**The Department of Homeland Security (DHS)**

Notice of Funding Opportunity (NOFO)

Fiscal Year 2025 Port Security Grant Program (PSGP)

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.

## Contents

## 1. Basic Information

| | |
|---|---|
| **A.** Agency Name | U.S. Department of Homeland Security (DHS), Federal Emergency Management Agency (FEMA) |
| **B.** NOFO Title | Fiscal Year 2025 Port Security Grant Program (PSGP) |
| **C.** Announcement Type | Initial |
| **D.** Funding Opportunity Number | DHS-25-GPD-056-00-99 |
| **E.** Assistance Listing Number | 97.056 |
| **F.** Expected Total Funding | $90,000,000 |
| **G.** Anticipated Number of Awards | 200 awards |
| **H.** Expected Award Range | $10,000 – $6,500,000 |
| **I.** Projected Application Start Date | 08/01/2025 12:00 p.m. Eastern Time (ET) |
| **J.** Projected Application End Date | 08/15/2025 05:00 p.m. Eastern Time (ET) |
| **K.** Anticipated Funding Selection Date | No later than August 23, 2025 |
| **L.** Anticipated Award Date | No later than September 30, 2025 |
| **M.** Projected Period of Performance Start Date | 09/01/2025 |
| **N.** Projected Period of Performance End Date | 08/31/2028 |
| **O.** Executive Summary | The PSGP is focused on enhancing security of Maritime Facilities within U.S. navigable waterways. Funding is prioritized towards terrorism prevention, response, recovery, and mitigation based on port area risk through implementation of Area Maritime Transportation Security Plans and facility security plans among port authorities, facility operators, and state and local government agencies required to provide port security services and to train public safety personnel under section 70132 of Title 46. |

| | |
|---|---|
| **P.** Agency Contact | **a. *Program Office Contact***<br>FEMA has assigned region-specific Preparedness Officers for the PSGP. If you do not know your Preparedness Officer, please contact FEMA Grants News by phone at (800) 368-6498 or by email at fema-grants-news@fema.dhs.gov, Monday through Friday, 9:00 AM – 5:00 PM ET.<br><br>**b. *FEMA Grants News***<br>This channel 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 Team is reachable at fema-grants-news@fema.dhs.gov. OR (800) 368-6498, Monday through Friday, 9:00 AM – 5:00 PM ET.<br><br>**c. *Grant Programs Directorate (GPD) Award Administration Division***<br>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.<br><br>**d. *FEMA Regional Offices***<br>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 https://www.fema.gov/fema-regional-contacts.<br><br>**e. *Civil Rights***<br>Consistent with Executive Order 14173, *Ending Illegal Discrimination & Restoring Merit-Based Opportunity*, the FEMA Office of Civil Rights 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-CivilRightsOffice@fema.dhs.gov.<br><br>**f. *Environmental Planning and Historic Preservation***<br>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.<br><br>**g. *FEMA GO***<br>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, 9:00 AM – 6:00 PM ET. |

| | |
|---|---|
| | **h. *Preparedness Grants Manual***<br>Recipients seeking guidance on policies and procedures for managing preparedness grants should reference the Preparedness Grants Manual at Preparedness Grants Manual. |

## 2. Eligibility

| | |
|---|---|
| **A.** Eligible Entities/Entity Types | Only the following entities or entity types are eligible to apply.<br><br>**a. *Applicants***<br>1. Eligible Applicants<br><br>All entities subject to an Area Maritime Security Plan (AMSP), as defined by 46 U.S.C. § 70103(b), may apply for PSGP funding. Eligible applicants include port authorities, facility operators, and state, local, and territorial government agencies. A facility operator owns, leases, or operates any structure or facility of any kind located in, on, under, or adjacent to any waters subject to the jurisdiction of the United States. Facility operators include those that are subject to the AMSP and verified by the Captain of the Port (COTP), which may include but are not limited to terminal operators, ferry systems, bar/harbor pilots, and merchant's exchanges. See the "Applications Submitted by Eligible Entities" section below for further detail.<br><br>2. Applicant Eligibility<br><br>Pursuant to the Maritime Transportation Security Act of 2002 (MTSA), Pub. L. No. 107-295, as amended, DHS established a risk-based grant program to support maritime security risk management. Funding is directed towards the implementation of AMSPs, Facility Security Plans (FSP), and Vessel Security Plans (VSP) among port authorities, facility operators, and state and local government agencies that are required to provide port security services. Entities, whether public or private, who provide maritime security services on a for hire basis are not eligible applicants (i.e. security companies, see "Subapplicants" below for additional detail). In administering the grant program, national, economic, energy, and strategic defense concerns based upon the most current risk assessments available will be considered.<br><br>**Port Area Definition**<br>A Port Area is a location on a coast, shore, or inland waterway containing one or more harbors where vessels can dock and transfer people or cargo to or from land. For the purposes of the PSGP, eligible ports included those identified by the U.S. Army Corps of Engineers (USACE) Principal Port List (PPL), as well as unlisted ports which have the presence of MTSA-regulated facilities. |

**Applications Submitted by Eligible Entities**
Subject to the information and exceptions in this section, ***an eligible entity may submit only one application within each Port Area. An application may contain up to five Investment Justifications (IJs).*** See Section D, below, for further instructions regarding IJs.

- A single eligible entity may have multiple facilities, departments, subcomponents, or agencies operating within a Port Area. ***FEMA will generally view multiple agencies within a local government (e.g., police department, fire department, emergency management office) operating within one Port Area as a single eligible entity.*** An applicant's Employer Identification Number (EIN) will help inform FEMA's determination of which applicants may constitute a single eligible entity.
  - An eligible entity operating multiple facilities, departments, subcomponents, or agencies within a single Port Area **may choose to submit separate applications** for facilities, departments, subcomponents, or agencies within it, but any such separate applications will be considered part of the same eligible entity for **purposes of the cost-share requirements** and limited to 5 projects total.
  - If a single eligible entity chooses to have its components submit separate applications, each individual facility, department, subcomponent, or agency of that single eligible entity should submit no more than one application. For example, a police department should submit no more than one collective application. If an individual facility, department, subcomponent, or agency of an eligible entity submits more than one application for a single Port Area, FEMA reserves the discretion to consolidate the projects or determine which application(s) to approve or deny.
- Funding allocation decisions are based partially on Port Area risk. Therefore, ***no single application should include IJs for projects intended to be implemented in multiple Port Areas.*** Applications that include multiple port areas may be deemed ineligible in whole or part. For example, a state agency or facility operator that operates in multiple Port Areas must submit separate applications to fund projects in each Port Area.
  - Exception: "Hub and spoke" cybersecurity projects may affect a parent organization's multiple eligible entities in multiple Port Areas. Such projects may be submitted within a primary Port Area for the project implementation. Proportionally, costs associated with *entities or*

| | |
|---|---|
| | *subcomponents that are not covered under an AMSP and are not instrumental to enhancing maritime security* must not be included in the detailed budget worksheet or IJ and thereby prorating the cost of the project only to those facilities that are covered by the AMSP.<br><br>**b. *Subapplicants***<br>Subapplicants and subawards are not allowed.<br><br>Applicants are **prohibited from applying on behalf of other, separate entities**. Notwithstanding this prohibition, community-based projects for maritime security planning, training, exercises, port-wide cyber vulnerability assessments and cyber interoperability projects may include multiple beneficiaries (participants from other separate entities). Only recipient incurred expenses are eligible under PSGP awards, meaning that 3rd party participating entities are responsible for their own incurred expenses.<br><br>For example, a port authority hosts a large exercise and may receive funding for port authority personnel expenses, venue rental, and contracted design/development/conduct of the exercise, but other participating agencies are responsible for their own incurred expenses for personnel, fringe benefits, equipment, travel, etc.<br><br>The primary purpose and use of PSGP funded equipment is for the recipient and only the recipient is permitted to take ownership of PSGP-funded equipment and other non-consumables until disposition actions are required.<br><br>Vendor, manufacturer, or service provider submitted applications on behalf of potential 'recipients' will not be considered for funding.<br><br>***c. All Recipients – Compliance with Federal Immigration Laws***<br>An immigration term and condition may be material to the Department of Homeland Security's decision to make this grant award, and the Department of Homeland Security may take any remedy for noncompliance, including termination, if the state or territorial recipient or any local government subrecipient fails to comply with this term and condition. No final agency determination has been made as of the date of this publication. |
| **B.** Project Type Eligibility | **a. *Unallowable Project Types***<br>See Section 3.F "Program-Specific Unallowable Costs" for more information on unallowable project types."<br><br>**b. *Allowable Project Types***<br>Costs generally need to fit within one of the categories listed below to be allowable under this program. |

| | |
|---|---|
| | Specific investments made in support of the NOFO funding priorities generally fall into one of the following allowable cost categories:<br><br>• Planning<br>• Operational Activities<br>• Equipment and Capital Projects<br>• Training and Awareness Campaigns<br>• Exercises<br><br>Please see the Appendix A for more information on these allowable categories. Applicants who have questions about whether a cost is allowable under this program should contact their Preparedness Officer. |
| **C.** Requirements for Personnel, Partners, and Other Parties | 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.<br><br>Further, the Authorized Organization Representative (AOR) and Signatory Authority (SA) must be a duly authorized current employee, personnel, official, staff, 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 or SA of the recipient. It is the sole responsibility of the recipient to keep their points of contact for the organization up-to-date and accurate in all federal systems.*** |
| **D.** Maximum Number of Applications | The maximum number of applications that can be submitted is:<br>1. One per eligible entity/subcomponent per Port Area<br><br>For additional information, see Section 2A "Eligible Entities/Entity Types." |
| **E.** Additional Restrictions | Applicants or recipients are required to certify their compliance with federal statues, DHS directives, polices, and procedures.<br><br>**a.** ***National Incident Management System (NIMS) Implementation***<br>Prior to allocation of any federal preparedness awards, recipients must ensure and maintain adoption and implementation of NIMS. The list of objectives used for progress and achievement reporting is on FEMA's website at https://www.fema.gov/emergency-managers/nims/implementation-training. |

| | |
|---|---|
| | Please see the Preparedness Grants Manual for more information on NIMS.<br><br>**b. *Compliance with Maritime Security Regulations***<br>As a condition of eligibility, all PSGP applicants must be fully compliant with relevant Maritime Security Regulations (33 C.F.R. Parts 101-106). Any applicant who, as of the grant application deadline, has an open or outstanding Notice of Violation (NOV) will not be considered for PSGP funding if:<br><br>1. The applicant has failed to pay the NOV within 45 days of receipt of the NOV and the applicant has failed to decline the NOV within 45 days of receipt of the NOV, resulting in the U.S. Coast Guard (USCG) entering a finding of default in accordance with 33 C.F.R. § 1.07- 11(f)(2); or<br>2. The applicant appealed the NOV pursuant to 33 C.F.R § 1.07-70 and received a final appeal decision from the Commandant, USCG, as described in 33 C.F.R. § 1.07-75, and failed to come into compliance with the terms of the final appeal decision within the timelines noted herein.<br><br>The local USCG Captain of the Port (COTP) will verify security compliance eligibility during the field review process. Eligibility does not guarantee grant funding.<br><br>**c. *Ferry Systems***<br>Ferry systems are eligible to apply for PSGP funds. However, any ferry system electing to participate (e.g., submit an application) under the PSGP will not be eligible to participate (e.g., submit an application) under the Transit Security Grant Program (TSGP) and will not be considered for funding under the TSGP. Likewise, any ferry system that participates in the TSGP will not be eligible for funding under the PSGP.<br><br>**d. *Foreign Adversarial System Users***<br>As proscribed in Section 825 of the National Defense Authorization Act (NDAA) for Fiscal Year 2024, Pub. L. No. 118-31 (2023), no funds may be awarded to any covered entity that utilizes or provides in part or in whole: the national transportation logistics public information platform (**commonly referred to as 'LOGINK'**) provided by the People's Republic of China, or departments, ministries, centers, agencies, or instrumentalities of the Government of the People's Republic of China; any national transportation logistics information platform provided by or sponsored by the People's Republic of China, or a controlled commercial entity; or a similar system provided by Chinese state-affiliated entities. |

