Nonprofit Security Grant Program
National Security Supplemental
Notice of Funding Opportunity (NOFO)

Grant Issued By:

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

Grant Issued Through:

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

Assistance Listing:

97.008

Funding Opportunity Title:

Nonprofit Security Grant Program – National Security Supplemental (NSGP-NSS)

Overview

The Nonprofit Security Grant Program – National Security Supplemental (NSGP-NSS) supplements one of three 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.

There are two funding sources appropriated for nonprofit organizations:

1) ***Nonprofit Security Grant Program (NSGP) - Urban Area (NSGP-UA):*** NSGP-UA funds nonprofit organizations located **within** FY 2024 Urban Area Security Initiative (UASI)-designated high-risk urban areas. Eligible applicant criteria is listed below under Applicant Eligibility Criteria.

2) ***Nonprofit Security Grant Program (NSGP) - State (NSGP-S):*** NSGP-S funds nonprofit organizations located **outside** of a FY 2024 UASI-designated high-risk urban area. Under NSGP-S, each state will receive a target allocation for nonprofit organizations located **outside** of FY 2024 UASI-designated urban areas. Eligible applicant criteria is listed below under Applicant Eligibility Criteria.

DHS is focused on building a national culture of preparedness and protecting against terrorism and other threats to our national security. The threats to our nation have evolved during the past two decades. We now face continuous cyber threats by sophisticated actors, threats to soft targets and crowded places, and threats from domestic violent extremists, who represent one of the most persistent threats to the nation today. Therefore, DHS/FEMA has identified one priority area related to some of the most serious threats that recipients should address with their NSGP funds: **enhancing the protection of soft targets/crowded places**.

DHS is also focused on forging partnerships to strengthen information sharing and collaboration among federal, state, local, tribal, and territorial law enforcement. There are no requirements for information sharing between nonprofit organizations and law enforcement; however, the NSGP-NSS seeks to bring nonprofit organizations into broader state and local preparedness efforts by removing barriers to communication and being more inclusive. DHS/FEMA encourages information sharing, while the goal of the NSGP-NSS is centered on improving and increasing a nonprofit organization's physical/cybersecurity and facility/target hardening to enhance the protection of soft targets/crowded places. All NSGP-NSS activities must be linked to enhancing the security and safety at the physical site of the nonprofit organization.

Goal, Objectives, and Priorities

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

Objectives: The objective of the NSGP-NSS is to provide funding for physical and cybersecurity enhancements and other security-related activities to nonprofit organizations that are at risk of a terrorist or other extremist attack within the period of performance. The NSGP-NSS also seeks to integrate the preparedness activities of nonprofit organizations with broader state and local preparedness efforts. Lastly, via funding spent on Planning, Organizational, Equipment, Training, and Exercises (POETE) towards enhancing the protection of soft targets and crowded places, the NSGP-NSS seeks to address and close capability gaps identified in individual nonprofit organization vulnerability assessments.

Priorities: Given the evolving threat landscape, DHS/FEMA has evaluated the national risk profile and set priorities that help ensure appropriate allocation of scarce security dollars. In assessing the national risk profile, one area warrants the most concern under the NSGP-NSS.

1) Enhancing the protection of soft targets/crowded places

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

1) Effective planning
2) Training and awareness campaigns
3) Exercises

A continuing area of concern is the threat posed by malicious cyber actors. Additional resources and information regarding cybersecurity and cybersecurity performance goals are available through the Cybersecurity and Infrastructure Security Agency, Cross-Sector Cybersecurity Performance Goals, and the National Institute of Standards and Technology.

The table below provides a breakdown of these priority areas for the NSGP-NSS, showing both the core capabilities enhanced and lifelines supported, 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.

