The U. S. Department of Homeland Security (DHS) Notice of Funding Opportunity (NOFO) Fiscal Year 2024 Port Security Grant Program

Release Date: Apr 16, 2024

Download a PDF version of this webpage.

> **All entities wishing to do business with the federal government must have a unique entity identifier (UEI). The UEI number is issued by the system. Requesting a UEI using System for Award Management (SAM.gov) can be found at:** https://sam.gov/content/entity- registration.

Updates in Grant Application Forms:

The Data Universal Numbering System (DUNS) Number was replaced by a new, non-proprietary identifier requested in, and assigned by SAM.gov. This new identifier is the Unique Entity Identifier.

Additional Information can be found on Grants.gov: https://www.grants.gov/forms/forms-development/planned-uei-updates.

Table of Contents

A. **Program Description**

1. Issued By
2. Assistance Listings Number
3. Assistance Listings Title
4. Funding Opportunity Title

5. Funding Opportunity Number
6. Authorizing Authority for Program
7. Appropriation Authority for Program
8. Announcement Type
9. Program Category
10. Program Overview, Objectives, and Priorities
11. Performance Measures

B. **Federal Award Information**

1. Available Funding for the NOFO: $90,000,000
2. Period of Performance: 36 months
3. Projected Period of Performance Start Date(s): September 1, 2024
4. Projected Period of Performance End Date(s): August 31, 2027
5. Projected Budget Period(s)
6. Funding Instrument Type: Grant

C. **Eligibility Information**

1. Eligible Applicants
2. Applicant Eligibility Criteria
3. Subawards and Beneficiaries
4. Other Eligibility Restrictions
5. Cost Share or Match

D. **Application and Submission Information**

1. Key Dates and Times
2. Agreeing to Terms and Conditions of the Award
3. Address to Request Application Package
4. Requirements: Obtain a Unique Entity Identifier (UEI) and Register in the System for Award Management (SAM)
5. Steps Required to Obtain a Unique Entity Identifier, Register in the System for Award Management (SAM), and Submit an Application
6. Electronic Delivery
7. How to Register to Apply
8. Create a login.gov account
9. Submitting the Application

10. Timely Receipt Requirements and Proof of Timely Submission
11. Intergovernmental Review
12. Funding Restrictions and Allowable Costs

E. Application Review Information

1. Application Evaluation Criteria
2. Review and Selection Process

F. Federal Award Administration Information

1. Notice of Award
2. Administrative and National Policy Requirements
3. Reporting
4. Monitoring and Oversight

G. DHS Awarding Agency Contact Information

1. Contact and Resource Information
2. Systems Information

H. Additional Information

1. Termination Provisions
2. Program Evaluation
3. Financial Assistance Programs for Infrastructure
4. Report issues of fraud, waste, abuse
5. Appendices

A. Program Description

1. Issued By

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

2. Assistance Listings Number

97.056

3. Assistance Listings Title

Port Security Grant Program

4. Funding Opportunity Title

Fiscal Year 2024 Port Security Grant Program (PSGP)

5. Funding Opportunity Number

DHS-24-GPD-056-00-99

6. Authorizing Authority for Program

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

7. Appropriation Authority for Program

Department of Homeland Security Appropriations Act, 2024, Pub. L. No. 118-47, Title III, "Protection, Preparedness, Response, and Recovery"

8. Announcement Type

Initial

9. Program Category

Preparedness: Infrastructure Security

10. Program Overview, Objectives and Priorities

a. Overview

The Fiscal Year (FY) 2024 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 of PSGP since inception (2001) to present includes approximately **$3,288,610,706** for approximately **4,800** grant awards dedicated specifically for enhancing maritime security capabilities throughout U.S. ports.

For FY 2024, DHS is focused on the criticality of information sharing and collaboration to building a national culture 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. The threat profile has changed in the past two decades. We now face continuous cyber threats by sophisticated actors, threats to soft targets and crowded places, and threats from domestic violent extremists, who represent one of the most persistent threats to the nation today . Therefore, for FY 2024, DHS has identified two priority areas related to some of the most serious threats that recipients should address with their PSGP funds for enhancing maritime security. These two priority areas are enhancing cybersecurity and enhancing the protection of soft targets/crowded places. DHS also will continue to forge partnerships to strengthen information sharing and collaboration in each of these priority areas.