| | |
|---|---|
| **F.** References for Eligibility Factors within the NOFO | Please see the following references provided below:<br><br>1. "Application Review Information" subsection<br>2. "Financial Integrity Criteria" subsection<br>3. "Supplemental Financial Integrity Criteria and Review" subsection<br>4. FEMA may/will request financial information such as EIN and bank information as part of the potential award selection. This will apply to everyone prospered, including subrecipients. |
| **G.** Cost Sharing Requirement | Applicants selected for this award must commit to an acceptable cost share agreement. Otherwise, they will not be funded. |
| **H.** Cost Share Description, Type and Restrictions | The PSGP has a cost-share requirement. The non-federal entity contribution can be cash (hard match) or third-party in-kind (soft match), with the exception of construction activities, which must be a cash (hard) match. In-kind contributions are defined as third-party contributions per 2 C.F.R. § 200.306.<br><br>All applicants will be required to commit to the cost-share requirement of each project at the time of application. ***The required cost share is based on and calculated against the total of all PSGP funds awarded to an eligible entity as described in the "Applications Submitted by Eligible Entities" section above during this fiscal year within a single Port Area.*** For example, if an entity operates multiple facilities under the same Unique Entity Identifier (UEI) within the same Port Area and each facility requests projects exempt of cost share due to being $25,000 or less, FEMA will view these projects collectively for purposes of determining the appropriate cost share and a cost share will be required if the total exceeds $25,000. As a result, multiple components within a single eligible entity (i.e., port authority, facility operator, local government, or state government) are strongly encouraged to coordinate their applications if they apply separately (even if addressing multiple, disparate projects within the Port Area) for these cost share purposes.<br><br>**Public-Sector Cost Share**<br>***All public sector and non-governmental, nonprofit PSGP award recipients—meaning recipients other than private, for-profit entities—must provide a non-federal entity contribution supporting 25% of the total of all project costs as submitted in the application and approved in the award.*** The non-federal contribution should be specifically identified for each proposed project. The non-federal contribution, whether cash or third-party in-kind match, has the same eligibility requirements as the federal share (e.g., operational costs for routine patrols are ineligible, and operational costs for overtime to conduct an approved exercise may be eligible as part of the IJ) and |

| | |
|---|---|
| | must be justified as part of the project within the investment justification.<br><br>Because the statute at 46 U.S.C. § 70107(c)(1) states that the federal share shall not exceed 75% of the total cost, any application of the percentages that would result in a decimal will be rounded down in favor of the federal share not exceeding 75%, even if normal rounding standards would indicate rounding up in certain instances.<br><br>In accordance with Public Law 96-205, title VI, section 601, Mar. 12,1980 as amended, 48 U.S.C. § 1469a(d), and OMB Controller Alert CA-23-04, Waiving Matching Fund Requirements for Insular Areas (Feb. 6, 2023), agencies are required to waive any requirement for local matching funds for grants to an Insular Area under $200,000, when the match is otherwise required by law. Insular Areas include the U.S. territories of American Samoa, Guam, the U.S. Virgin Islands, and the Commonwealth of the Northern Mariana Islands. For the four Insular Areas, agencies may waive the requirement for matching where the local match amount otherwise required by law is $200,000 or greater. For amounts $200,000 or greater it is at the applicable program's discretion to waive cost shares either in part or in total.<br><br>**Private-Sector Cost Share**<br>***Private, for-profit PSGP award recipients must provide a non-federal entity contribution supporting 50% of the total of all project costs as submitted in the application and approved in the award.*** The non-federal entity contribution should be specifically identified for each proposed project. The non-federal contribution, whether cash (hard) or third-party in-kind (soft), has the same eligibility requirements as the federal share (e.g., operational costs for routine patrols are ineligible, and operational costs for overtime to conduct an approved exercise may be eligible as part of the IJ) and must be justified as part of the project within the IJ.<br><br>Ultimately, the recipient is responsible for ensuring that it contributes the proper cost share to its actual project costs. ***If actual total project costs exceed the projected total project costs stated in the Federal Award, the recipient will not receive any additional federal funding and will be responsible for contributing additional funds above the required cost match.*** If actual total project costs are less than the projected total project costs stated in the federal award, the recipient will be responsible for contributing a cost match calculated as a percentage of those actual project costs. |

| | |
|---|---|
| | Cash and third-party in-kind matches must consist of eligible costs (i.e., same allowability as the federal share) and must be identified as part of the submitted detailed budget worksheet. A cash-match includes cash spent for project-related costs, while a third-party in-kind match includes the valuation of in-kind services. The cost match requirement for the PSGP award may not be met by funds from another federal grant or assistance program, or by funds used to meet matching requirements for another federal grant program, unless otherwise permitted by federal statute. Likewise, third-party in-kind matches used to meet the matching requirement for the PSGP award may not be used to meet matching requirements for any other federal grant program. Additionally, normal routine operational costs cannot be used as a cost match unless a completely new capability is being awarded and must be justified as "reasonable and necessary" to complete the project. Please see 2 C.F.R. § 200.306, as applicable, for further guidance regarding cost matching.<br><br>**Exceptions to the Cost Match Requirements**<br>The following exceptions to the cost match requirement may apply:<br><br>• **Port-Wide Benefit:** The cost match requirements for projects that have a port-wide benefit need only to be funded at the public-sector matching fund level of 25% (with a federal share not to exceed 75% per 46 U.S.C. § 70107(c)(1)). These projects must be certified by the COTP as having a port-wide benefit. Examples of projects with a port-wide benefit include, but are not limited to:<br>  o Port-wide planning, training, and exercises;<br>  o Security camera systems with shared access;<br>  o Response vessels; and<br>  o Other maritime domain awareness systems.<br>• **$25,000 or Less:** There is no matching requirement for grant awards where the total project cost for all projects under the award is $25,000 or less in accordance with 46 U.S.C. § 70107(c)(2)(A). If multiple small projects for the same Port Area by the same entity (i.e., same UEI) are submitted totaling more than $25,000 under this exemption, a cost match is required to be demonstrated at the time of application.<br>• **Public Safety Personnel Security Zone Training:** There is no matching requirement for grants to train public safety personnel in the enforcement of security zones as defined by 46 U.S.C. § 70132 or in assisting in the enforcement of such security zones. Per 46 U.S.C. § 70132(d), the term "public safety personnel" includes any federal, state (or political subdivision thereof), territorial, or tribal law enforcement officer, firefighter, or emergency response provider. |

| | |
|---|---|
| | • **Waiver Requests:** Requests for cost match waivers as outlined in 46 U.S.C. § 70107(c) may be considered for successful applicants only after awards have been made. Applicants must have demonstrated the ability to comply with the cost match requirement at the time of application and since being awarded the grant, have experienced significant financial constraints as outlined in DHS/FEMA Information Bulletin (IB) 376, (i.e., specific economic issues preclude provision of the cost share identified in the original grant application). Cost share waiver requests that do not demonstrate new, post-award difficulties and cost share waivers submitted at the time of application will not be considered. Cost share waiver requests must comply with the process identified in IB 376. |
| **I.** Cost Sharing Calculation Example | **Public Sector:** If the federal award for a public sector recipient requires a 25% cost share and the total project cost is $100,000, then:<br>• Federal share is 75% of $100,000 = $75,000<br>• Recipient cost share is 25% of $100,000 = $25,000<br>**Private Sector:** If the federal award for a private sector recipient requires a 50% cost share and the total project cost is $100,000, then:<br>• Federal share is 50% of $100,000 = $50,000<br>• Recipient cost share is 50% of $100,000 = $50,000 |
| **J.** Required information for verifying Cost Share | Applicants should submit the following cost share (or match) documents:<br>1. FF-207-FY-23-108 (formerly 089-5) IJ-Budget<br>Please see the "Application Format and Contents" subsection for more details. |

## 3. Program Description

**A.** Background, Program Purpose, and Program History

The Port Security Grant Program (PSGP) is one of four grant programs that constitute DHS/FEMA's focus on transportation infrastructure security activities. These grant programs are part of a comprehensive set of measures authorized by Congress and implemented by the Administration to help strengthen the nation's critical infrastructure against risks associated with potential terrorist attacks. The PSGP provides funds to state, local, territorial, and private sector maritime partners to support increased port-wide risk management and protect critical marine transportation system infrastructure from acts of terrorism, major disasters, and other emergencies. Cumulative funding for the PSGP from inception (2001) to present is approximately $3,378,610,706, representing approximately 5,000 grant awards dedicated specifically for enhancing maritime security capabilities throughout U.S. ports

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 cruise and ferry terminals. PSGP 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 2025 NPAs are:

a. Enhancing the protection of soft targets and crowded places,
    i. This includes faith-based organizations and election sites;
b. Supporting Homeland Security Task Forces and fusion centers;
c. Enhancing and integrating cybersecurity resiliency;
d. Enhancing election security; and
e. Supporting Border Crisis Response and Enforcement.
    i. Example activities under border crisis response and enforcement support may include:
        1. Participation in the Department of Homeland Security/Immigration and Customs Enforcement 287(g) training program;
        2. Cooperation with Immigration and Customs Enforcement detainers; and
        3. Other jurisdictional responsibilities to support the enforcement of United States immigration law.

For FY 2025, the Administration encourages applicants to propose innovative solutions that support the broader homeland security mission reflected in the NPAs, as applicable. Applicants must clearly demonstrate how their proposed projects address an NPA and how they align with the stated purpose and objectives of this NOFO. Projects that do so will have their final review scores increased by a multiplier of 20%.

For FY 2024, 466 applications were received and 203 were approved for funding. For a full list of recipients, please refer to Information Bulletin (IB) 517a.

**B.** Goals, Objectives, and Priorities

Goals: The goal of PSGP is strengthened port-wide risk management and protection of critical surface transportation infrastructure from acts of terrorism, major disasters, and other emergencies.

Objectives: PSGP provides resources that support port authorities; facility operators; and state, local, and territorial agencies in meeting the following objectives:

1. Build and sustain core capabilities of maritime infrastructure systems in alignment with the FY 2025 NPAs.
2. Address and close gaps identified in Area Maritime Security Plans and Facility Security Plans.

3. Implement a comprehensive and coordinated (all-inclusive) approach to address enduring security needs of communities that includes planning, training and awareness campaigns, equipment and capital projects, and exercises.

Priorities: Given the evolving threat landscape, it is incumbent upon DHS/FEMA to continuously evaluate the national risk profile and set priorities that help ensure appropriate allocation of scarce security dollars. The FY 2025 NPAs reflect FEMA's broader mission across all preparedness efforts. Applicants should be familiar with these NPAs, as they represent DHS's current focus areas and may shape future guidance:

1. Enhancing the protection of soft targets and crowded places,
    a. 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. Supporting Border Crisis Response and Enforcement.
    a. Example activities under border crisis response and enforcement support may include:
    b. Participation in the Department of Homeland Security/Immigration and Customs Enforcement 287(g) training program;
    c. Cooperation with Immigration and Customs Enforcement detainers; and
    d. Other jurisdictional responsibilities to support the enforcement of the United States immigration law.

Enduring needs include:

6. Effective planning
7. Training and awareness campaigns
8. Equipment and capital projects
9. Exercises

The table below provides a breakdown of the NPAs, and core capabilities impacted, as well as examples of eligible maritime security project types for each area. More information on allowable investments can be found in the Funding Restrictions and Allowable Costs section below. As discussed in Section E, projects that sufficiently address one or more of the NPAs will have their final review scores increased by a multiplier of 20%.

## FY 2025 PSGP Funding Priorities

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

| Priority Areas | Core Capabilities | Example Project Types |
|---|---|---|
| **National Priorities** | | |
| Enhancing the Protection of Soft Targets and Crowded Places | • Operational coordination<br>• Public information and warning<br>• Intelligence and Information Sharing<br>• Interdiction and disruption<br>• Screening, search, and detection<br>• Access control and identity verification<br>• Physical protective measures<br>• Risk management for protection programs and activities | • Physical security enhancements at cruise and ferry terminals<br>  ○ Explosive detection canine teams<br>  ○ Security cameras (closed circuit television [CCTV])<br>  ○ Security screening equipment for people and baggage<br>  ○ Access controls<br>  ▪ Landside fencing, gates, barriers, etc.<br>  ▪ Marine (floating) barriers to prevent access to sensitive berthing areas<br>• Enhanced security aboard ferries<br>  ○ Explosive detection canine teams<br>  ○ Security cameras (CCTV)<br>• Rapid response boats for preventing or responding to security incidents on waterways, especially in and around airports, cruise terminals, ferry terminals, etc. |
| Supporting Homeland Security Task Forces and Fusion Centers | • Intelligence and information sharing<br>• Interdiction and disruption<br>• Public information and warning<br>• Operational coordination<br>• Risk management for protection programs and activities | • Establishing or enhancing multi-agency Homeland Security Task Forces (HSTFs), including operational coordination centers<br>• Enhancing capabilities and integration with local fusion centers<br>• Procurement of technology or equipment to support surveillance, communications, and data analysis<br>• Development of standard operating procedures for information sharing, joint operations, and immigration enforcement coordination<br>• Personnel training, credentialing, and certification to improve interoperability and mission alignment<br>• Intelligence analysis, reporting, and suspicious activity monitoring<br>• Exercises and simulations focused on joint operations, intelligence sharing, or interdiction/disruption of criminal or smuggling networks<br>• Community engagement efforts to foster trust and encourage threat reporting<br>• Information sharing with all DHS components; fusion centers; other operational, investigative, and analytic entities; and other federal law enforcement and intelligence entities<br>• Cooperation with DHS and other entities in intelligence, threat recognition, assessment, analysis, and mitigation<br>• Identification, assessment, and reporting of threats of violence<br>• Intelligence analysis training, planning, and exercises |