NSGP-NSS Funding Priorities

All priorities in this table concern 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 activities
	• Cybersecurity
	• Long-term vulnerability reduction
	• Situational assessment
	• Infrastructure systems
		• Private contracted security guards
		• Physical security enhancements
		  ○ Closed circuit television (CCTV) security cameras
		  ○ Security screening equipment for people and baggage
		  ○ Access controls
		  ○ Fencing, gates, barriers etc.
		  ○ Card readers, associated hardware/software
		• Cybersecurity enhancements
		  ○ Risk-based cybersecurity planning and training
		  ○ Improving cybersecurity of access control and identify verification systems
		  ○ Improving cybersecurity of security technologies (e.g., CCTV systems)
		  ○ Adoption of cybersecurity performance goals (CISA's Cross-Sector Cybersecurity Performance Goals)

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:
		  ○ Security plans and protocols
		  ○ Emergency/contingency plans
		  ○ Evacuation/shelter in place plans

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

Alignment to Program Purpose and the DHS and FEMA Strategic Plan

Among the five basic homeland security missions, noted in the DHS Strategic Plan for Fiscal Years 2020-2024, NSGP-NSS supports the goal to Strengthen National Preparedness and Resilience.

The 2022-2026 FEMA Strategic Plan outlines three bold, ambitious goals in order to position FEMA to address the increasing range and complexity of disasters, support the diversity of communities we serve,

and complement the nation's growing expectations of the emergency management community. The NSGP-NSS supports FEMA's efforts to instill equity as a foundation of emergency management (Goal 1), as well as promote and sustain a ready FEMA and prepared nation (Goal 3). We invite our stakeholders and partners to also adopt these priorities and join us in building a more prepared and resilient nation.

NSGP-UA Maximum Award

St. Louis Urban Area

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

If an applicant applies for multiple sites, it must submit one complete Investment Justification (IJ) for each site.

Kansas City Urban Area

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

If an applicant applies for multiple sites, it must submit one complete Investment Justification (IJ) for each site.

NSGP-S Maximum Award

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

If an applicant applies for multiple sites, it must submit one complete Investment Justification (IJ) for each site.

Consortium Applications

Consortium applications are eligible under the NSGP-NSS. Under a consortium application, an eligible nonprofit organization (lead consortium member/organization) would apply on behalf of their organization and other eligible nonprofit organizations. Consortium applications may apply for up to $200,000 per site for a maximum of ten sites, not to exceed $1,000,000. If the consortium application is successful, the lead consortium member/organization will be responsible for accepting the award, implementing the approved projects/contracts for all consortium member sites, and managing the award throughout the period of performance.

Period of Performance: 24 months

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

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

Projected Period of Performance End Date(s): April 30, 2027

Funding Instrument Type: Grant

Applicant Eligibility Criteria

Eligible nonprofit organizations are those organizations that are:

1. Described under section 501(c)(3) of the Internal Revenue Code of 1986 (IRC) and exempt from tax under section 501(a) of such code. ***This includes entities designated as "private" (e.g., private institutions of higher learning), as private colleges and universities can also be designated as 501 (c)(3) entities.***

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

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

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

3. NSGP-NSS-UA
   a. located **inside** of the FY 2024 St. Louis UASI-designated urban area (St. Louis City and the Missouri Counties of Franklin, Jefferson, St. Charles, and St. Louis and Illinois counties of Madison, St. Clair, and Monroe)
   b. located **inside** of the FY 2024 Kansas City UASI-designated urban area (Missouri Counties of Jackson, Cass, Platte, Clay, and Ray and Kansas counties of Leavenworth, Wyandotte, and Johnson)

4. NSGP-NSS-S, located within the State of Missouri **outside** of the FY 2024 St. Louis UASI-designated urban area (St. Louis City and the Missouri Counties of Franklin, Jefferson, St. Charles, and St. Louis) and Kansas City UASI-designated urban area (Missouri Counties of Jackson, Cass, Platte, Clay, and Ray)

5. For the NSGP-NSS, a consortium of eligible nonprofit organizations is eligible. An eligible nonprofit organization would act as a lead and submit an application for funding on behalf of itself and other eligible NSGP-NSS eligible nonprofit organizations (up to ten sites/locations).

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

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

Application and Submission Information

1. Key Dates and Times

a. Application Start Date: October 30, 2024

b. Application Submission Deadline: December 2, 2024, 5:00 p.m. CST

2. Agreeing to Terms and Conditions of the Award

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

Nonprofit Organization Specific Application Instructions

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

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

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

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

NSGP-NSS Application Submission Requirements (Non-Consortium Applicants)

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

1. NSGP-NSS Investment Justification (IJ)

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

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

- Be for the location(s)/physical address that the nonprofit occupies at the time of application
- Address an identified risk, including threat and vulnerability, regardless of whether it is submitting for similar projects at multiple sites
- Demonstrate the ability to provide enhancements consistent with the purpose of the program and guidance provided by DHS/FEMA
- Be both feasible and effective at reducing the risks for which the project was designed
- Be able to be fully completed within the two-year period of performance
- Be consistent with all applicable requirements outlined in the NOFO and the Preparedness Grants Manual.