For FY 2023, 403 applications were received and 299 approved for funding. For a full list of recipients, please refer to Information Bulletin (IB) 490a.

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 to meet the following objectives:

1. Build and sustain core capabilities of maritime infrastructure systems in annual national priority areas, including for FY 2024 the priorities of

enhancing cybersecurity and enhancing the protection of soft targets/crowded places.
2. Address and close gaps identified in Area Maritime Transportation 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. In assessing the national risk profile for FY 2024, two areas warrant the most concern:

1. Enhancing cybersecurity; and
2. Enhancing the protection of soft targets/crowded places.

For more information about these priorities, see Section D.10.b.

Likewise, there are several enduring security needs that crosscut the homeland security enterprise. The following are second-tier priorities that help recipients implement a comprehensive approach to securing critical maritime transportation infrastructure:

3. Effective planning;
4. Training and awareness campaigns;
5. Equipment and capital projects; and
6. Exercises.

The table below provides a breakdown of these priority areas for the FY 2024 PSGP, showing both the 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 two National Priorities (enhancing cybersecurity or enhancing the protection of soft targets/crowded places) will have their final review scores increased by a multiplier of 20%.

FY 2024 PSGP Funding Priorities

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

National Priorities

Priority Areas	Core Capabilities	Example Project Types

Enhancing Cybersecurity	Cybersecurity Intelligence and information sharing Planning Public information and warning Operational coordination Screening, search, and detection Access control and identity verification Supply chain integrity and security Risk management for protection programs and activities Long-term vulnerability reduction Situational assessment Infrastructure systems Operational communications	Cybersecurity risk assessments Projects that address vulnerabilities identified in cybersecurity risk assessments Improving cybersecurity of critical infrastructure 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 Adoption of cybersecurity performance goals (CISA's Cross-Sector Cybersecurity Performance Goals) Cybersecurity training and planning

Enhancing the Protection of Soft Targets and Crowded Places	Operational coordination Public information and warning Intelligence and Information Sharing Interdiction and disruption Screening, search, and detection Access control and identity verification Physical protective measures Risk management for protection programs and activities	Operational coordination Public information and warning Intelligence and Information Sharing Interdiction and disruption Screening, search, and detection Access control and identity verification Physical protective measures Risk management for protection programs and activities

Enduring Needs

Priority Areas	Core Capabilities	Example Project Types

Planning	Planning Risk management for protection programs and activities Risk and disaster resilience assessment Threats and hazards identification Operational coordination Community resilience	Development of: Port-wide Security Risk Management Plans Continuity of Operations Plans Response Plans Port-wide and/or asset-specific vulnerability assessments Assessments should consider the impacts of climate change on investments to close identified security gaps Efforts to strengthen governance integration between/among regional partners
Training and Awareness	Long-term vulnerability reduction Public information and warning Operational coordination Situational assessment Community resilience	Active shooter training, including integrating the needs of persons with disabilities Shipboard firefighting training Public awareness/preparedness campaigns Maritime domain awareness projects

Equipment and Capital Projects	Long-term vulnerability reduction Infrastructure systems Operational communications Interdiction and disruption Screening, search, and detection Access control and identity verification Physical protective measures Supply chain integrity and security Threats and hazards identification Infrastructure systems Intelligence and information sharing	Implementing risk management projects that support port resilience and recovery Implementing physical security enhancement projects Transportation Worker Identification Credential projects Sharing and leveraging intelligence and information Chemical, Biological, Radiological, Nuclear, and Explosive prevention, detection response and recovery equipment Unmanned Aircraft Systems and detection technologies

Exercises	Long-term vulnerability reduction Operational coordination Operational communications Community resilience	Response exercises

c. Alignment to Program Purpose and the DHS and FEMA Strategic Plan

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

The 2022-2026 FEMA Strategic Plan outlines three bold, ambitious goals in order to position FEMA to address the increasing range and complexity of disasters, support the diversity of communities we serve, and complement the nation's growing expectations of the emergency management community. The PSGP supports Goal 3 to Promote and Sustain a Ready FEMA and Prepared Nation. We invite our stakeholders and partners to also adopt these priorities and join us in building a more prepared and resilient nation.