| Priority Areas | Core Capabilities | Example Project Types |
|---|---|---|
| | | • 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<br>• Intelligence and information sharing<br>• Planning<br>• Public information and warning<br>• Operational coordination<br>• Screening, search, and detection<br>• Access control and identity verification<br>• Supply chain integrity and security<br>• Risk management for protection programs and activities<br>• Long-term vulnerability reduction<br>• Situational assessment<br>• Infrastructure systems<br>• Operational communications | • Cybersecurity risk assessments<br>• Projects that address vulnerabilities identified in cybersecurity risk assessments<br>○ Improving cybersecurity of critical port infrastructure, such as cranes, to meet minimum levels identified by Cybersecurity and Infrastructure Security Agency, and the National Institute of Standards and Technology Cybersecurity Framework (Version 1.1) or equivalent<br>○ Adoption of cybersecurity performance goals (CISA's Cross-Sector Cybersecurity Performance Goals)<br>• Cybersecurity training and planning |
| Enhancing Election Security | • Cybersecurity<br>• Intelligence and information sharing<br>• Planning<br>• Long-term vulnerability reduction<br>• Situational assessment<br>• Infrastructure systems<br>• Operational coordination<br>• Community resilience | • Prioritize compliance with the VVSG 2.0 established by the U.S. Election Assistance Commission<br>• Complete testing through a VSTL accredited by the U.S. Election Assistance Commission<br>• Physical security planning and exercise support<br>• Physical/site security measures – e.g., locks, shatter proof glass, alarms, access controls, etc.<br>• General election security navigator support<br>• Cyber and general election security navigator support<br>• Cybersecurity risk assessments, training, and planning<br>• Projects that address vulnerabilities identified in cybersecurity risk assessments<br>• Iterative backups, encrypted backups, network segmentation, software to monitor/scan, and endpoint protection<br>• Distributed Denial of Service protection<br>• Migrating online services to the ".gov" internet domain<br>• Online harassment and targeting prevention services<br>• Public awareness/preparedness campaigns discussing election security and integrity measures<br>• Long-term vulnerability reduction and community resilience |

| Priority Areas | Core Capabilities | Example Project Types |
|---|---|---|
| Supporting Border Crisis Response and Enforcement | • Training and awareness<br>• Community resilience<br>• Operational coordination<br>• Risk management for protection programs and activities | • Staffing support to expand 287(g) screening operations within correctional facilities<br>• Operational overtime costs directly tied to 287(g) screening, processing, and enforcement activities<br>• Training programs for state and local law enforcement officers in immigration law, civil rights protections, and 287(g) procedures<br>• Development or enhancement of information-sharing platforms between ICE and local agencies<br>• Procurement of screening, detection, and communications technology to support immigration enforcement activities<br>• Establishing secure and dedicated communication networks with ICE Field Offices<br>• Conducting joint training exercises with ICE and local law enforcement to test operational coordination<br>• Support for facilities upgrades, such as creating dedicated interview rooms and secure processing spaces<br>• Community engagement and public briefings to promote transparency and understanding of 287(g) operations and protections |
| **Enduring Needs** | | |
| Planning | • Planning<br>• Risk management for protection programs and activities<br>• Risk and disaster resilience assessment<br>• Threats and hazards identification<br>• Operational coordination<br>• Community resilience | • Development of:<br>○ Port-wide Security Risk Management Plans<br>○ Continuity of Operations Plans<br>○ Response Plans<br>○ Port-wide and/or asset-specific vulnerability assessments<br>○ Efforts to strengthen governance integration between/among regional partners |
| Training and Awareness | • Long-term vulnerability reduction<br>• Public information and warning<br>• Operational coordination<br>• Situational assessment<br>• Community resilience | • Active shooter training, including integrating the needs of persons with disabilities<br>• Shipboard firefighting training<br>• Public awareness/preparedness campaigns<br>• Maritime domain awareness projects |
| Equipment and Capital Projects | • Long-term vulnerability reduction<br>• Infrastructure systems<br>• Operational communications<br>• Interdiction and disruption<br>• Screening, search, and detection<br>• Access control and identity verification<br>• Physical protective measures<br>• Supply chain integrity and security<br>• Threats and hazards identification<br>• Infrastructure systems<br>• Intelligence and information sharing | • Implementing risk management projects that support port resilience and recovery<br>• Implementing physical security enhancement projects<br>• Transportation Worker Identification Credential projects<br>• Sharing and leveraging intelligence and information<br>• Chemical, Biological, Radiological, Nuclear, and Explosive prevention, detection response and recovery equipment<br>• Unmanned Aircraft Systems and detection technologies |
| Exercises | • Long-term vulnerability reduction | • Response exercises |

| Priority Areas | Core Capabilities | Example Project Types |
|---|---|---|
| | • Operational coordination<br>• Operational communications<br>• Community resilience | |

**C.** Program Rationale

The stated goals, objectives, and priorities of PSGP support Section 102 of the Maritime Transportation Security Act of 2002 (Pub. L. No. 107-295, as amended) (46 U.S.C. § 70107) to implement Area Maritime Transportation Security Plans and facility security plans among port authorities, facility operators, and State and local government agencies.

**D.** Federal Assistance Type

Grant

**E.** Performance Measures and Targets

Performance metrics for this program are as follows:

- Percentage of funding allocated by the recipient to core capabilities to build or sustain the national priorities identified in Section B above.

**F.** Program-Specific Unallowable Costs

Specific unallowable costs for the **PSGP** include:

- Projects in which federal agencies are the primary beneficiary or that enhance federal property, including sub-components of a federal agency;
- Projects that study technology development for security of national or international cargo supply chains (e.g., e-seals, smart containers, container tracking or container intrusion detection devices);
- Proof-of-concept projects;
- Development of training;
- Projects that duplicate capabilities being provided by the Federal Government (e.g., vessel traffic systems);
- Business operating expenses (certain security-related operational and maintenance costs are allowable—see "Maintenance and Sustainment" and "Operational Costs" for further guidance);
- Transportation Worker Identification Credential (TWIC) card fees;
- Reimbursement of pre-award security expenses;
- Outfitting facilities, vessels, or other structures with equipment or items providing convenience rather than a direct security benefit. Examples of such equipment or items include but are not limited to office furniture, CD players, DVD players, AM/FM radios, TVs, stereos, entertainment satellite systems, entertainment cable systems and other such entertainment media, unless sufficient justification is provided. This includes weapons and associated equipment (i.e., holsters, optical sights, and scopes), including but not limited to, non-lethal or less-than-lethal weaponry including firearms, ammunition, and weapons affixed to facilities, vessels, or other structures;
- Standard issue uniforms (other than maritime security personal protective equipment [PPE]);

- Expenditures for items such as general-use software, general-use computers, and related equipment (other than for allowable M&A activities, or otherwise associated preparedness or response functions), general-use vehicles and licensing fees;
- Land acquisitions and right of way purchases;
- Funding for standard operations vehicles utilized for routine duties, such as patrol cars and fire trucks;
- Fuel costs (except as permitted for training and exercises);
- Exercise(s) that do not support maritime security preparedness efforts;
- Patrol vehicles and firefighting apparatus, other than those chemical, biological, radiological, nuclear, and explosives (CBRNE) detection equipped vehicles for port area and/or facility patrol or response purposes;
- Specialty vehicles such as trucks for towing boat trailers/equipment and armored personnel carriers;
- Providing protection training to public police agencies or private security services to support protecting VIPs or dignitaries;
- Aircraft pilot training, including aircraft operations such as aircraft ditch training (does not include sUAS training when requested in conjunction with sUAS purchases);
- Post incident investigation training;
- Basic or advanced dive training (except marine unit CBRNE detection/response dive training);
- Training for personnel not primarily assigned to maritime security activities or MTSA required security personnel (e.g., vessel patrol officers, facility security officers); and
- Reimbursement for the maintenance and wear and tear costs of general use vehicles (e.g., construction vehicles) and emergency response apparatus (e.g., fire trucks, ambulances, repair, or cleaning of PPE, etc.).

**G.** 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, the Preparedness Grants Manual, and the terms and conditions of the federal award. This includes, among other requirements, that costs must be incurred, and products and services must be delivered within the budget period. 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).

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

**H.** Indirect Costs (Facilities and Administrative Costs)

Indirect costs are allowed for recipients of the PSGP.

Indirect costs (IDC) are costs incurred for a common or joint purpose benefitting 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. See the Preparedness Grants Manual for information on establishing indirect cost rates.

**I.** Management and Administration (M&A) Costs

M&A costs are allowed by the Full-Year Continuing Appropriations and Extensions Act, 2025, Pub. L. No. 119-4. Recipients may use *up to* 5% of the amount of the award's federal share for their M&A costs. M&A activities are those defined as directly relating to the management and administration of PSGP 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. PSGP funds may be used for the following M&A costs:

- Hiring full-time or part-time staff, including contractors and consultants, to execute the following:
  - Management of the awarded fiscal years' PSGP award;
  - Design and implementation of the awarded fiscal years' PSGP submission meeting compliance with reporting/data collection requirements, including data calls;
  - Information collection and processing necessary to respond to FEMA data calls;
  - Domestic travel expenses related to PSGP grant administration (International travel is not an allowable cost under this program unless approved in advance by DHS/FEMA.); and
  - Acquisition of authorized office equipment, including personal computers or laptops for PSGP M&A purposes.

M&A costs are not overhead costs but are necessary costs incurred in direct support of the federal award or as a consequence of it, such as travel, meeting-related expenses, and salaries of full/part-time staff in direct support of the program. As such, M&A costs can be itemized in financial reports. Other M&A cost 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, responding to official information requests from state and federal oversight authorities, and grant performance measurement or evaluation activities.

If an applicant uses an outside consultant or contractor to provide pre-award grant writing services or post-award grant management services, the considerations and requirements in the "Authorized Use of Contractual Grant Writers and/or Grant Managers" section below apply.

**J.** Pre-Award Costs
Pre-award costs are not allowed and will not be approved, with the exception of costs resulting from pre-award grant writing services provided by an independent contractor that shall not exceed $1,500 per applicant per year.

**K.** Beneficiary Eligibility
There are no program requirements for beneficiary eligibility. This NOFO and any subsequent federal awards create no rights or causes of action for any beneficiary.

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

**M.** Authorizing Authority
Section 102 of the Maritime Transportation Security Act of 2002 (Pub. L. No. 107-295, as amended) (46 U.S.C. § 70107)

**N.** Appropriation Authority
Full-Year Continuing Appropriations and Extensions Act, 2025, Pub. L. No. 119-4, § 1101.

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

**P.** Prohibition on Covered Equipment or Services
See the Preparedness Grants Manual for information on prohibitions on expending funds on covered telecommunications and surveillance equipment and services.

## 4. Application Contents and Format

**A.** Pre-Application, Letter of Intent, and Whitepapers
The PSGP does not require nor will staff review pre-applications, letters of intent, or whitepapers. Applicants are encouraged to pre-socialize projects with the USCG via Area Maritime Security Committee (AMSC) meetings.

**B.** Application Content and Format
The PSGP Investment Justification and Detailed Budget Worksheet are required to be completed in full and attached within FEMA GO at the time of application submission to be considered for funding. Applicants who fail to complete the "Eligibility" section of this form or fail to attach the form in FEMA GO will not be considered for funding.

**C.** Application Components
The following forms or information are required to be submitted via FEMA GO. Applicants can complete these forms directly in FEMA GO without needing to upload PDF versions of the forms. The Standard Forms (SF) are also available at Forms | Grants.gov

- SF-424, Application for Federal Assistance

- Grants.gov Lobbying Form, Certification Regarding Lobbying
- SF-424A, Budget Information (Non-Construction)
    - For construction under an award, submit SF-424C, Budget Information (Construction), in addition to or instead of SF-424A
- SF-424B, Standard Assurances (Non-Construction)
    - For construction under an award, submit SF-424D, Standard Assurances (Construction), in addition to or instead of SF-424B
- SF-LLL, Disclosure of Lobbying Activities

**D.** Program-Specific Required Documents and Information
The following program-specific forms or information are required to be submitted in FEMA GO:

- Associated Investment Justification (IJs) template with detailed budget(s); and
- Associated Memoranda of Understanding (MOU)/Memoranda of Agreement (MOA) is situationally required. See "***MOU/MOA Requirement for Security Services Providers***" below.

**a.** ***Priority Investments***
FY 2025 PSGP aligns with the Administration's priorities by directing resources toward the most urgent threats facing the Nation. PSGP supports the development and sustainment of core capabilities essential to achieving the National Preparedness Goal (NPG): "A secure and resilient Nation."

To ensure strategic focus, DHS has identified five NPAs that reflect the evolving risk landscape and national policy objectives. These priorities serve as a framework for targeting investments that build capability, reduce risk, and promote cross-sector coordination.

The FY 2025 NPAs are:

1. Enhancing the protection of soft targets and crowded places,
    a. 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. Supporting Border Crisis Response and Enforcement.
    a. Example activities under border crisis response and enforcement support may include:
    b. Participation in the Department of Homeland Security/Immigration and Customs Enforcement 287(g) training program;
    c. Cooperation with Immigration and Customs Enforcement detainers; and
    d. Other jurisdictional responsibilities to support the enforcement of United States immigration law.