Applicants are required to self-identify with one of the following four categories in the IJ as part of the application process:

1. Ideology-based/Spiritual/Religious (Houses of Worship, Educational Institutions, Medical Facilities, etc.)
2. Educational (secular)
3. Medical (secular)
4. Other

The **fillable version of the NSGP-NSS IJ** must be submitted as an attachment to the application through the WebGrants System. Non-fillable and older versions of the IJ will **NOT** be accepted. **If a non-fillable IJ or older version of the IJ is submitted, the application will be deemed ineligible.**

If you are submitting for more than one site/location, you must submit an application for each site/location in the WebGrants System.

2. Vulnerability/Risk Assessment

Each applicant must include a vulnerability/risk assessment **unique to the site** the IJ is being submitted for.

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

3. Mission Statement

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

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

4. Audit

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

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

5. 501(c)(3) Documentation

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

NSGP-NSS Application Submission Requirements (Consortium Applicants)

As part of the NSGP-NSS consortium application, the lead nonprofit organization within the consortium must submit the same documents as non-consortium applications as listed above. However, the responses must represent the collective of the consortium:

1. NSGP-NSS Investment Justification (IJ)

Each nonprofit organization with one site in the consortium may apply for up to $200,000 for that site. Consortium applications are limited to a maximum of $1,000,000 per consortium. A fillable IJ form is available on the DPS website under Grant Applications and Forms, Nonprofit Security

Grant Program National Security Supplemental (NSGP-NSS). The IJ form will also be linked in the WebGrants System.

The IJ must summarize the goal for the consortium investments proposed for funding. The investments or projects in the IJ must:

- Address an identified risk, including threat and vulnerability that will be mitigated by the consortium investment
- Demonstrate the ability to provide enhancements consistent with the purpose of the program and guidance provided by DHS/FEMA
- Be both feasible and effective at reducing the risks for which the project was designed
- Be able to be fully completed within the two-year period of performance
- Be consistent with all applicable requirements outlined in the NOFO and the Preparedness Grants Manual.

The consortia lead nonprofit organization is required to self-identify with one of the following four categories in the IJ as part of the application process:

5. Ideology-based/Spiritual/Religious (Houses of Worship, Educational Institutions, Medical Facilities, etc.)
6. Educational (secular)
7. Medical (secular)
8. Other

In **Part I** of the IJ, Nonprofit Organization Subapplicant Information, the lead nonprofit organization of the consortium must complete the required fields based solely on the lead nonprofit organization's information.

In **Part II** of the IJ, Background Information, the lead nonprofit organization of the consortium must summarize the shared background information of all nonprofit organizations within the consortium.

In **Part III** of the IJ, Risk, the lead nonprofit organization of the consortium must summarize the threats, vulnerabilities, and potential consequences facing all nonprofit organizations within the consortium. Additional space for further detail is available in the Consortium Workbook.

In **Part IV** of the IJ, Facility Hardening, the lead nonprofit organization of the consortium must summarize how the proposed activities or investments of the consortium address the shared vulnerabilities identified in Part III. For Section IV-B, the lead organization must input the total funding requested for all nonprofit organizations within the consortium under each AEL investment.

In **Part V** of the IJ, Milestone, the lead nonprofit organization of the consortium must provide the key milestones from all nonprofit organizations within the consortiums proposed activities.

In **Part VI** of the IJ, Project Management, an individual must be identified from solely the lead nonprofit organization that will oversee the projects carried out by the nonprofit organizations in the consortium and assess their plan.

In **Part VII** of the IJ, Impact, the lead nonprofit organization of the consortium must describe the key measurable outputs and outcomes for all nonprofit organizations within the consortium's investments.

In **Funding History and the Nonprofit Subapplicant Contact Information sections**, the lead nonprofit organization of the consortium must complete the required fields based solely on the lead nonprofit organization's investments.