11. Performance Measures

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 the section above.

B. Federal Award Information

1. Available Funding for the NOFO: $90,000,000

2. Period of Performance: 36 months

Extensions to the period of performance are allowed. For additional information on period of performance extensions, please refer to the Preparedness Grants Manual (FM-207-23-001).

3. Projected Period of Performance Start Date(s): September 1, 2024

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

5. Projected Budget Period(s) : There will be only a single budget period with the same start and end dates as the period of performance. See 2 C.F.R. § 200.1 for definitions of "budget period" and "period of performance."

6. Funding Instrument Type: Grant

C. Eligibility Information

1. Eligible Applicants

All entities subject to an AMSP, as defined by 46 U.S.C. § 70103(b), may apply for PSGP funding. Eligible applicants include but are not limited to 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. Examples of facility operators 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.

2. Applicant Eligibility Criteria

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. In administering the grant program, national, economic, energy, and strategic defense concerns based upon the most current risk assessments available will be considered.

Port Area Definition

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, as discussed later in this NOFO.

- 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.*** 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.

An application submitted by an otherwise eligible non-federal entity (i.e., the applicant) may be deemed ineligible when the person that submitted the application is not: 1) a ***current employee, personnel, official, staff, or leadership*** of the non-federal entity; and 2) ***duly authorized to apply*** for an award on behalf of the non-federal entity at the time of application.

Further, the Authorized Organization Representative (AOR) 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.***

Compliance with Maritime Security Regulations

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:

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
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.

The local USCG Captain of the Port (COTP) will verify security compliance eligibility during the field review process. Eligibility does not guarantee grant funding..

Ferry Systems

Ferry systems are eligible to apply for FY 2024 PSGP funds. However, any ferry system electing to participate (e.g., submit an application) under the FY 2024 PSGP will not be eligible to participate (e.g., submit an application) under the FY 2024 Transit Security Grant Program (TSGP) and will not be considered for funding under the FY 2024 TSGP. Likewise, any ferry system that participates in the FY 2024 TSGP will not be eligible for funding under the FY 2024 PSGP.

Subawards

Subawards are prohibited under PSGP. Applicants are also prohibited from applying on behalf of other, separate entities. Notwithstanding this prohibition, however, community-based projects, to include planning, training, exercises, and port-wide cyber vulnerability assessments and cyber interoperability projects that may include multiple beneficiaries (e.g., a port authority hosts a large training session or exercise) in which the applicant applies for and administers the grant award are allowable. Only the eligible applicant is permitted to take ownership of PSGP-funded equipment and other non-consumables until disposition actions are required.

3. Subawards and Beneficiaries

a. *Subaward allowability*

Subawards are prohibited under the PSGP. Applicants are also prohibited from applying on behalf of other, separate entities. Notwithstanding this prohibition, however, community-based projects, to include planning, training, exercises, and port-wide cyber vulnerability assessments and cyber interoperability projects that may include multiple beneficiaries (e.g., a port authority hosts a large training session or exercise) in which the applicant applies for and administers the grant award are allowable. Only the eligible applicant is permitted to take ownership of PSGP-funded equipment and other non-consumables until disposition actions are required.

b. Beneficiaries or Participants

This NOFO and any subsequent federal awards create no rights or causes of action for any participant or beneficiary.

4. Other Eligibility Restrictions

a. National Incident Management System (NIMS) Implementation

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.

5. Cost Share or Match

The FY 2024 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.

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 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.

Public-Sector Cost Share

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. For example, if the federal award for a public sector recipient requires a 25% cost share and the total project cost is $100,000, then:

- Federal share is 75% of $100,000 = $75,000
- Recipient cost share is 25% of $100,000 = $25,000

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.

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.