These NPAs are rooted in the core mission areas of the NPG—prevention, protection, mitigation, response, and recovery—and reflect a whole-of-government approach to homeland security. Applicants should use these priorities to guide planning, investment, and implementation to drive measurable outcomes and long-term resilience.

**b.** ***Additional Information***

1. Soft Targets and Crowded Places

Soft targets and crowded places are increasingly appealing to terrorists and other violent extremist actors because of their relative accessibility and the large number of potential targets. This challenge is complicated by the prevalent use of simple tactics and less sophisticated attacks. Segments of our society are inherently open to the general public, and by nature of their purpose do not incorporate strict security measures. Given the increased emphasis by terrorists and other violent extremist actors to leverage less sophisticated methods to inflict harm in public areas, it is vital that the public and private sectors collaborate to enhance security of locations such as transportation centers, cruise terminals, ferry systems/terminals, and similar facilities. Additional resources and information regarding securing soft targets and crowded places are available through the Cybersecurity and Infrastructure Security Agency.

2. Supporting Homeland Security Task Forces and Fusion Centers

This priority supports the Administration's direction under Executive Order 14159, *Protecting the American People Against Invasion*, which calls for the establishment of Homeland Security Task Forces (HSTFs) nationwide. These multi-agency teams—composed of federal and local law enforcement partners—are tasked with disrupting and dismantling transnational criminal organizations, targeting cross-border human smuggling and trafficking networks (especially those involving children), and using all appropriate law enforcement tools to support lawful immigration enforcement.

Activities under this NPA also enhance broader national efforts in:

- Counterterrorism
- Cybersecurity
- Border security
- Immigration enforcement
- Transnational organized crime
- Protection of economic and critical infrastructure

3. Cybersecurity

Cybersecurity investments must support the security and functioning of critical port infrastructure and core capabilities as they relate to achieving target capabilities related to preventing, preparing for, protecting against, or responding to acts of terrorism at maritime infrastructure facilities. 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.

4. Election Security

In January 2017, DHS designated the infrastructure used to administer the Nation's elections as critical infrastructure. This designation recognizes that the United States' election infrastructure is of such vital importance to the American way of life that its incapacitation or destruction would have a devastating effect on the country. Additionally, the Homeland Threat Assessment 2024 indicates that electoral processes remain an attractive target for many adversaries.

Securing election infrastructure, ensuring its continued operation in the face of threats and harassment, advancing the safety of election officials, and protecting against foreign interference are national security priorities. Because threats to election systems are constantly evolving, defending these systems requires constant vigilance, innovation, and adaptation. By integrating the directives of Executive Order 14248, *Preserving and Protecting the Integrity of American Elections*, into the Election Security NPA, recipients can ensure that their efforts contribute to a secure, transparent, and resilient electoral process, thereby reinforcing public trust and the integrity of democratic institutions.

5. Supporting Border Crisis Response and Enforcement

State and local law enforcement agencies are essential partners in safeguarding national security and public safety. Pursuant to Executive Order 14159, Protecting the American People Against Invasion, it is the policy of the United States to enforce immigration laws against all inadmissible and removable aliens—particularly those who threaten the safety or security of the American people. This includes the efficient execution of these laws through lawful incentives and enhanced detention capabilities.

This NPA supports efforts that align with this policy and promote cooperation between local and federal partners. Projects may include, but are not limited to:

- Participation in the DHS/ICE 287(g) program, allowing trained local officers to support ICE with immigration enforcement;
- Cooperation with ICE detainers and other jurisdictional responsibilities related to immigration enforcement; and
- Supportive activities such as officer training, technology, and information sharing, operational support, and community engagement.

**a. *Investment Justification (IJ)***

As part of the PSGP application process, applicants must use the current Office of Management and Budget (OMB) approved IJ template on Grants.gov to address each initiative being proposed for funding, including a project's management and administration (M&A) costs. Applications submitted that do not use the OMB approved IJ template as provided will not be considered for funding. Applications with modified data fields, incomplete data fields, or are segmented into multiple attachments will not be considered for funding. A separate tab within the IJ template

should be used for each proposed project. The detailed budget worksheet noted below is included in the IJ template. ***Please refer to the "Applications Submitted by Eligible Entities" language in Section C above regarding the limitations on the number of applications per eligible entity or facilities, departments, subcomponents, or agencies within a single eligible entity. No single application or IJ may include projects intended to be implemented in different Port Areas, subject to the provisions of this section, below.*** Applicants may submit up to five IJs within a single application. Due to limited available funds, applicants are encouraged to include a statement within the IJ project description identifying a minimum funding level for a project to be feasible in the event that a project can only be partially funded based on available funds.

IJs must demonstrate how proposed projects address gaps and deficiencies in one or more of the core capabilities outlined in the National Preparedness Goal (the Goal). In the IJ, the applicant must demonstrate the ability to provide enhancements consistent with the purpose of the program and guidance provided by DHS/FEMA. PSGP projects must be both 1) feasible and effective at reducing the risks for which the project was designed; and 2) able to be fully completed within the 36-month period of performance. For information on the feasibility and effectiveness determination, please see the Review and Selection Process as outlined in this NOFO.

***For the purposes of a PSGP application, a Port Area is selected for funding based on the project location. Eligible entities that have facilities in multiple Port Areas should apply for projects based on the Port Area where the project/asset will be implemented, housed, or maintained, not the entity's headquarters location.*** For entities submitting applications for a single project that spans multiple Port Areas, such as one patrol vessel that may be deployed outside of the primary Port Area, the project location is considered to be the Port Area that will see the most benefit from the project. Large projects that implement multiple components in multiple Port Areas, such as state agency purchases of multiple patrol vessels for multiple Port Areas, must be submitted as separate applications (e.g., State Police vessel project in Port Area #1 is one application; State Police vessel project in Port Area #2 is a separate application). All eligible and complete applications will be provided to the applicable COTP for further review.

Applicants seeking to participate in large-scale regional projects requiring the purchase of services or equipment should directly reference this need in their applications. Applicants should specify their portion of the requested project funding and role in the project. Applicants should also note if their portion of a project can be completed independently of the large-scale regional project. ***Applicants are prohibited from applying for equipment or other non-consumables intended to be solely used by another agency.***

Applicants will find the IJ template on Grants.gov in the "Related Documents" tab of the PSGP posting. This IJ template must be used for each project submitted. Applicants must provide information in the following categories for each proposed investment:

1. Background;
2. Strategic and Program Priorities;
3. Impact; and
4. Funding/Implementation Plan.

Applicants must use the following file naming convention when submitting an IJ as part of the PSGP:

***Name of Applicant_IJ Numbers (Example: XYZ Oil_IJ 1-3)***

**b.** ***Detailed Budget***

Detailed budget worksheets are incorporated within the PSGP IJ template. Applicants must use the IJ template provided. All applicants must complete the detailed budget worksheets for each corresponding project requested at the time of application. The detailed budget must be complete, reasonable, and cost-effective in relation to the proposed project and should provide the basis of computation of all project-related costs (including M&A costs) and any appropriate narrative. Review panels must be able to thoroughly evaluate the projects being submitted based on the information provided. Consequently, applicants must provide an appropriate level of detail within the budget detail worksheets to clarify what will be purchased and spent. ***Applications that do not include a detailed budget narrative will not be considered for funding.*** Detailed budgets often assist reviewers in determining what type of equipment or service is being purchased, which may assist in determining the effectiveness of a project. Additionally, a detailed budget must demonstrate the required cost share, either cash (hard) or third-party in-kind (soft), of the recipient based on the projected project cost. ***Applications failing to demonstrate the required cost share within the detailed budget will not be considered for funding.***

Cash and third-party in-kind matches must consist of eligible costs (i.e., same allowability as the federal share), reasonable and necessary to complete the project, and must be identified as part of the submitted budget detail worksheet. A cash (hard) match includes cash spent for project-related costs while a third-party in-kind (soft) match includes the valuation of in-kind services. The cost match requirement for a PSGP award may not be met by funds from another federal grant or assistance program or funds used to meet matching requirements for another federal grant program. Likewise, third-party in-kind matches used to meet the matching requirement for the PSGP award may not be used to meet matching requirements for any other federal grant program. Please see Section C of this NOFO, and reference 2 C.F.R. § 200.306 as applicable, for further guidance regarding cost matching.

**c.** ***MOU/MOA Requirement for Security Services Providers***

State and local agencies that are identified in the AMSP of their respective COTP/Federal Maritime Security Coordinator as providing security services to one or more MTSA regulated facilities within a Port Area may apply for PSGP funding and are not required to provide FEMA with an MOU/MOA. However, ***state, local, and territorial agencies that are not specifically identified in their respective AMSP but are otherwise required to provide port security services must have a signed MOU/MOA between the security service agency and the MTSA regulated facilities receiving these services within the applicant Port Area prior to receipt of PSGP funding*** and must include an acknowledgement of the security services, roles, and responsibilities of all entities involved. This includes agencies or entities that are new to the port area or are newly participating in Area Maritime Security Committee activities but are not yet included in the AMSP. These entities must have an MOU/MOA with the respective MTSA regulated facility pending AMSP updates. This information must be maintained by the grant recipient and provided to DHS/FEMA upon request; or verification through the field review

process that the agency is identified within the MOU/MOA as an entity that provides maritime security services or is otherwise required to provide port security services. The MOU/MOA must address the following points:

1. The nature of the security service that the applicant agrees to supply to the MTSA regulated facility (e.g., waterside surveillance, increased screening);
2. The roles and responsibilities of the MTSA regulated facility and the applicant during different Maritime Security levels;
3. An acknowledgement by the MTSA regulated facility that the applicant is part of the facility's security plan; and,
4. An acknowledgment that the applicant will provide semi-annual progress reports on project status to the local applicable Area Maritime Security Committee and/or COTP.

The signed MOU/MOA for state or local agencies providing security services to regulated entities should be submitted with the grant application as a file attachment within FEMA GO. A sample MOU/MOA can be found below. Applicants must use the following file naming convention for MOUs and MOAs:

***Name of Applicant_MOU (Example: Harris County_MOU)***

See the appendix in Section H.5 of this NOFO for a sample MOU/MOA. The sample MOU/MOA demonstrates all of the elements required in the PSGP NOFO for acceptance for review as part of a grant application from a state or local agency providing security services to MTSA-regulated entities.

**d.** ***Sensitive Security Information (SSI) Requirements***

A portion of the information that is routinely submitted in the course of applying for funding or reporting under certain programs or that is provided in the course of an entity's grant management activities under those programs that are under federal control is subjected to protection under SSI requirements and must be properly identified and marked. SSI is a control designation used by DHS/FEMA to protect transportation security related information. It is applied to information about security programs, vulnerability and threat assessments, screening processes, technical specifications of certain screening equipment and objects used to test screening equipment, and equipment used for communicating security information relating to air, land, or maritime transportation. Further information can be found in 49 C.F.R. §§ 1520.1-15.20.19.

For the purposes of the PSGP, and due to the high frequency of SSI found in IJs, all IJs shall be considered SSI and treated as such until they have been subject to review for SSI by DHS/FEMA. This means that applicants shall label these documents as SSI in accordance with 49 C.F.R. § 1520.13.

**E.** Post-Application Requirements for Successful Applicants

Not applicable.

## 5. Submission Requirements and Deadlines

**A.** Address to Request Application Package

Applications are processed through the FEMA GO system. To access the system, go to https://go.fema.gov/.

Steps Required to Apply for an Award Under this Program and Submit an Application:

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

a. Apply for, update, or verify their Unique Entity Identifier (UEI) number and EIN from the Internal Revenue Service;
b. In the application, provide an UEI number;
c. Have an account with login.gov;
d. Register for, update, or verify their SAM account and ensure the account is active before submitting the application;
e. 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 https://www.fema.gov/media-library/assets/documents/181607;
f. Submit the complete application in FEMA GO; and
g. Continue to maintain an active SAM registration with current information at all times during which it has an active federal award or 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.

How to Register to Apply:

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 Unique Entity Identifier (UEI) number, Employer Identification Number (EIN), and an active System for Award Management (SAM) registration.

Obtain a UEI Number:

All entities applying for funding, including renewal funding, must have a UEI number. Applicants must enter the UEI number in the applicable data entry field on the SF-424 form. For more detailed instructions for obtaining a UEI number, refer to SAM.gov.

Obtain Employer Identification Number:

In addition to having a UEI number, all entities applying for funding must provide an Employer Identification Number (EIN). The EIN can be obtained from the IRS by visiting https://www.irs.gov/businesses/small-businesses-self-employed/apply-for-an-employer-identification-number-ein-online.

Create a login.gov account:

Applicants must have a login.gov account in order to register with SAM or update their SAM registration. Applicants can create a login.gov account at: https://secure.login.gov/sign_up/enter_email?request_id=34f19fa8-14a2-438c-8323-a62b99571fd.

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 https://www.sam.gov/SAM/pages/public/loginFAQ.jsf.

Register with SAM:

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

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

**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 within the past three years, if applicable.

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 registration may need to be involved in this step. For step-by-step instructions, see 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.