The **fillable version of the NSGP-NSS IJ** must be submitted as an attachment to the application through the WebGrants System. Nson-fillable and older versions of the IJ will **NOT** be accepted. **If a non-fillable IJ or older version of the IJ is submitted, the application will be deemed ineligible.**

The lead nonprofit organization should be the submitting agency for the application in the WebGrants System.

2. NSGP-NSS Consortium Workbook

Full Consortium Workbook Instructions are found in the instructions tab of the Consortium Workbook.

The Consortium Workbook must expand upon the information provided in the consortium lead nonprofit organization's IJ. The Consortium Workbook must contain the number of nonprofit organizations within the consortium and the following information for each nonprofit organization within the consortium:

a. **Demographic information**, including the name, address, nonprofit organization type, organization function, and organization affiliation;
b. **Required programmatic information**, including eligibility information, UEI number (lead consortium member only), past funding history, total funding requested per site, and a point of contact for each nonprofit organization; and
c. **Additional narrative information**, including how each nonprofit organization's projects address the objective of the consortium application as outlined in the lead nonprofit organization's IJ.

The Consortium Workbook must be submitted as an attachment the application through the WebGrants System for all consortium applications.

3. Vulnerability/Risk Assessments

Consortia have the option to either submit individual Vulnerability/Risk Assessments for each nonprofit in the consortium or a shared vulnerability/risk assessment that reflects the collective risks faced by all consortium members as summarized in the IJ.

The Vulnerability/Risk Assessments must be submitted as an attachment to the application through the WebGrants System. If individual Vulnerability/Risk Assessments were completed for each nonprofit organization in the consortium, they must be clearly labeled to identify the nonprofit organization. All of the Vulnerability/Risk Assessments must be combined into a single file and uploaded in the Vulnerability/Risk Assessment section of the Named Attachments Form in the WebGrants System.

4. Mission Statement

Each consortium must submit Mission Statements for all participating nonprofit organizations in the consortium and any mission implementation policies or practices that may elevate the organization's risk.

The Mission Statement must be submitted as an attachment to the application through the WebGrants System. Mission Statements for each nonprofit organization in the consortium must be submitted. The Mission Statements must be clearly labeled to identify the nonprofit organization. All of the Mission Statements must be combined into a single file and uploaded in the Mission Statement section of the Named Attachments Form in the WebGrants System.

5. Audit

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

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

6. 501(c)(3) Documentation

Consortia members, that are required by the IRS to apply for and receive a recognition of exemption under section 501 (c)(3), must submit recognition of exemption for all participating nonprofit organizations. The 501 (c)(3) documentation must be clearly labeled to identify the nonprofit organization. All of the 501 (c)(3) documentation must be combined into a single file and uploaded in the 501 (c)(3) Documentation section of the Named Attachments Form in the WebGrants System.

Funding Restrictions and Allowable Costs

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

Federal funds made available through this award may be used for the purpose set forth in this NOFO, the Preparedness Grants Manual, and the terms and conditions of the award and must be consistent with the statutory authority for the award. Award funds may not be used for matching funds for any other federal awards, lobbying, or intervention in federal regulatory or adjudicatory proceedings. In addition, federal funds may not be used to sue the Federal Government or any other government entity. See the Preparedness Grants Manual for more information on funding restrictions and allowable costs.

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

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

Guidance is available at Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services (Interim) FEMA Policy #405-143-1, or superseding document.

Additional guidance is available at Contract Provisions Guide: Navigating Appendix II to Part 200 – Contract Provisions for Non-Federal Entity Contracts Under Federal Awards (fema.gov).

Effective August 13, 2020, FEMA recipients and subrecipients **may not** use any FEMA funds under open or new awards to:

a. Procure or obtain any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology of any system;

b. Enter into, extend, or renew a contract to procure or obtain any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology of any system; or

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

I. Replacement Equipment and Services

FEMA grant funding may be permitted to procure replacement equipment and services impacted by this prohibition, provided the costs are otherwise consistent with the requirements of the funding notice, the Preparedness Grants Manual, and any other state-specific requirements.

II. Covered Telecommunications

Per section 889(f)(2)-(3) of the FY 2019 NDAA and 2 C.F.R. § 200.216, covered telecommunications equipment or services means:

i. Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation, (or any subsidiary or affiliate of such entities);

ii. For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by

Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);

iii. Telecommunications or video surveillance services provided by such entities or using such equipment; or

iv. Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the People's Republic of China.