Private-Sector Cost Share

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. For example, if the federal award for a private sector recipient requires a 50% cost share and the total project cost is $100,000, then:

- Federal share is 50% of $100,000 = $50,000
- Recipient cost share is 50% of $100,000 = $50,000

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.

Exceptions to the Cost Match Requirements

The following exceptions to the cost match requirement may apply:

- **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:
  - Port-wide planning, training, and exercises;
  - Security camera systems with shared access;
  - Response vessels; and
  - Other maritime domain awareness systems.
- **$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.
- **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.

D. Application and Submission Information

1. Key Dates and Times

a. Application Start Date: 04/16/2024

b. Application Submission Deadline: 06/24/2024 at 5 p.m. ET

All applications **must** be received by the established deadline.

FEMA’s Grants Outcomes System (FEMA GO) automatically records proof of timely submission and the system generates an electronic date/time stamp when FEMA GO successfully receives the application. The individual with the AOR role that submitted the application will also receive the official date/time stamp and a FEMA GO tracking number in an email serving as proof of their timely submission. For additional information on how an applicant will be notified of application

receipt, see the subsection titled “Timely Receipt Requirements and Proof of Timely Submission” in Section D of this NOFO.

FEMA will not review applications that are received after the deadline or consider these late applications for funding. FEMA may, however, extend the application deadline on request for any applicant who can demonstrate that good cause exists to justify extending the deadline. Good cause for an extension may include technical problems outside of the applicant’s control that prevent submission of the application by the deadline, other exigent or emergency circumstances, or statutory requirements for FEMA to make an award.

Applicants experiencing technical problems outside of their control must notify FEMA as soon as possible and before the application deadline. Failure to timely notify FEMA of the issue that prevented the timely filing of the application may preclude consideration of the award. “Timely notification” of FEMA means the following: prior to the application deadline and within 48 hours after the applicant became aware of the issue.

A list of FEMA contacts can be found in Section G of this NOFO, “DHS Awarding Agency Contact Information.” 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 Eastern Time (ET). For programmatic or grants management questions, please contact your Preparedness Officer or Grants Management Specialist. If applicants do not know who to contact or if there are programmatic questions or concerns, please contact fema-grants-news@fema.dhs.gov, Monday through Friday, 9:00 AM – 5:00 PM ET.

c. Anticipated Funding Selection Date: No later than August 23, 2024

d. Anticipated Award Date: No later than September 30, 2024

e. Other Key Dates:

Event	Suggested Deadline for Completion
Obtaining Unique Entity Identifier (UEI) number	Four weeks before actual submission deadline
Obtaining a valid Employer Identification Number (EIN)	Four weeks before actual submission deadline
Creating an account with login.gov	Four weeks before actual submission deadline
Registering in SAM or updating SAM registration	Four weeks before actual submission deadline
Registering Organization in FEMA GO	Prior to beginning application
Submitting complete application in FEMA GO	One week before actual submission deadline

2. Agreeing to Terms and Conditions of the Award

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

3. Address to Request Application Package

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

4. Requirements: Obtain a Unique Entity Identifier (UEI) and Register in the System for Award Management (SAM.gov)

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

1. Be registered in Sam.Gov before application submission.
2. Provide a valid UEI in its application.

3. Continue to always maintain an active SAM registration with current information during the federal award process. Note: Per 2 C.F.R. § 25.300, subrecipients are NOT required to go through the full SAM registration process. First-tier subrecipients (meaning entities receiving funds directly from the recipient) are only required to obtain a UEI through SAM, but they are not required to complete the full SAM registration in order to obtain a UEI. Recipients may not make subawards unless the subrecipient has obtained and provided the UEI.

Lower-tier subrecipients (meaning entities receiving funds passed through by a higher-tier subrecipient) are not required to have a UEI and are not required to register in SAM. Applicants are also not permitted to require subrecipients to complete a full registration in SAM beyond obtaining the UEI.