Submitting the Final Application:

Applicants will be prompted to submit the standard application information and any program-specific information required. Standard Forms (SF) may be accessed in the Forms tab under the SF-424 family on Grants.gov. Applicants should review these forms before applying to ensure they are providing all required information.

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

**B.** Application Deadline
08/15/25 05:00:00 PM Eastern Time

**C.** Pre-Application Requirements Deadline
Not applicable.

**D.** Post-Application Requirements Deadline
Not applicable.

**E.** Effects of Missing the Deadline
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 via email the 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 3:00 PM 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.

## 6. 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.

## 7. Application Review Information

**A.** Threshold Criteria
Applicants who have existing or recently closed PSGP awards that, as of the date of publication of this NOFO, are non-compliant with 2 C.F.R. § 200.329 (Monitoring and reporting program performance) requirements; or have 2 or more instances of delinquent reporting within the past 12 months, will not be considered for funding.

**B.** Application Criteria

**a.** ***Overview***

The PSGP uses a risk-based methodology for making funding decisions whereby each Port Area's relative threat, vulnerability, and consequences from acts of terrorism are considered. This approach helps ensure that program funding is directed toward those Port Areas that present the highest risks in support of the Goal a secure and resilient Nation. Please refer to the Preparedness Grants Manual for further information on the Goal. PSGP will only fund those eligible projects that close or mitigate maritime security risk vulnerabilities gaps as identified in the applicable AMSP, FSP, VSP, and/or Port-wide Risk Management Plan (PRMP). Projects that enhance business continuity and resumption of trade within a Port Area will also be considered for funding.

***Projects submitted by a public sector applicant or projects otherwise certified by the USCG COTP as having a port-wide benefit (please see the cost match section of this NOFO for further information regarding what constitutes a port-wide benefit) will have their final scores increased by a multiplier of 10%.***

FY 2025 PSGP applications will be evaluated through a three-part review and selection process that encompasses: 1) an Initial Screening; 2) a Field Review; and 3) a National Review. The PSGP scoring criteria applied in each step of this process are centric to projects addressing program authorizing legislation.

The COTP field review will be provide FEMA a numerical listing of projects ranked in descending order. For example, a COTP with 10 projects to review will rank those projects from 1 – 10, with 1 being their highest ranked/most desired project to be funded.

Project addresses national economic, energy, and strategic defense concerns based upon the most current risk assessments available, in combination with the authorities, responsibilities, and discretion vested by law to the COTP, and considering national PSGP and local COTP priorities, for their effectiveness in addressing or correcting Coast Guard identified security vulnerabilities in the marine transportation system.

0 = None; 1 = Minimal; 3 = Moderate; 9 = Significant

**b.** ***National Review***

DHS/FEMA will lead a National Review. The National Review encompasses 1) a review by a panel of subject-matter experts (SME) from DHS/FEMA and other federal partners that validates the USCG COTP-led Field Review results; and 2) a detailed administrative/financial review of applications recommended for funding. ***As part of the National Review, the SME panel will increase the score of any proposed project that sufficiently addresses one or more of the NPAs by 20%.*** Projects that are not dedicated to specifically enhancing a National Priority will not receive a score increase (e.g., a port area patrol vessel that is not solely dedicated to patrolling the soft target/crowded place or a camera replacement project that includes a cybersecurity software installation will not receive a 20% score increase). To be considered for a 20% score increase, projects must be submitted as distinct and standalone, and dedicated to supporting an NPA.

As part of the National Review, the SME panel may also recommend partial funding for individual projects and eliminate others that are determined to be duplicative or require a sustained federal commitment to fully realize the intended risk mitigation. In addition, the SME panel will validate proposed project costs. ***Decisions to reduce requested funding amounts or eliminate requested items deemed inappropriate under the scope of the PSGP will take into consideration the ability of the revised project to address the NPAs and whether it will achieve the intended risk mitigation goal.*** Historically, the PSGP has placed a high priority on providing full project funding rather than partial funding.

Elements of the application considered during the National Review include the following as specified within this NOFO:

- Eligibility of an applicant;
- Allowable costs;
- Required cost share; and
- Alignment with program priorities.

**c. *Risk Score***

Independent of the Field and National Reviews, a risk score will also be calculated for each Port Area in which an eligible entity applies for PSGP funding. A Port Area risk score will be calculated based on the relative threat, vulnerability, and consequences from acts of terrorism. The risk methodology used to calculate this score is focused on three elements:

- *Threat* – likelihood of an attack being attempted by an adversary;
- *Vulnerability* – likelihood that an attack is successful, given that it is attempted; and
- *Consequence* – effect of an event, incident, or occurrence.

The risk methodology determines the relative risk of terrorism faced by a given Port Area, considering the potential risk of terrorism to people, critical infrastructure, economic security, and national security missions. A risk and effectiveness prioritization will then be applied to the SME panel's recommended list of projects for each Port Area. This analysis considers the following factors to produce a comprehensive national priority ranking of port security proposals:

- Relationship of the project to one or more of the National Priorities;
- Relationship of the project to the local port security priorities;
- Risk level of the Port Area in which the project would be located;
    - Those Port Areas that have a measurable risk of at least 1% of the overall maritime security risk based on the comprehensive DHS/FEMA risk methodology would be prioritized above those with less than 1% of the overall risk;
    - To ensure that the most effective projects are funded, the risk and effectiveness prioritization could be limited by Port Area, based on the Port Area's relative risk score; and
- Effectiveness and feasibility of the project to be completed in support of the priorities highlighted above during the period of performance.

Projects recommended for funding will also receive a detailed administrative/financial review to ensure compliance with all program requirements. As a part of this, applications will be reviewed to ensure there are no ineligible costs, there is an appropriate nexus to maritime security, etc.

***FEMA may place a risk-based funding cap on Port Areas to ensure a broad distribution of program funds among multiple Port Areas. This will ensure that minimally effective projects in the highest risk Port Areas are not funded ahead of highly effective projects in lower risk Port Areas; however, this does not guarantee that Port Areas with minimal risk scores will receive funding.*** All funding recommendations will be provided to the inter-agency partners for concurrence. All final funding determinations will then 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.

**C**. Financial Integrity Criteria
Before making an award, FEMA 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 Review
Before making an award expected to exceed the simplified acquisition threshold (currently a total federal share of $250,000) over the period of performance:

1. FEMA 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, FEMA will consider any comments by the applicant.

**E**. Reviewers and Reviewer Selection
National Review Panelists are comprised of FEMA's joint Federal agency working group member SMEs from USCG, Transportation Security Administration (TSA), Maritime Administration (MARAD), and FEMA.

Administrative reviewers are comprised of full-time FEMA staff assigned to the PSGP. All reviewers are provided review guidelines that are aligned to this NOFO and include references to ensure consistency and standardization of reviews.

**F.** Merit Review Process
Each COTP is responsible for establishing field reviews of applications submitted in support of his/her port area(s). In general, reviews are coordinated with local MARAD Gateway Directors. See section "7. Application Review Information" for evaluation criteria, weighted scoring and merit-based approach for application reviews.

**G.** Final Selection
FEMA summarizes a prioritized ranking of all projects recommended for funding based on Risk x Effectiveness (merit review). Recommended funding is then transmitted to the Secretary of Homeland Security for a final determination.

## 8. 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 submitting an application, applicants agree to comply with the prerequisites stated in this NOFO, the Preparedness Grants Manual, and the material terms and conditions of the federal award, should they receive an award.

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 via the FEMA GO system.

Funds will remain on hold until the recipient accepts the award via 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
Not Applicable. The PSGP does not permit pass-through funding.

**C**. Note Regarding Pre-Award Costs
Even if pre-award costs are allowed, beginning performance prior to award acceptance is at the applicant and/or sub-applicant's own risk.

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

**E.** Notification to Unsuccessful Applicants
Unsuccessful Applicants will be notified through the FEMA GO system after all successful awards have been made, but not sooner than October 1st of the FY 2025 award cycle. Applicants may contact the program office for additional feedback.

## 9. Post-Award Requirements and Administration

**A.** Administrative and National Policy Requirements

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.

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.

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.

**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 date of the federal award. The DHS Standard Terms and Conditions are available online: 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.

**C.** Financial Reporting Requirements
See the Preparedness Grants Manual for information on financial reporting requirements.

**D.** Programmatic Performance Reporting Requirements
See the Preparedness Grants Manual for information on performance reporting requirements.

**E.** Closeout Reporting Requirements
See the Preparedness Grants Manual for information on closeout reporting requirements and administrative closeout.

Additional Reporting Requirements

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

**F.** Disclosing Information per 2 C.F.R. § 180.335
See the Preparedness Grants Manual for information on disclosing information per 2 C.F.R. § 180.335.

**G.** Reporting of Matters Related to Recipient Integrity and Performance
See the Preparedness Grants Manual for information on reporting of matters related to recipient integrity and performance.

**H.** Single Audit Report
See the Preparedness Grants Manual for information on single audit reports.

**I.** 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 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 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 must respond in a timely and accurate manner to DHS requests for information relating to a federal award. See the Preparedness Grants Manual for more information on monitoring and oversight.

**J.** Program Evaluation
Title I of the Foundations for Evidence-Based Policymaking Act of 2018, Pub. L. No. 115-435 (2019) (Evidence Act), PUBL435.PS 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 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 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 allowable and may not be charged to the federal award.

**K.** Additional Performance Reporting Requirements.
Not applicable.

**L.** Termination of the Federal Award

1. Paragraph C.XL of the FY 2025 DHS Standard Terms and Conditions, v.3 sets forth a term and condition entitled "Termination of a Federal Award." The termination provision condition listed below applies to the grant award and the term and condition in Paragraph C.XL of the FY 2025 DHS Standard Terms and Conditions, v.3 does not.

2. Termination of the Federal Award by FEMA

FEMA may terminate the federal award in whole or in part for one of the following reasons identified in 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. If DHS/FEMA, in its sole discretion, determines that a specific award objective is ineffective at achieving program goals as described in this NOFO;
ii. If DHS/FEMA, in its sole discretion, determines that an objective of the award as described in this NOFO will be ineffective at achieving program goals or agency priorities;
iii. If DHS/FEMA, in its sole discretion, determines that the design of the grant program is flawed relative to program goals or agency priorities;
iv. If DHS/FEMA, in its sole discretion, determines that the grant program is not aligned to either the DHS Strategic Plan, the FEMA Strategic Plan, or successor policies or documents;
v. If DHS/FEMA, in its sole discretion, 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.
vii. If the awardee falls out of compliance with the Agency's statutory or regulatory authority, award terms and conditions, or other applicable laws.

3. Termination of a Subaward by the Pass-Through Entity

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:

a. If the subrecipient fails to comply with the terms and conditions of the federal award.
b. 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.
c. If the pass-through entity's award has been terminated the pass-through recipient will terminate its subawards.

4. Termination by the Recipient or Subrecipient

The recipient or subrecipient may terminate the federal award in whole or in part for the following reason 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 the pass-through entity may terminate the federal award in its entirety.

5. Impacts of Termination

a. When FEMA terminates the federal award prior to the end of the period of performance due to the recipient'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 the pass-through entity and the 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.

**M.** Best Practices
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." 2 C.F.R. § 200.303(e).

**N.** Payment Information
Recipients will submit payment requests in FEMA GO for FY25 awards under this program.

**Instructions to Grant Recipients Pursuing Payments**

FEMA reviews all grant payments and obligations to ensure allowability in accordance with 2 C.F.R. § 200.305. These measures 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 recipients SAM.gov financial information. If FEMA disapproves a payment, FEMA will inform the recipient.

**Processing and Payment Timeline**

FEMA must comply with regulations governing payments to grant recipients. See 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) agreements ("Treasury-State agreement") and default procedures codified at 31 C.F.R. part 205 and Treasury Financial Manual (TFM) 4A-2000, "Overall Disbursing Rules for All Federal Agencies." *See* 2 C.F.R. § 200.305(a).

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. 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." 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.

**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 submittal of 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 DEI practices.
5. Supporting documentation to demonstrate that expenses are allowable, allocable, reasonable, and necessary under 2 CFR part 200 and in compliance with the grant's NOFO, award terms, and applicable federal regulations.

O. Immigration Conditions

1. Materiality of Pending Immigration Condition

An immigration term and condition, including those in the DHS Standard Terms and Conditions, may be material to the Department of Homeland Security's decision to make this grant award, and the Department of Homeland Security may take any remedy for noncompliance, including termination, if the state or territorial recipient or any local government subrecipient fails to

comply with this term and condition. No final agency decision has been made as of the date of this publication.

## 10. Other Information

**A.** Period of Performance Extension

Extensions to the period of performance are allowed. See the Preparedness Grants Manual for information on period of performance extensions.

**B.** Other Information

**a. *Environmental Planning and Historic Preservation (EHP) Compliance***

See the Preparedness Grants Manual for information on EHP compliance.

**b. *Procurement Integrity***

See the Preparedness Grants Manual for information on procurement integrity.