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

2. Pre-Award Costs

Nonprofit organization applicants cannot claim pre-award costs except in exigent circumstances. Please contact the DPS/OHS should exigent circumstances exist.

3. Management and Administration (M&A) Costs

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

M&A costs are for activities directly related to the management and administration of the award. M&A activities are those defined as directly relating to the management and administration of NSGP-NSS funds, such as financial management and monitoring. M&A expenses must be based on actual expenses or known contractual costs. Requests that are simple percentages of the award, without supporting justification, will not be allowed or considered for reimbursement.

M&A costs are not operational costs, but are necessary costs incurred in direct support of the federal award or as a consequence of it. 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.

4. Indirect Facilities & Administrative (F&A) Costs

Indirect (F&A) costs (IDC) mean those costs incurred for a common or joint purpose benefitting more than one cost objective and not readily assignable to the cost objectives specifically benefitted, without effort disproportionate to the results achieved. Indirect costs are allowable under this program as described in 2 C.F.R. Part 200, including 2 C.F.R. § 200.414. Applicants with a current negotiated indirect cost rate agreement that desire to charge indirect costs to a federal award must provide a copy of their negotiated indirect cost rate agreement at the time of application. Not all applicants are required to have a current negotiated indirect cost rate agreement. Applicants that are not required to have a negotiated indirect cost rate agreement but are required to develop an indirect cost rate proposal must provide a copy of their proposal at the

time of application. Applicants who do not have a current negotiated indirect cost rate agreement (including a provisional rate) and wish to charge the de minimis rate must reach out to the DPS/OHS for further instructions. Applicants who wish to use a cost allocation plan in lieu of an indirect cost rate must also reach out to the DPS/OHS.

5. Other Direct Costs

a. Planning

Funding may be used for security or emergency planning expenses and the materials required to conduct planning activities. Planning must be related to the protection of the facility and the people within the facility and should include consideration of access and functional needs as well as those with limited English proficiency. Planning efforts can also include conducting risk and resilience assessments on increasingly connected cyber and physical systems, on which security depends, using the Resilience Planning Program and related CISA resources. Examples of planning activities allowable under this program include:

- Development and enhancement of security plans and protocols
- Development or further strengthening of security assessments
- Emergency contingency plans
- Evacuation/Shelter-in-place plans
- Coordination and information sharing with fusion centers
- Other project planning activities with prior approval from FEMA/DPS/OHS

b. Organization

Organization costs are not allowed under this program.

c. Equipment

Allowable costs are focused on facility hardening and physical security enhancements. Funding can be used for the acquisition and installation of security equipment on real property (including buildings and improvements) owned or leased by the nonprofit organization, specifically in prevention of and/or protection against the risk of a terrorist or other extremist attack. This equipment is **limited to select items** on the Authorized Equipment List (AEL):

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 provide warning to the public in the event of an incident, such as sirens, the Emergency Alert System (EAS), the Integrated Public Alert and Warning System (IPAWS), and Wireless Emergency Alerts (WEA).
04AP-11-SAAS	Applications, Software as a Service	Sometimes referred to as "on-demand software," this application runs on the provider's servers, delivering functionality via the internet to any device having connectivity and the required browser or interface. Access to the application is obtained via a service subscription rather than outright purchase, with all updates and configuration requirements handled by the service provider. This item is limited to those services that support security systems such as access controls, camera networks, cybersecurity services, or other critical infrastructure security.
05AU-00-TOKN	System, Remote Authentication	Systems used to provide enhanced remote authentication, often consisting of a server or synchronization scheme and a device, token, or smartphone application.
05EN-00-ECRP	Software, Encryption	Encryption software used to protect stored data files or email messages.
05HS-00-MALW	Software, Malware/Anti-Virus Protection	Software for protection against viruses, spyware, and malicious code. May be obtained for individual hosts or for entire network segments.