5. Steps Required to Obtain a Unique Entity Identifier, Register in the System for Award Management (SAM), and Submit an Application

Applying for an award under this program is a multi-step process and requires time to complete. Applicants are encouraged to register early as the registration process can take four weeks or more to complete. Therefore, registration should be done in sufficient time to ensure it does not impact your ability to meet required submission deadlines. Please review the table above for estimated deadlines to complete each of the steps listed. Failure of an applicant to comply with any of the required steps before the deadline for submitting an application may disqualify that application from funding.

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

- Apply for, update, or verify their UEI number and Employer Identification Number (EIN) from the Internal Revenue Service;
- In the application, provide an UEI number;
- Have an account with login.gov;
- Register for, update, or verify their SAM account and ensure the account is active before submitting the application;
- Register in FEMA GO, add the organization to the system, and establish the 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/grants/guidance-tools/fema-

go/startup;
- Submit the complete application in FEMA GO; and
- 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.

Applicants are advised that FEMA may not make a federal award until the applicant has complied with all applicable SAM requirements. Therefore, an applicant's SAM registration must be active not only at the time of application, but also during the application review period and when FEMA is ready to make a federal award. Further, as noted above, an applicant's or recipient's SAM registration must remain active for the duration of an active federal award. If an applicant's SAM registration is expired at the time of application, expires during application review, or expires any other time before award, FEMA may determine that the applicant is not qualified to receive a federal award and use that determination as a basis for making a federal award to another applicant.

Per 2 C.F.R. § 25.110(c)(2)(iii), 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 by contacting fema-grants-news@fema.dhs.gov and providing the details of the circumstances that prevent completion of these requirements. If FEMA determines that there are exigent circumstances and FEMA has decided to make an award, the applicant will be required to obtain an UEI number, if applicable, and complete SAM registration within 30 days of the federal award date.

6. Electronic Delivery

DHS is participating in the Grants.gov initiative to provide the grant community with a single site to find and apply for grant funding opportunities. DHS encourages or requires applicants to submit their applications online through Grants.gov, depending on the funding opportunity.

For this funding opportunity, FEMA requires applicants to submit applications through FEMA GO.

7. How to Register to Apply

1. **General Instructions:**

   Registering and applying for an award under this program is a multi-step process and requires time to complete. Read the instructions below about registering to apply for FEMA funds. Applicants should read the registration instructions carefully and prepare the information requested before beginning the registration process. Reviewing and assembling the required information before beginning the registration 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 an UEI number, an EIN, and an active SAM registration to apply for a federal award under this funding opportunity.

2. **Obtain an 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

3. **Obtain Employer Identification 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.

4. **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 here: https://secure.login.gov/sign_up/enter_email?request_id=34f19fa8-14a2-438c-8323-a62b99571fd3.
Applicants only have to create a login.gov account once. For applicants that are existing SAM users, use the same email address for the login.gov account as with 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.

5. Register with SAM:
All applicants applying online through FEMA GO must register with SAM. Failure to register with SAM will prevent an applicant from completing the application in FEMA GO. SAM registration must be renewed annually. Organizations will be issued a UEI number with the completed SAM registration.

For more detailed instructions for registering with SAM, refer to: https://apply07.grants.gov/help/html/help/Register/RegisterWithSAM.htm.

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 last three years, if applicable.

i. Additional SAM Reminders

Existing SAM.gov account holders should check their account to make sure it is "ACTIVE." SAM registration should be completed at the very beginning of the application period and should be renewed annually to avoid being "INACTIVE." ***Please allow plenty of time before the grant application submission deadline to obtain an UEI number and then to register in SAM. It may be four weeks or more after an applicant submits the SAM registration before the registration is active in SAM, and then it may be an additional 24 hours before FEMA's system recognizes the***

information.

It is imperative that the information applicants provide is correct and current. Please ensure that your organization's name, address, and EIN are up to date in SAM and that the UEI number used in SAM is the same one used to apply for all other FEMA awards. Payment under any FEMA award is contingent on the recipient's having a current SAM registration.

ii. Help with SAM

The SAM quick start guide for new recipient registration and SAM video tutorial for new applicants are tools created by the General Services Administration (GSA) to assist those registering with SAM. If applicants have questions or concerns about a SAM registration, please contact the Federal Support Desk at https://www.fsd.gov/fsd-gov/home.do or call toll free (866) 606-8220.