**c. *Financial Assistance Programs for Infrastructure***

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

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

The Buy America preference only applies to articles, materials, and supplies that are consumed in, incorporated into, or affixed to an infrastructure project. As such, it does not apply to tools, equipment, and supplies, such as temporary scaffolding, brought to the construction site and removed at or before the completion of the infrastructure project. Nor does a Buy America preference apply to equipment and furnishings, such as movable chairs, desks, and portable computer equipment, that are used at or within the finished infrastructure project but are not an integral part of the structure or permanently affixed to the infrastructure project.

To see whether a particular FEMA federal financial assistance program is considered an infrastructure program and thus required to implement FEMA's Build America, Buy America requirements, please see Programs and Definitions: Build America, Buy America Act | FEMA.gov.

2. Waivers

When necessary, recipients 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, 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.

3. 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.

**d. *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.

**e. *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.

**f. *Record Retention***
See the Preparedness Grants Manual for information on record retention

**g. *Actions to Address Noncompliance***
See the Preparedness Grants Manual for information on actions to address noncompliance.

**h. *Audits***
See the Preparedness Grants Manual for information on audits.

## 11. Appendix A: Allowable Costs

**A.** Planning

PSGP funds may be used for the following types of planning activities:

1. Development or updating of port wide risk mitigation plan (PRMP), including the conduct of port security vulnerability assessments as necessary to support plan update/development;
2. Development and enhancement of security plans and protocols within the AMSP, PRMP, and the Business Continuity and Resumption of Trade Plans (BCRTP) in support of maritime security and risk mitigation planning;
3. Materials required to conduct planning activities noted in this section;
4. Travel and per diem related to the professional planning activities noted in this section;
5. Coordination and information sharing with fusion centers;
6. Planning activities related to alert and warning capabilities;
7. Conducting risk and resilience assessments on increasingly connected cyber and physical systems, on which security depends, using the Infrastructure Resilience Planning Framework and related CISA resources;
8. Other port wide maritime security project planning activities, which emphasize the ability to adapt to changing conditions and be prepared to withstand, and recover from, disruptions due to emergencies with prior approval from FEMA; and
9. Backfill, overtime, hiring of part-time temporary personnel, and contractors or consultants to assist with planning activities. Copies of PSGP-funded plans must be made available to FEMA and the U. S. Coast Guard (USCG) upon request.

**B.** Operational Activities

**a.** ***Explosive Detection Canine Teams (EDCTs)***

Use of canines (K-9) for explosive detection is one of the most effective solutions for the detection of vehicle-borne IEDs. When combined with the existing capability of a port or ferry security/police force, the added value provided through the addition of a canine team is significant. EDCTs are a proven, reliable resource to detect explosives and are a key component in a balanced counter-sabotage program.

Eligibility for funding of EDCTs is restricted to:

1. U.S. Ferry Systems regulated under 33 C.F.R. Parts 101, 103, 104, and the passenger terminals these specific ferries service under 33 C.F.R. Part 105;
2. Maritime Transportation Security Act (MTSA) regulated facilities; and
3. Port authorities, port police, and local law enforcement agencies that provide direct layered security for these U. S. Ferry Systems and MTSA-regulated facilities, and are defined in an AMSP, Facility Security Plan (FSP), or Vessel Security Plan (VSP).

Applicants may apply for up to $450,000 ($150,000/year for three years) per award to support this endeavor. At the end of the grant period (36 months), recipients will still be responsible for continuing the heightened level of capability provided by the EDCT. ***A sustainment plan must be submitted with the applicant's IJ to address the 12-month period beyond the period of performance of the award.***

**b. *Eligible EDCT Costs***

Funds for these EDCTs may **not** be used to fund drug detection and apprehension technique training. Only explosives detection training for EDCTs will be funded. The PSGP EDCT funds may only be used for ***new or expanded*** capabilities/programs and cannot be used to pay for existing K-9 teams, personnel, or K-9 training costs already supported by the port area. Repair and replacement of existing EDCT equipment is allowed. Eligible costs include:

1. Contracted K-9 and handler providing services in accordance with PSGP guidance;
2. Salary and fringe benefits of new full- or part-time K-9 handler positions;
3. Training and certifications (travel costs associated with training for new or expanded full or part time agency handlers, and canines are allowable);
4. K-9 and handler equipment costs;
5. Purchase and train a new K-9 and handler for CBRNE detection; and
6. K-9 maintenance costs including but not limited to veterinary, housing, and feeding costs.

Ineligible EDCT costs include, but are not limited to:

1. Hiring costs, including costs associated with initial police academy training of new officers;
2. Meals and incidentals associated with travel for initial certification;
3. Vehicles modified to be used solely to transport canines; and
4. Repair or replacement of unallowable equipment.

For additional information on EDCTs, see the Preparedness Grants Manual.

**C.** Equipment and Capital Projects

Equipment costs are allowed under this program. Please see the Preparedness Grants Manual for more information. Additionally, recipients that are using PSGP 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. For more information about SAFECOM, see the Preparedness Grants Manual.

**a. *Equipment Acquisition***

PSGP funds may be used for the following categories of equipment. A comprehensive listing of allowable equipment categories and types is found in the Authorized Equipment List (AEL). Requests for vehicles of any type are subject to secondary review and approval by the National Review Panel. These costs include:

1. Personal Protective Equipment (PPE) for maritime security providers, such as ballistic protective body armor (not including uniforms);
2. CBRNE response and remediation equipment for maritime security providers;
3. CBRNE decontamination equipment for direct maritime security providers and MTSA-regulated industry;
4. CBRNE detection-equipped patrol vehicles ***(not including armored personnel carriers or tow trucks),*** provided they will be used ***exclusively for port/facility CBRNE detection***

security operations. A CBRNE detection equipped patrol vehicle must include specifically identified, permanently mounted detection equipment;
5. Trailers (not vehicles) designed to carry maritime security equipment essential to maritime security, mitigation, and response (such as boat trailers, dive trailers, or mobile command trailers);
6. Mobile Command Centers ***only when validated by the COTP as essential to address a specifically required capability outlined in the approved AMSP***. This does not include prime movers (tow-trucks), personnel carriers, or equipment transport vehicles;
7. CBRNE detection-equipped and patrol watercraft vessel/small boat used to directly support maritime security for a facility or within a Port Area on a routine basis (CBRNE detection equipment requested with the watercraft/small boat in the IJ must be listed and also detailed in the budget). However, a vessel is not required to be CBRNE equipped;
8. Marine firefighting vessels, provided they are outfitted with CBRNE detection equipment and are designed and equipped to meet NFPA 1925: Standard on Marine Fire-Fighting Vessels;
9. Firefighting foam and Purple-K Powder (PKP) may be purchased by public fire departments that have jurisdictions in a port area and would respond to an incident at an MTSA regulated facility; MTSA facilities may also receive funding for this purpose. Funding will be limited to a one-time purchase based on a worst-case incident at the facility or facilities;
10. Information-sharing technology; components or equipment designed to share maritime security risk information and maritime all-hazards risk information with other agencies (equipment must be compatible with generally used equipment);
11. Maritime security risk mitigation interoperable communications equipment, including alert and warning capabilities;
12. Terrorism incident prevention and response equipment for maritime security risk mitigation;
13. Physical security enhancements, to include TWIC projects (e.g., card readers, fences, blast resistant glass, turnstiles, hardened doors, and vehicle gates) at maritime facilities;
14. Portable fencing, closed-circuit televisions (CCTVs), passenger vans, minibuses, etc. to support secure passage of vessel crewmembers through a MTSA regulated facility;
15. Equipment that enhances continuity capabilities, such as interoperable communications, intrusion prevention/detection, physical security enhancements, software and other equipment needed to support essential functions during a disruption to normal operations;
16. Generators with appropriate capability (size) to provide back-up power to security systems and equipment that support Maritime Domain Awareness (not including routine operational capabilities):
    - Access control equipment and systems;
    - Detection and security surveillance equipment; and
    - Enhancement of Command-and-Control facilities.
17. Equipment for new personnel, such as personal protective equipment, is an allowable expense. Weapons and equipment associated with weapons maintenance/security (e.g., firearms, ammunition, and gun lockers) are not allowable.

Recipients may purchase maritime security equipment not listed on the AEL, but **only** if they first seek and obtain **prior approval** from FEMA.

**b. *Requirements for Small Unmanned Aircraft Systems***

For information on sUAS allowability, please see the Preparedness Grants Manual.

**c. *Improvised Explosive Device (IED) and CBRNE Prevention, Protection, Response, Recovery Capabilities***

Port areas should continue to enhance their capabilities to prevent, detect, respond to, and recover from terrorist attacks employing IEDs, CBRNE devices, and other non-conventional weapons. Please refer to DHS Small Vessel Security Strategy (Apr. 2008).

**d. *Sonar Devices***

The four types of allowable sonar devices are: imaging sonar, scanning sonar, side scan sonar, and three-dimensional sonar. These types of sonar devices are intended to support the detection of underwater improvised explosive devices and enhance maritime domain awareness. The eligible types of sonar, and short descriptions of their capabilities, are provided below:

1. **Imaging Sonar:** A high-frequency sonar that produces "video-like" imagery using a narrow field of view. The sonar system can be pole-mounted over the side of a craft or hand-carried by a diver.
2. **Scanning Sonar:** Consists of smaller sonar systems that can be mounted on tripods and lowered to the bottom of the waterway. Scanning sonar produces a panoramic view of the surrounding area and can cover up to 360 degrees.
3. **Side Scan Sonar:** Placed inside a shell and towed behind a vessel. Side scan sonar produces strip-like images from both sides of the device.
4. **Three-Dimensional Sonar:** Produces 3-dimensional imagery of objects using an array receiver.

**e. *Physical Security***

Physical security is security measures that are designed to deny unauthorized access to facilities, equipment, and resources and to protect personnel and property from damage or harm (such as espionage, theft, or terrorist attacks). Physical security involves the use of multiple layers of interdependent systems and techniques. Physical security has been a focus of PSGP since the program's inception in 2002. Primarily, physical security is intended to harden MTSA-regulated facilities against attacks. Law enforcement may contribute to physical security through patrols; however, patrol vessels generally enhance multiple core capabilities with a focus on CBRNE detection, deterrence, and response. Funding through PSGP for physical security projects should be only directed toward those projects that address identified MTSA required activities and identified in the entity FSP and/or the port area AMSP. Some examples of funded projects include TWIC-related equipment, fencing, lighting, gates, and CCTV. Physical security projects typically require EHP review prior to obligating PSGP funds.

**f. *Capital (Construction) Projects Guidance***

See the Preparedness Grants Manual for more information about PSGP Capital (Construction) Projects Guidance.

**g. *Controlled Equipment***

For decades, the federal government has provided equipment to state, local, territorial, and tribal law enforcement agencies (LEAs) through federal grants. Some federal grant programs have

assisted LEAs as they carry out their critical missions to keep the American people safe. The equipment acquired by LEAs through these programs includes administrative equipment, such as office furniture and computers. Some federal grant programs also may include military and military-styled equipment, firearms, and tactical vehicles provided by the federal government, including property covered under 22 C.F.R. Part 121 and 15 C.F.R. Part 774 (collectively, "controlled equipment").

However, not all equipment that is considered controlled equipment is allowable under the PSGP. As discussed further below, there are certain "prohibited equipment" that are not allowable under the PSGP. And for the procurement of certain controlled equipment that is allowable under the PSGP, there are additional submission requirements and reviews that must be met before DHS/FEMA will permit funding to be used for this purpose, including but not limited to the provision of policies and procedures in place to safeguard individuals' privacy, civil rights, and civil liberties.

DHS/FEMA will continue to collaborate with federal agency partners to ensure that there is a consistent and reasonable approach to the restrictions placed on controlled equipment expenditures while continuing to support these investments when there is a justifiable need. Further, DHS/FEMA will continue to maintain an awareness of the evolving policy developments related to controlled equipment expenditures and keep grant recipients up to date on future developments.

Grant funds under this program may not be used for the purchase of equipment not approved by DHS/FEMA. The purchase of weapons and weapons accessories, including ammunition, is not allowed with PSGP funds. Grant funds under this program may not be used for the purchase of the following equipment: 1) firearms; 2) ammunition; 3) grenade launchers; 4) bayonets; or 5) weaponized aircraft, vessels, or vehicles of any kind with weapons installed.

Additional information on controlled equipment is pending publication. Please visit FEMA's website for current and upcoming guidance.

**h. *Cybersecurity Projects***

PSGP funds may be used for projects that enhance the cybersecurity of:

1. Access controls;
2. Sensors;
3. Security cameras;
4. Badge/ID readers;
5. Industrial Control System (ICS)/Supervisory Control and Data Acquisition (SCADA) systems for cranes and other port infrastructure;
6. Process monitors and controls (such as firewalls, network segmentation, predictive security cloud, etc.); and
7. Passenger/vehicle/cargo security screening equipment (cybersecurity assessments are allowable).

When requesting funds for cybersecurity, applicants are encouraged to propose projects that would aid in implementation of all or part of the Framework for Improving Critical Infrastructure

Cybersecurity, Version 1.1 (the "Framework") developed by the National Institute of Standards and Technology (NIST), or other similar sources. The Framework gathers existing international standards and practices to help organizations understand, communicate, and manage their cyber risks. For organizations that do not know where to start with developing a cybersecurity program, the Framework provides initial guidance. For organizations with more advanced practices, the Framework offers a way to improve their programs, such as better communication with their leadership and suppliers about management of cyber risks.