05HS-00-PFWL	System, Personal Firewall	Personal firewall for operation on individual workstations. This item is usually a software solution, but appliances are also available. See also: 05NP-00-FWAL.
05NP-00-FWAL	Firewall, Network	Firewall (software or standalone appliance) for use in protecting networks. See also 05HS-00-PFWL.
05NP-00-IDPS	System, Intrusion Detection/Prevention	Intrusion Detection and/or Prevention System deployed at either host or network level to detect and/or prevent unauthorized or aberrant (i.e., abnormal) behavior on the network.
06CP-01-PORT	Radio, Portable	Individual/portable radio transceivers, for notifications and alerts.
06CP-01-REPT	Repeater	Electronic device that receives a weak or low-level signal and retransmits that signal to extend usable range.
06CC-02-PAGE	Services/Systems, Paging	Paging services/systems/applications; one-way text messaging for notifications or alerts.
06CP-03-ICOM	Intercom/Intercom System	Communication system for a limited number of personnel in close proximity to receive alerts or notifications.
06CP-03-PRAC	Accessories, Portable Radio	Speaker/microphone extensions to portable radios.
10GE-00-GENR	Generators	Generators (gasoline, diesel, propane, natural gas, etc.) and their required installation materials, including 10PE-00-PTSW (a power switch) if not already included, to support a redundant power supply for security systems, alarms, lighting, and other physical security/cybersecurity infrastructure or systems.
10PE-00-UPS	Supply, Uninterruptible Power (UPS)	Systems that compensate for power loss to serviced equipment (e.g., short-duration battery devices, standby generator devices for longer duration).
13IT-00-ALRT	System, Alert/Notification	Alert/notification software that allows for real-time dissemination of information for situational awareness or alerts among a group via means such as smartphones, landlines, pagers, etc. This item may also be a subscription cloud-based service using

		a web browser interface or a mobile application instead of a software.
14CI-00-COOP	System, Information Technology Contingency Operations	Back-up computer hardware, operating systems, data storage, and application software necessary to provide a working environment for contingency operations. May be a purchased as a remote service or a dedicated alternate operating site.
14EX-00-BCAN	Receptables, Trash, Blast-Resistant	Blast-resistant trash receptacles.
14EX-00-BSIR	Systems, Building, Blast/Shock/Impact Resistant	Systems to mitigate damage from blasts, shocks, or impacts, such as column and surface wraps, wall coverings, portable or fix ballistic boards/barriers, breakage/shatter resistant glass, window wraps/films/velums, etc.
14SW-01-ALRM	Systems, Sensors, Alarm	Systems and standalone sensors designed to detect access violations or intrusions using sensors such as door/window switches, motion sensors, acoustic sensors, seismic sensors, and thermal sensors. May also include temperature sensors for critical areas.
14SW-01-ASTN	Network, Acoustic Sensor Triangulation	Network of deployed acoustic sensors and one or more processing nodes for data integration and analysis. Such networks can be set to one or more ranges of frequencies to detect sounds such as gunshots, heavy weapons discharge, explosions, man-portable air defense system launches, vehicle noises, etc., and utilize acoustic triangulation to provide accurate location data. Such networks can be wired, wireless, or hybrid, and are capable of operation near critical infrastructure assets or in wide areas.
14SW-01-DOOR	Doors and Gates, Impact Resistant	Reinforced doors and gates with increased resistance to external impact for increased physical security.
14SW-01-LITE	Lighting, Area, Fixed	Fixed high-intensity lighting systems for improved visibility in areas such as building perimeters, parking lots, and other critical zones to increase physical security.
14SW-01-PACS	System, Physical Access Control	Locking devices and entry systems for control of physical access to facilities.

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

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

Unless otherwise stated, equipment must meet all mandatory statutory, regulatory, and FEMA-adopted standards to be eligible for purchase using these funds, including the Americans with Disabilities Act. In addition, recipients will be responsible for obtaining and maintaining all necessary certifications and licenses for the requested equipment, whether with NSGP-NSS funding or other sources of funds.

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

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

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

d. Training and Exercises

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

Nonprofit organizations may use NSGP-NSS funds for the following training-related costs:

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

Allowable training-related costs under the NSGP-NSS are limited to attendance fees for training and related expenses, such as materials, supplies, and/or equipment. Overtime, backfill, and travel expenses are **NOT** allowable costs.