6. Register in FEMA GO, Add the Organization to the System, and Establish the AOR:

Applicants must register in FEMA GO and add their organization to the system. The organization's electronic business point of contact (EBiz POC) from the SAM registration may need to be involved in this step. For step-by-step instructions, see https://www.fema.gov/grants/guidance-tools/fema-go/startup.

Note: FEMA GO will support only the most recent major release of the following browsers:

- Google Chrome
- Internet Explorer
- Mozilla Firefox
- Apple Safari
- Microsoft Edge

Users who attempt to use tablet type devices or other browsers may encounter issues with using FEMA GO.

8. Submitting the Application

Applicants will be prompted to submit the standard application information and any program-specific information required as described in Section D. of this NOFO, in the subsection "Content and Form of Application Submission." The Standard Forms (SF) may be accessed in the Forms tab under the https://grants.gov/forms/forms-repository/sf-424-family. Applicants should review these forms before applying to ensure they have all the information required.

After submitting the final application, FEMA GO will provide either an error message or a successfully received transmission in the form of an email sent to the AOR that submitted the application. Applicants using slow internet connections, such as dial-up connections, should be aware that transmission can take some time before FEMA GO receives your application.

For additional application submission requirements, including program-specific requirements, please refer to the subsection titled "Content and Form of Application Submission" under Section D of this NOFO.

9. Timely Receipt Requirements and Proof of Timely Submission

All applications must be completed in FEMA GO by the application deadline. FEMA GO automatically records proof of timely submission and the system generates an electronic date/time stamp when FEMA GO successfully receives the application. The individual with the AOR role that submitted the application will also receive the official date/time stamp and a FEMA GO tracking number in an email serving as proof of their timely submission on the date and time that FEMA GO received the application.

Applicants who experience system-related issues will be addressed until 3:00 PM ET on the date applications are due. No new system-related issues will be addressed after this deadline. Applications not received by the application submission deadline will not be accepted.

10. Content and Form of Application Submission

a. Standard Required Application Forms and Information

Generally, applicants have to submit either the non-construction forms (i.e., SF-424A and SF-424B) or construction forms (i.e., SF-424C and SF-424D), meaning that applicants that only have construction work and do not have any non-construction work need only submit the construction forms (i.e., SF-424C and SF-424D) and not the non-construction forms (i.e., SF-424A and SF-424B), and vice versa. However, applicants who have both construction and non-construction work under this program need to submit both the construction and non-construction forms.

The following forms or information are required to be submitted via FEMA GO. The Standard Forms (SF) are also available at https://grants.gov/forms/forms-repository/sf-424-family

- **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**

b. Program-Specific Required Forms 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).

i. Priority Investments

Cybersecurity

Cybersecurity investments must support the security and functioning of critical 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.

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.

ii. Investment Justification (IJ)

As part of the FY 2024 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 FY 2024 PSGP:

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

iii. 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.

iv. 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. 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 FY 2024 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.

v. 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.

11. Intergovernmental Review

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 (See https://www.archives.gov/federal-register/codification/executive-order/12372.html; Intergovernmental Review (SPOC List) (whitehouse.gov))

12. Funding Restrictions and Allowable Costs

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

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

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

See the Preparedness Grants Manual for information on prohibitions on expending FEMA award funds for covered telecommunications equipment or services.

b. Pre-Award Costs

Pre-award costs are not allowable 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.

c. Management and Administration (M&A) Costs

M&A costs are allowed by the FY 2024 Annual Appropriation (Department of Homeland Security Appropriations Act, 2024, Pub. L. No. 118-47, Title III, "Protection, Preparedness, Response, and Recovery," Section 302). 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 operational costs but are necessary costs incurred in direct support of the federal award or as a consequence of it, such as travel, meeting-related expenses, and salaries of full/part-time staff in direct support of the program. As such, M&A costs can be itemized in financial reports. Other M&A 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, including completing the Civil Rights Evaluation Tool as required by DHS; 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.