DHS's Enhanced Cybersecurity Services (ECS) program is an example of a resource that assists in protecting U.S.-based public and private entities and combines key elements of capabilities under the "Detect" and "Protect" functions to deliver an impactful solution relative to the outcomes of the Cybersecurity Framework.

Specifically, ECS offers intrusion prevention and analysis services that help U.S.-based companies and SLTT governments defend their computer systems against unauthorized access, exploitation, and data exfiltration. ECS works by sourcing timely, actionable cyber threat indicators from sensitive and classified Government Furnished Information (GFI). DHS then shares those indicators with accredited Commercial Service Providers (CSPs). Those CSPs in turn use the indicators to block certain types of malicious traffic from entering a company's networks. Groups interested in subscribing to ECS must contract directly with a CSP in order to receive services. Please visit http://www.cisa.gov/enhanced-cybersecurity-services-ecs for a current list of ECS CSP points of contact.

"Hub and spoke" cybersecurity projects are allowable under PSGP for cybersecurity projects that span multiple port area facilities. Hub and spoke cybersecurity projects may affect a parent organization's multiple eligible entities, and maritime security partners, in multiple port areas to provide a port-wide benefit. Such projects may be submitted within a primary Port Area for the project implementation. For example, an applicant in a major port may submit a hub and spoke project within their primary port area which includes system hardening throughout the organization's facilities in that port, as well as two adjacent ports. Proportionally, costs associated with entities or subcomponents that are not covered under an AMSP and are not instrumental to enhancing maritime security must not be included in the detailed budget worksheet or investment justification and thereby prorating the cost of the project only to those facilities that are covered by the AMSP. Following the example noted above, the applicant may not include costs associated with cybersecurity of their non-maritime facilities, such as a non-MTSA regulated facility located inland from the port. Hub and spoke projects are limited only to the enhancement of maritime security as outlined in this section and may not include non-maritime systems or facilities. Please clearly identify hub and spoke projects as such within your IJ and consult your COTP to verify project applicability to enhancing maritime security.
***Cybersecurity projects should address risks to the marine transportation system and/or Transportation Security Incidents (TSIs) outlined in the applicable AMSP, or priorities prescribed under applicable FSP or VSP, as mandated under the MTSA or the PRMPs. At the port level, examples of cybersecurity projects include but are not limited to projects that enhance the cybersecurity of access control, sensors, security cameras, badge/ID readers, ICS/SCADA systems, process monitors and controls (such as those that monitor flow rates, valve positions, tank levels, etc.), security/safety of the ship-to-port-to-facility-to-intermodal***

***interface, and systems that control vital cargo machinery at the ship/shore interface (such as cranes, manifolds, loading arms, etc.), and passenger/vehicle/cargo security screening equipment.***

Vulnerability assessments are generally not funded under PSGP. However, considering the evolving malicious cyber activity, the relative novelty of cybersecurity as a priority within the program, and the need to adopt best practices included in the voluntary Cybersecurity Framework, vulnerability assessments may be funded as contracted costs. Port-wide assessments are eligible and must demonstrate that the assessment includes port area partners and are necessary to be completed as a single project to ensure a comprehensive evaluation of port area cyber security vulnerabilities. Personnel costs (other than M&A) are not an allowable expense for conducting these assessments.

CISA offers free resources to assist with initial assessments, please see https://www.cisa.gov/cyber-resource-hub for additional information. Applicants are encouraged to utilize free resources prior to requesting funds under this program.

***Copies of completed cybersecurity assessments funded under PSGP that impact the maritime transportation system, lead to a "transportation security incident" (as that term is defined under 46 U.S.C. § 70101(6)), or are otherwise related to systems, personnel, and procedures addressed by the facility and vessel plan shall be made available to FEMA and/or the local COTP upon request. The results of these cybersecurity assessments may be designated as Sensitive Security Information (SSI) and may be used to inform national maritime cybersecurity assessments.***

Where a vulnerability assessment has been completed either through contracts or qualified personnel to identify existing gaps and required mitigation efforts, mitigating projects may be funded that include purchase of equipment, software, and infrastructure designed to harden cybersecurity. Specific questions on conducting vulnerability assessments should be referred to the respective FEMA Preparedness Officer.

**C.** Training and Awareness Campaigns

**a.** ***Training***

Port areas should assess their training and qualification requirements and coordinate the training needs and qualification requirements of incident response personnel. Funding for personnel training is limited to those courses that are **essential to enhance *maritime* security, are certified training courses, and personnel costs of only the applicant agency personnel are allowed**. A listing of courses that are currently approved for PSGP funding is included in the table below.

Some training activities require EHP Review, including training that requires any type of land, water, or vegetation disturbance, or building of temporary structures, or that are not located at facilities designed to conduct training. Additional information on the EHP review process can be found online at Environmental & Historic Preservation Grant Preparation Resources | FEMA.gov.

Funding for certified training **courses not listed** in the table below may be permitted on a case-by-case basis depending on the specific maritime security risk mitigation training needs of the eligible PSGP applicant. In such cases, an applicant **MUST** provide the course number, course description, training service provider, explain in the IJ why none of the approved courses referenced in the table below satisfy the identified training need, and submit detailed course information for review and consideration by the local COTP field review team and the Nation Review Panel. **In-house training not provided by certified instructors, and certification provided to graduating students equivalent to the FEMA, State, and Federal Course Catalogs, will not be considered for funding.**

Further, in accordance with 46 U.S.C. § 70107(c)(2)(C), no cost share is required to train public safety personnel in the enforcement of security zones under section 46 U.S.C. § 70132 or assisting the enforcement of such security zones. Per 46 U.S.C. § 70132(d), the term "public safety personnel" includes any federal, state (or political subdivision thereof), territorial, or tribal law enforcement officer, firefighter, or emergency response provider.

Trainings denoted with an asterisk (*) in the table below are exempt from cost share only to train public safety personnel who enforce security zones. Additional training of public safety personnel may be exempt if specifically identified by the COTP as exempt and necessary for enforcement or the assistance of enforcement of security zones as specified by 46 U.S.C. § 70132. ***Requests that fail to include a cost share for training that is not exempt from cost share requirements as outlined in 46 U.S.C. § 70132 will not be considered for funding.*** Training for public safety personnel who do not provide enforcement of security zones are not exempt from cost share. Training rosters and certificates must be provided to FEMA upon request. Please consult your COTP prior to requesting cost share exempt training for enforcement of security zones.

**Seminars, drills, and workshops are not considered "Training;"** however, applicants wishing to host seminars, drills, or workshops with PSGP funding may be eligible for funding following the criteria set forth in the "Exercise" section of this guidance.

**Approved PSGP Training Courses**

| National Training and Education Division | |
|---|---|
| **Course Number** | **Course Name** |
| AWR-144 | Port and Vessel Security for Public Safety and Maritime Personnel |
| AWR-213 | Critical Infrastructure Security and Resilience Awareness |
| AWR-366-W | Developing a Cyber Security Annex for Incident Response |
| MGT-335 | Event Security Planning for Public Professionals |
| MGT-335-W | Event Security Planning for Public Professionals, Web Based |
| MGT-400 | Master of Arts Degree in Homeland Security |
| MGT-425 | Homeland Security Executive Leaders Program (ELP) |
| MGT-452 | Physical and Cybersecurity for Critical Infrastructure |
| MGT-456 | Integration of Cybersecurity Personnel into the Emergency Management Operations Center for Cyber Incidents |

| | |
|---|---|
| PER-330 | The Surface Transportation Emergency Preparedness and Security for Mass Transit and Passenger Rail (STEPS-PT) |
| PER-331 | Surface Transportation Emergency Preparedness and Security for Senior Officials or Administrators (STEPS Sr) |
| **Federal-Sponsored** | |
| **Course Number** | **Course Name** |
| DHS-006-PREV | Seaport Security Anti-Terrorism Training Program (SSATP) |
| DHS-011-PREV | Maritime PRND Operations Course |
| DHS-016-PREV | Protective Measures Training for Security Officers, Mid-Level Safety/Security Supervisors, and Property Managers |
| *DHS-011-PROT | NASBLA BOAT Tactical Operators Course |
| *DHS-009-PROT | Boat Operator's Anti-Terrorism Training |
| DHS-126-RESP | NASBLA BOAT Crew Member Course |
| *DHS-128-RESP | NASBLA - Pursuit and Stop Course |
| **State-Sponsored** | |
| **Course Number** | **Course Name** |
| CA-006-PREV | Maritime Company, Vessel, and Facility Security Officer |
| CA-007-PREV | Basic Maritime Security Awareness |
| CA-008-PREV | Basic First Responder Operational Maritime Security (FROMS) |
| CA-015-RESP | Maritime Facility Security Officer |
| CA-020-RESP | WMD & Terrorism Awareness for Security Professionals |
| ME-001-PROT | Maritime Security Awareness for Military, First Responder and Law Enforcement Personnel |
| ME-002-PROT | Command Strategies and Tactics for Marine Emergencies |
| *ME-003-PROT | Tactical Boat Operations for Maritime Security and LE Personnel |
| ME-002-RESP | Emergency Medical Operations in the Maritime Domain |
| NJ-003-PREV | Government Agency Maritime Security Awareness Program (GAMSAP) |
| NJ-015-PREV | Security Awareness & Vigilance for Everyone |
| NY-001-PREV | Maritime Infrastructure Protection |
| NY-001-PROT | Safe Boat Operators |
| *NY-002-PREV | Tactical Escorts and Security Zones |
| NY-002-PROT | Pattern Line Search/Recovery Course |
| NY-004-RESP | Vehicle Borne Improvised Explosive Device Security Checkpoint |
| **Federal Law Enforcement Training Center (FLETC)** | |
| **Course Number** | **Course Name** |
| *MTOTP | Marine Law Enforcement Training Program |
| IBOT | Inland Boat Operator’s Training |
| ENTP | Electronic Navigation Training Program |

| | |
|---|---|
| *BOAT | Boat Operator's Anti-Terrorism Training Program |
| *MLETP | Marine Law Enforcement Training Program |
| *CVBTP | Commercial Vessel Boarding Training Program |
| *SSATP | Seaport Security Anti-Terrorism Training Program |

**b.** ***Awareness Campaigns***
Program funds may be used for the development and implementation of awareness campaigns to raise public awareness of indicators of terrorism and terrorism-related crime and for associated efforts to increase the sharing of information with public and private sector partners, including nonprofit organizations. DHS currently sponsors or supports a number of awareness campaigns. Please review materials, strategies, and resources at https://www.dhs.gov/dhs-campaigns before embarking on the development of an awareness campaign for local constituencies and stakeholders.

***Note: DHS requires that all public and private sector partners wanting to implement and/or expand the DHS "If You See Something, Say Something®" campaign ("campaign") using grant funds work directly with the DHS Office of Partnership and Engagement (OPE). This will help ensure that the awareness materials (e.g., videos, posters, trifolds, etc.) remain consistent with DHS's messaging and strategy for the campaign and compliant with the initiative's trademark, which is licensed to DHS by the New York Metropolitan Transportation Authority. Coordination with OPE, through the campaign's office (seesay@hq.dhs.gov), must be facilitated by the applicable FEMA HQ Preparedness Officer.***

**D.** Exercises
Exercises funded under the PSGP typically include Seminars, Workshops, Tabletops, Functional, Drills, and Full-Scale exercises. PSGP-funded exercises must have a maritime security focus and include applicable documentation, after action reports, and improvement plans. See below for additional information.

Maritime entity training needs and qualification requirements of incident response personnel should be regularly tested through emergency exercises and drills. Exercises must test operational protocols that would be implemented in the event of a terrorist attack in the maritime environment in accordance with the Area Maritime Security Training Exercise Program (AMSTEP) or the TSA Intermodal Security Training Exercise Program (I-STEP) guidelines. AMSTEP or I-STEP exercises will follow the latest change in requirements contained in the Navigation and Inspection Circular (NVIC) 09-02. Exercises must be designed, developed and conducted consistent with the Homeland Security Exercise and Evaluation Program (HSEEP). Funding used for exercises will only be permitted for those exercises that are in direct support of a MTSA-regulated facility or a port area's MTSA-required exercises (*see* 33 C.F.R. § 105.220 for a facility and 33 C.F.R. § 103.515 for the AMSP). These exercises must be coordinated with the COTP and AMSC and be consistent with HSEEP.

Some exercise activities require EHP Review, typically including drills, functional and full-scale exercises that require any type of land, water, or vegetation disturbance or building of temporary structures or that are not located at facilities designed to conduct exercises. Additional information

on EHP review can be found online at Environmental & Historic Preservation Grant Preparation Resources | FEMA.gov.