Allowable training topics are limited to the protection of critical infrastructure key resources, including physical and cybersecurity, facility hardening, and terrorism/other extremism awareness/employee preparedness such as Community Emergency Response Team (CERT) training, indicators and behaviors indicative of terrorist/other extremist threats, Active Shooter training, and emergency first aid training. Additional examples of allowable training courses include: "Stop the Bleed" training, kits/equipment, and training aids; First Aid and other novice level "you are the help until the help arrives" training, kits/equipment, and training aids; and

Automatic External Defibrillator (AED) and AED/Basic Life Support training, kits/equipment, and training aids.

Training conducted using NSGP-NSS funds must address a specific threat and/or vulnerability, as identified in the nonprofit organization's Investment Justification. Training should provide the opportunity to demonstrate and validate skills learned as well as to identify any gaps in these skills. Proposed attendance at training courses and associated costs using the NSGP-NSS must be included in the nonprofit organization's IJ.

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

The Homeland Security Exercise and Evaluation Program (HSEEP) provides a set of guiding principles for exercise programs, as well as a common approach to exercise program management, design and development, conduct, evaluation, and improvement planning. For additional information on HSEEP, refer to Homeland Security Exercise and Evaluation Program. In accordance with HSEEP guidance, subrecipients are reminded of the importance of implementing corrective actions iteratively throughout the progressive exercise cycle. This link provides access to a sample After Action Report (AAR)/Improvement Plan (IP) template: Improvement Planning – HSEEP Resources – Preparedness Toolkit.

e. Maintenance and Sustainment

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

f. Construction and Renovation

NSGP-NSS funding may not be used for construction and renovation projects without prior written approval from FEMA. In some cases, the installation of equipment may constitute construction and/or renovation. If you have any questions regarding whether an equipment installation project could be considered construction or renovation, please

contact the DPS/OHS. The total cost of any construction or renovation paid for using NSGP funds may not exceed 15% of the NSGP award.

g. Contracted Security

Contracted security personnel are allowed under this program only as described in this funding notice and must comply with guidance set forth in IB 441. NSGP-NSS funds may not be used to purchase equipment for contracted security.

Unallowable Costs

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

- Organization costs, and operational overtime costs
- Hiring of public safety personnel
- General-use expenditures
- Overtime and backfill
- Initiatives that do not address the implementation of programs/initiatives to build prevention and protection-focused capabilities directed at identified facilities and/or the surrounding communities
- The development of risk/vulnerability assessment models
- Initiatives that fund risk or vulnerability security assessments or the development of the IJ
- Initiatives in which federal agencies are the beneficiary or that enhance federal property
- Initiatives which study technology development
- Proof-of-concept initiatives
- Initiatives that duplicate capabilities being provided by the Federal Government
- Organizational operating expenses
- Reimbursement of pre-award security expenses
- Cameras for license plate readers/license plate reader software
- Cameras for facial recognition software
- Weapons or weapons-related training
- Knox boxes

Administrative and National Policy Requirements

In addition to the requirements in this section and in this NOFO, FEMA/DPS/OHS may place specific terms and conditions on individual awards in accordance with 2 C.F.R. Part 200.

In addition to the information regarding DHS Standard Terms and Conditions and Ensuring the Protection of Civil Rights, see the Preparedness Grants Manual for additional information on administrative and national policy requirements, including the following:

- Environmental Planning and Historic Preservation (EHP) Compliance
- FirstNet
- National Incident Management System (NIMS) Implementation
- SAFECOM Guidance on Emergency Communications Grants

1. DHS Standard Terms and Conditions

All successful applicants for DHS grant and cooperative agreements are required to comply with DHS Standard Terms and Conditions, which are available online at: DHS Standard Terms and Conditions.

The applicable DHS Standard Terms and Conditions will be those in effect at the time the award was made. What terms and conditions will apply for the award will be clearly stated in the award package at the time of award.

2. Ensuring the Protection of Civil Rights

As the Nation works towards achieving the National Preparedness Goal, it is important to continue to protect the civil rights of individuals. Subrecipients must carry out their programs and activities, including those related to the building, sustainment, and delivery of core capabilities, in a manner that respects and ensures the protection of civil rights for protected populations.

Federal civil rights statutes, such as Section 504 of the Rehabilitation Act of 1973 and Title VI of the Civil Rights Act of 1964, along with DHS and FEMA regulations, prohibit discrimination on the basis of race, color, national origin, sex, religion, age, disability, limited English proficiency, or economic status in connection with programs and activities receiving federal financial assistance from FEMA, as applicable.