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

Indirect (F&A) costs (IDC) mean those costs incurred for a common or joint purpose benefitting more than one cost objective and not readily assignable to the cost objectives specifically benefitted, without effort disproportionate to the results achieved. IDC are allowable by the recipient and subrecipients as described in 2 C.F.R. Part 200, including 2 C.F.R. § 200.414. 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 who do not have 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 the FEMA Point of Contact for further instructions. As it relates to the IDC for subrecipients, a recipient must follow the requirements of 2 C.F.R. §§ 200.332 and 200.414 in approving the IDC rate for subawards. For information on procedures for establishing indirect cost rates, see the Preparedness Grants Manual.

e. Evaluation Costs

Evaluation costs are allowable. See Section H.2 "Program Evaluation" for more details.

f. Other Direct Costs

Costs generally need to fit within one of the categories listed below to be allowable under this program. Applicants who have questions about whether a potential cost is allowable or not under this program should contact their Preparedness Officer.

Specific investments made in support of the funding priorities generally fall into one of the following allowable expense categories:

- Planning;
- Operational Activities;
- Equipment and Capital Projects;
- Training and Awareness Campaigns; and
- Exercises.

The following provides guidance on allowable costs within each of these areas:

i. Planning

Planning activities address the Soft Targets/Crowded Places; Cybersecurity; and Planning Priorities.

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 Area Maritime Security Plan (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.

ii. Operational Activities

Operational Activities address the Soft Targets/Crowded Places Priority.

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.

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.

iii. Equipment and Capital Projects

Equipment and Capital Projects address the Soft Targets/Crowded Places; Cybersecurity; and Equipment/Capital Projects Priorities.

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.

Equipment Acquisition

PSGP funds must comply with FEMA Policy 207-22-0002, Prohibited or Controlled Equipment Under FEMA Awards. 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.

Requirements for Small Unmanned Aircraft Systems

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

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).

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.

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.

Capital (Construction) Projects Guidance

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

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 must also comply with FEMA Policy 207-22-0002, Prohibited or Controlled Equipment Under FEMA Awards and 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.

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;
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 the Port of Houston may submit a hub and spoke project within the Houston/Galveston port area which includes system hardening throughout the organization's facilities in Houston, Port Lavaca, and Corpus Christi. 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 in San Antonio. 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.

iv. Training and Awareness Campaigns

Training and Awareness Campaigns address the Soft Targets/Crowded Places; Cybersecurity; and Training and Awareness Campaign Priorities.

Training

Port areas should assess their training and qualification requirements and coordinate 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**. A listing of courses that are currently approved for PSGP funding is included in the table below.

Some training activities require EHP Review, including exercises, drills or trainings 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 training and exercises. Additional information on training requirements and EHP review can be found online at Environmental & Historic Preservation Grant Preparation Resources | FEMA.gov.

Funding for 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 will be required to explain in the IJ why none of the approved courses referenced in the table below satisfy the identified training need and must submit detailed course information for review and consideration by the local COTP field review team and

the Nation Review Panel.

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 is 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. Refer to Section C of this NOFO for more specific cost share information.

Seminars and workshops are not considered “Training,” however applicants wishing to host seminars 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

Course Number	Course Name
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

Course Number	Course Name
*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**

Course Number	Course Name
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

Course Number	Course Name
*CVBTP	Commercial Vessel Boarding Training Program
*SSATP	Seaport Security Anti-Terrorism Training Program

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.

Exercises

Exercise activities address the Soft Targets/Crowded Places; Cybersecurity; and Exercises Priorities.

Exercises funded under the PSGP typically include Seminars, Workshops, Tabletop, 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, including exercises, drills or trainings 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 training and exercises. Additional information on training requirements and 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. 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. Such costs must be included within the funding allowed for program management personnel expenses, which must not exceed 10% of the total allocation. 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.

vi. Maintenance and Sustainment Costs

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

vii. 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.

viii. 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 conducted under this grant only to the extent that such expenses are 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.

1. **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.

1. **Personnel or contracted costs to:**

- Install, repair, and replace port security equipment acquired with FEMA preparedness grant funds. 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.

