
		3	The proposed equipment/activities/projects **effectively address** the listed vulnerability.
Milestones			
How well did the subapplicant describe the milestones and the associated key activities that lead to	The subapplicant should describe the milestones needed to accomplish the goals of the NSGP funding and should include the	0	The subapplicant **did not provide** information on milestones and associated key activities.
		1	The subapplicant **provided some description** of milestone events and the associated key activities

Investment Justification Requirement	Criteria	Score	Explanation
the milestone event over the NSGP period of performance?	key activities that will be necessary to accomplish those milestones.		over the NSGP POP.
		2	The subapplicant **provided adequate description** of milestone events and the associated key activities over the NSGP POP.
		3	The subapplicant **fully and effectively described** milestone events and the associated key activities over the NSGP POP.
Did the subapplicant include milestones and associated key activities that are feasible over the NSGP period of performance?	Milestones should be realistic, potentially include the entire period of performance (36 months), be inclusive of all proposed activities, and consider the Environmental Planning and Historic Preservation review process. Milestones should not exceed 36 months and should not begin prior to the Period of Performance	0	The subapplicant **did not include** milestones and key activities that are feasible over the NSGP POP.
		1	The subapplicant included milestones and key activities that are **somewhat feasible** over the NSGP POP.
		2	The subapplicant included milestones and key activities that **are feasible** over the NSGP POP.
Project Management			
How well did the subapplicant justify the effectiveness of the proposed management team's roles and responsibilities and the governance structure to support	Brief description of the project manager(s) and level of experience.	0	The subapplicant **did not justify** the effectiveness of the proposed management team or the structure in place to support the implementation.
		1	The subapplicant **somewhat justified** the effectiveness of the proposed management team and the structure in place to the support implementation.

Investment Justification Requirement	Criteria	Score	Explanation
implementation of the Investment?		2	The subapplicant **fully justified** the effectiveness of the proposed management team and the structure in place to the support implementation.
Impact			
How well did the subapplicant describe the outcomes/outputs that would indicate that the Investment was successful?	Measurable outputs and outcomes should directly link to the vulnerabilities and consequences outlined in the "Risk" Section.	0	The subapplicant **did not describe** the outcomes and/or outputs that would indicate the Investment was successful.
		1	The subapplicant **provided minimal information** on the outcomes and/or outputs that would indicate the Investment was successful.
		2	The subapplicant **provided some information** on the outcomes and/or outputs that would indicate the Investment was successful.
		3	The subapplicant **provided an adequate discussion** of the outcomes and/or outputs that would indicate the Investment was successful.
		4	The subapplicant **provided a full and detailed description** of the outcomes and/or outputs that would indicate the Investment was successful.