The DHS Standard Terms and Conditions include a fuller list of the civil rights provisions that apply to recipients. These terms and conditions can be found in the DHS Standard Terms and Conditions. Additional information on civil rights provisions is available at FEMA: External Civil Rights Division.

In accordance with civil rights laws and regulations, subrecipients must ensure the consistent and systematic fair, just and impartial treatment of all individuals, including individuals who belong to underserved communities that have been denied such treatment.

3. Environmental Planning and Historic Preservation (EHP) Compliance

FEMA must consider the effects of its actions on the environment and historic properties to ensure that all activities and programs funded by FEMA, including grant-funded projects, comply with federal Environmental Planning and Historic Preservation (EHP) regulations, laws, Executive Orders (EO), as applicable.

Subrecipients proposing projects that have the potential to impact the natural or built environment, including, but not limited to, the construction of communication towers, modification or renovation of existing buildings, structures and facilities, new construction including replacement of or relocation of facilities, and some training activities must participate in the FEMA EHP review process. The EHP review process involves the submission of a detailed project description along with any supporting documentation requested by FEMA to determine whether the proposed project has the potential to impact the environmental resources, including but not limited to, threatened or endangered species and historic properties, identify mitigation measures and/or alternative courses of action that may lessen any impact to those resources and bring the project into compliance with EHP requirements.

In some cases, FEMA is also required to consult with other regulatory agencies and the public in order to complete the review process. Federal law requires EHP review to be completed before funds are released

to carry out the proposed project. FEMA may not be able to fund projects that are not incompliance with EHP laws, Executive Orders, regulations and policies.

DHS and FEMA EHP policy is found in directives and instructions available on the FEMA Environmental and Historic Preservation Guidance for FEMA Grant Applications, and includes documents regarding EHP responsibilities and program requirements, including implementation of the National Environmental Policy Act and other EHP laws, regulations and Executive Orders. Information on the DHS and FEMA EHP policy is also found at EHP Directive & Instruction.

An EHP Screening Form and supporting documentation for preparedness projects requiring EHP review should be submitted to DPS/OHS. Additionally, all subrecipients under this funding opportunity are required to comply with the FEMA Policy #108-023-1, Revision 2 Grant Programs Directorate Environmental Planning and Historic Preservation Policy Guidance.

4. Monitoring and Oversight

The regulation at 2 C.F.R. § 200.337 provides DHS and any of its authorized representatives with the right of access to any documents, papers, or other records of the subrecipient that are pertinent to a federal award in order to make audits, execute site visits, or for any other official use. The right also includes timely and reasonable access to the subrecipient's personnel for the purpose of interview and discussion related to such documents. Pursuant to this right and per 2 C.F.R. § 200.329, DHS/DPS/OHS may conduct desk reviews and make site visits to review project accomplishments and management control systems to evaluate project accomplishments and to provide any required technical assistance. During site visits, DHS/DPS/OHS may review a subrecipient's files pertinent to the federal award and interview and/or discuss these files with the subrecipient's personnel. Subrecipient's must respond in a timely and accurate manner to DHS requests for information relating to a federal award.

5. Build America, Buy America Act

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

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

The Buy America preference only applies to articles, materials, and supplies that are consumed in, incorporated into, or affixed to an infrastructure project. As such, it does not apply to tools, equipment, and supplies, such as temporary scaffolding, brought to the construction site and removed at or before the completion of the infrastructure project. Nor does a Buy America preference apply to equipment and furnishings, such as movable chairs, desks, and portable computer equipment, that are used at or within the finished infrastructure project but are not an integral part of the structure or permanently affixed to the infrastructure project. For FEMA's official policy on BABAA, please see FEMA Policy 207-22-0001: Buy America Preference in FEMA Financial Assistance Programs for Infrastructure. To see whether a particular FEMA federal financial assistance program is considered an infrastructure program and thus required to include a Buy America preference, please see Programs and Definitions: Build America, Buy

America Act and https://www.fema.gov/sites/default/files/documents/fema_build-america-buyamerica-act-policy.pdf.

a. Waivers

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

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

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

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

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

Contact Information:

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

Applications must be submitted through the WebGrants System.

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

Debbie Musselman
Grants Specialist
(573) 751-5997
Debbie.Musselman@dps.mo.gov

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

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

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