Recipients are required to submit an After-Action Report/Improvement Plan (AAR/IP) for each PSGP-funded exercise to hseep@fema.dhs.gov, and the appropriate local COTP no later than 90 days after completion of the exercise conducted within the PSGP period of performance (POP). Recipients are reminded of the importance of implementing corrective actions iteratively throughout the progressive exercise cycle. Recipients are required to use the HSEEP AAR/IP template located at https://preptoolkit.fema.gov/web/hseep-resources/improvement-planning.

Recipients of PSGP funding for exercises should verify in progress reports the completion of the exercise(s), after-action report(s), improvement plan(s), and notifications made to hseep@fema.dhs.gov and the COTP.

PSGP funds may be used for the following exercise activities:

1. **Funds Used to Design, Develop, Conduct, and Evaluate an Exercise.** This includes costs related to planning, meeting space, and other meeting costs, facilitation costs, materials and supplies, travel, and documentation. See "2 CFR § 200.432 Conferences" for related allowable costs. 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. Any shortcoming or gap identified, including those for children and individuals with disabilities or other access and functional needs, should be identified in an effective corrective action program that includes development of improvement plans that are dynamic documents, with corrective actions continually monitored and implemented as part of improving preparedness through the exercise cycle.
2. **Hiring of Full- or Part-Time Staff or Contractors/Consultants.** Full- or part-time staff may be hired to support exercise-related activities. Hiring of contractors/consultants must follow the applicable federal procurement requirements at 2 C.F.R. § 200.317-200.327. Dual compensation is never allowable, meaning, in other words, that an employee of a unit of government may not receive compensation from his or her unit or agency of government and from an award for a single period of time (e.g., 1:00 p.m. to 5:00 p.m.), even though such work may benefit both entities. Personnel hiring, overtime, and backfill expenses are permitted under this grant only to the extent that such expenses are for the allowable activities within the scope of the grant.
3. **Overtime and Backfill Costs.** The entire amount of overtime costs, including payments related to backfilling personnel that are the direct result of time spent on the design, development and conduct of exercises are allowable expenses. These costs are allowed only to the extent the payment for such services is in accordance with the policies of the state or unit(s) of local government and has the approval of the state or the awarding agency, whichever is more restrictive. Dual compensation is never allowable.
4. **Travel.** Domestic travel costs are allowable as expenses by employees who are on travel status for official business related to the planning and conduct of exercise project(s). International travel costs are not permitted.
5. **Supplies.** Supplies are items that are expended or consumed during the course of the planning and conduct of the exercise project(s) (e.g., gloves, non-sterile masks, and

disposable protective equipment).

6. **Other Items.** These costs include the rental of space/locations for exercise planning and executing, rental of equipment, etc. Recipients are encouraged to use free public space, locations, or facilities, whenever available, prior to the rental of space, locations, or facilities. These also include costs that may be associated with inclusive practices and the provision of reasonable accommodations and modifications to provide full access for children and adults with disabilities.

The National Exercise Program (NEP) serves as the principal exercise mechanism for examining national preparedness and measuring readiness. Recipients are strongly encouraged to nominate exercises into the NEP. For additional information on the NEP, please refer to http://www.fema.gov/national-exercise-program.

**E.** Maintenance and Sustainment Costs

Maintenance and sustainment related costs are allowed and **limited to repair and replacement** under this program only as described in this NOFO and the Preparedness Grants Manual.

**F.** Construction and Renovation

Construction and renovation costs are allowed under this program. For construction costs to be allowed, they must be specifically approved by DHS/FEMA in writing prior to the use of any program funds for construction or renovation. Additionally, recipients are required to submit a SF-424C Budget and budget detail citing the project costs. All proposed construction and renovation activities must undergo an Environmental Planning and Historic Preservation (EHP) review, including approval of the review from FEMA, prior to undertaking any action related to the project. Failure of a grant recipient to meet these requirements may jeopardize Federal funding. See the Preparedness Grants Manual for additional information.

**G.** Organization Costs

Allowable organization-related costs are limited to those activities associated with new and ongoing maritime security operations essential to the national priorities. All such activities must be focused **exclusively on maritime security** and coordinated with the local Captain of the Port (COTP). PSGP funding used for organizational costs will only fund immediate needs for personnel that will be directly engaged in maritime security activities. Allowable organization personnel costs include:

1. **Backfill, Overtime, Hiring of Full or Part-Time Personnel or Contractors/Consultants.** Full or part-time staff or contractors/consultants may be hired to support maritime-security-related activities and/or training or exercises conducted under this grant only for the allowable activities within the scope of the grant. Hiring of contractors/consultants must follow the applicable federal procurement requirements at 2 C.F.R. §§ 200.317-200.327. Salary and fringe benefit payments must be in accordance with the policies of the state or unit(s) of local government and have the approval of the state or awarding agency. Dual compensation is not allowable. That is, an employee of a unit of government may not receive compensation from their unit or agency of government AND from an award for a single period of time (e.g., 1:00 p.m. to 5:00 p.m.), even though such work may benefit both activities. Limitations may apply for grant related activities. See specific guidance provided within this Manual for additional details

on allowable organization costs (i.e., Training – Personnel costs are limited to backfill and overtime).

2. **Hiring new, full-time personnel to:**
   - Operate maritime security patrol vessels (first response agencies only);
   - Staff a new or expanded interagency maritime security operation center;
   - Support maritime security/counterterrorism efforts in the local Joint Terrorism Task Force (JTTF) and/or fusion center; and
   - Support credentialing access to a MTSA facility.
3. **Backfill and Overtime costs for existing personnel to:**
   - Operate patrol vessels in support of pre-planned, mission critical activities, as identified by the local COTP (not including routine patrol); and
   - Attend approved maritime security training courses.
   - Participate in approved maritime security exercises.
4. **Personnel or contracted costs to:**
   - Install, repair, and replace maritime security equipment. Note this does not include routine maintenance, such as oil changes and daily/weekly systems tests; and
   - Management and administration (M&A) of projects funded under this program.
   - Design, develop and conduct maritime security exercises.
5. **Contracted costs to:**
   - Provide approved training courses; and
   - Provide warranty, maintenance, and service agreements for equipment purchased under this grant.

Organization costs will only be funded to address port (or facility) security needs as outlined in this NOFO. PSGP funding for new permanent or part-time personnel will not exceed the 36-month period of performance. Applicants must provide reasonable assurance that personnel costs can be sustained beyond the 36-month award period. ***A sustainment plan must be submitted with the applicant's IJ to address the 12-month period beyond the period of performance of the award.***

**H.** Authorized Use of Contractual Grant Writers and/or Grant Managers

A grant applicant may procure the services of a contractor to provide support and assistance for pre-award grant development services (grant writing) or post-award grant management and administrative services (grant management). As with all federal grant-funded procurements, grant writer or grant management services must be procured in accordance with the federal procurement standards at 2 C.F.R. §§ 200.317 – 200.327. See the Preparedness Grants Manual regarding Procurement Integrity, particularly the sections applicable to non-state entities that discuss organizational conflicts of interest under 2 C.F.R. § 200.319(b) and traditional conflicts of interest under 2 C.F.R. § 200.318(c)(1). States must follow the same policies and procedures it uses for procurements of its non-federal funds, pursuant to 2 C.F.R. § 200.317, which also applies 2 C.F.R. §§ 200.321, 200.322, 200.323, and 200.327.

As applicable to non-state entities, DHS/FEMA considers a contracted grant writer to be an agent of the recipient for any subsequent contracts the recipient procures under the same federal award in which the grant-writer provided grant writing services. Federal funds and funds applied to a federal award's cost share generally cannot be used to pay a contractor to carry out the work

if that contractor also worked on the development of such specifications unless the original contract was properly procured and included both grant writing and grant management services in the solicitation's scope of work.

As applicable to all non-federal entities, regardless of whether an applicant or recipient uses grant writing and/or grant management services, the recipient is solely responsible for the fiscal and programmatic integrity of the grant and its authorized activities and expenditures. The recipient must ensure adequate internal controls, including separation of duties, to safeguard grant assets, processes, and documentation, in keeping with the terms and conditions of its award, including this NOFO, and 2 C.F.R. Part 200.

**a. *Grant Writers***

Grant writing contractors may assist the applicant in preparing, writing, and finalizing grant application materials and assisting the applicant with handling online application and submission requirements in FEMA GO. Grant writers may assist in a variety of ways. Ultimately, however, the applicant that receives an award is solely responsible for all grant award and administrative responsibilities.

By submitting the application, applicants certify that all of the information contained therein is true and an accurate reflection of the organization and that regardless of the applicant's intent, the submission of information that is false or misleading may result in actions by DHS/FEMA. These actions include but are not limited to the submitted application not being considered for an award, temporary withholding of funding under the existing award pending investigation, or referral to the DHS Office of the Inspector General.

To assist applicants with the cost of grant writing services, DHS/FEMA is permitting a one-time pre-award cost of no more than $1,500 per applicant per year for contractual grant writing services as part of the recipient's M&A costs. This is only intended to cover costs associated with a grant writer and may not be used to reimburse the applicant for their own time and effort in the development of a grant application. Additionally, the applicant may be required to pay this fee with its own funds during the application preparation and submission period. If the applicant subsequently receives an award, the applicant may then request to be reimbursed once grant funds become available for that cost, not to exceed $1,500. If the applicant does not receive an award, this cost will not be reimbursed by the federal government. The applicant must understand this risk and be able to cover this cost if an award is not made.

If an applicant intends to request reimbursement for this one-time pre-award cost, it must include this request in its application materials, including in the budget detail worksheet for each IJ. Failure to clearly identify this as a separate cost in the application may result in its disallowance. This is the only pre-award cost eligible for reimbursement. Recipients must maintain grant writer fee documentation including, but not limited to, a copy of the solicitation, such as a quote request, rate request, invitation to bid, or request for proposals, if applicable; a copy of the grant writer's contract agreement; a copy of the invoice or purchase order; and a copy of the canceled check or proof of payment. These records must be made available to DHS/FEMA upon request.

***Consultants or contractors are not permitted to be the AOR or SA of the recipient.*** Further, an application must be officially submitted by 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.

**b.** ***Grant Managers***
Grant management contractors provide support in the day-to-day management of an active grant retain grant management contractors at their own expense.

***Consultants or contractors are not permitted to be the AOR or SA of the recipient.*** The AOR is responsible for submitting programmatic and financial performance reports, accepting award packages, signing assurances and certifications, and submitting award amendments.

**c.** ***Restrictions Regarding Grant Writers and Grant Managers***
Pursuant to 2 C.F.R. Part 180, recipients may not use federal grant funds to reimburse any entity, including a grant writer or preparer, if that entity is presently suspended or debarred by the Federal Government from receiving funding under federally funded grants or contracts. Recipients must verify that a contractor is not suspended or debarred from participating in specified federal procurement or non-procurement transactions pursuant to 2 C.F.R. § 180.300. FEMA recommends recipients use SAM.gov to conduct this verification. Further, regardless of whether any grant writer fees were requested, as applicable to non-state entities, unless a single contract covering both pre- and post-award services was awarded to the grant writer and procured in compliance with 2 C.F.R. §§ 200.317 – 200.327, federal funds cannot be used to pay the grant writer to provide post-award services.

**I.** Reprogramming Award Funds
Reprogramming award funds is limited under this program and is generally only approved for allowable program activities that are related to the original approved scope of work .

**J.** Limitations on Funding
As part of the PSGP application process, applicants must complete the approved Investment Justification (IJ) template and detailed budget sheets (incorporated into the IJ) provided addressing each initiative being proposed for funding (FF-207-FY-23-108 (formerly 089-5) IJ-Budget). **Only ONE form** should be submitted with each application. A corresponding detailed budget tab is included within the IJ and must be completed for each project, including the budget summary at the bottom of the form. Each project should represent the complete scope of work and materials required to achieve a single overall capability. For example, a project could be to procure a boat specifically designed and equipped as a CBRNE detection, prevention, response, and/or recovery platform. The IJ for this example project should include the CBRNE equipment in the same IJ as the vessel. The corresponding detailed budget should include a description of the equipment (i.e., 24’ Response Vessel) and computation (i.e., 1 x $375,000, total $375,000; Vessel mounted Rad/Nuke detection device, 1 x $25,000, total $25,000). Additionally, the total computation for the Total Project Cost, Federal Share, and non-Federal Share must be included in the detailed budget (i.e., Total $400,000; Federal Share $300,000; non-Federal Share $100,000). This demonstrates that the applicant and FEMA understand the level of Federal funding requested, as well as a commitment to the Cost Share required by the applicant to

complete the project. (see “Cost-Share or Match” in Section C above).

In accordance with 46 U.S.C. § 70107(b)(2), PSGP funding for projects for the cost of acquisition, operation, and maintenance of security equipment or facilities to be used for security monitoring and recording, security gates and fencing, marine barriers for designated security zones, security-related lighting systems, remote surveillance, concealed video systems, security vessels, and other security-related infrastructure or equipment that contributes to the overall security of passengers, cargo, or crewmembers **cannot exceed $1 million federal share per project**. The $1 million per project limitation applies only to those projects funded under 46 U.S.C. § 70107(b)(2) and does not apply to projects funded under other provisions of Section 70107.