1. **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.***

ix. 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.

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.

Grant Managers

Grant management contractors provide support in the day-to-day management of an active grant and their services may be incurred as M&A costs of the award. Additionally, recipients may 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.

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.

g. Reprogramming Award Funds

Reprogramming award funds is permitted under this program only as described in this NOFO. Please also see Section C of this NOFO regarding cost-share requirements, including the implications if the project costs end up being less than what was applied for.

h. Limitations on Funding

As part of the PSGP application process, applicants must complete the approved Investment Justification (IJ) template on Grants.gov and included detailed budget sheets (incorporated into the IJ) provided addressing each initiative being proposed for funding. A single IJ 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 chemical, biological, radiological, nuclear and explosives (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.

i. Unallowable Costs

Projects that do not provide a compelling maritime security benefit or have a direct nexus toward maritime security risk mitigation are not permitted. For example, projects that are primarily for economic or safety benefit (as opposed to having a direct maritime security risk mitigation benefit) are ineligible for PSGP funding. In addition, projects that provide a broad homeland security benefit (e.g., a communication system or fusion center for an entire city, county, state, etc.) as opposed to providing primary benefit to the port are ineligible for PSGP funding since these projects should be eligible for funding through other preparedness grant programs. The following projects and costs are considered ineligible for award consideration:

- ***Grant funds must comply with FEMA Policy 207-22-0002, Prohibited or Controlled Equipment Under FEMA Awards, and may not be used for the purchase of the following equipment: firearms, ammunition, grenade launchers, bayonets, or weaponized aircraft, vessels, or vehicles of any kind with weapons installed;***
- 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 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;
- 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.).

j. Indirect Costs

Indirect costs are allowable under this program. Please refer to the Preparedness Grants Manual for more information.

E. Application Review Information

1. Application Evaluation Criteria

a. Programmatic Criteria

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 2024 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. There are four core PSGP scoring criteria applied in each step of this process:

i. Projects that support development and sustainment of the core capabilities in the Goal.

- Projects are ranked and weighted based on alignment with core capabilities across the five mission areas of the Goal: Prevention, Protection, Mitigation, Response, and Recovery. A composite score is given to each project to determine a Port Area prioritized ranking of all reviewed projects. The following scale shall be used:

0=None; 1=Minimal; 3=Moderate; 9=Significant/Gap Filled

ii. Projects that address priorities outlined in the applicable AMSP, FSP, and/or VSP, as mandated under the MTSA and/or in an applicable PRMP.

- AMSP priorities are the top three Transportation Security Incidents (TSIs) (as defined in 46 U.S.C. § 70101(6)) ranked and correspondingly weighted. Each IJ will be given a score (using the same scale as the National Priorities module) based on how well it addresses one or more TSIs within the context of the five mission areas of the Goal. The following scale shall be used:

0=None; 1=Minimal; 3=Moderate; 9=Significant/Gap Filled

- COTPs may require proposed projects to be socialized with the COTP/Area Maritime Security Committee (AMSC) prior to applying. Applicants are encouraged to coordinate with the COTP/AMSC routinely to ensure their projects align with Port Area priorities.

iii. Projects that are eligible and feasible, based on the period of performance. In addition, a recipient's past performance demonstrating competent stewardship of Federal funds may influence funding decisions.

- IJs should justify the scope, breadth, and cost of a project, as well as a timeline for completing the project as required within this NOFO. Projects failing to demonstrate these minimum funding considerations may be denied funding. The following scale shall be used:

0=No Funding Recommended; 1=Funding Recommended

b. Financial Integrity Criteria

Prior to making a federal award, FEMA is required by 31 U.S.C. § 3354, as enacted by the Payment Integrity Information Act of 2019, Pub. L. No. 116-117 (2020); 41 U.S.C. § 2313; and 2 C.F.R. § 200.206 to review information available through any Office of Management and Budget (OMB)-designated repositories of governmentwide eligibility qualification or financial integrity information, including whether SAM.gov identifies the applicant as being excluded from receiving federal awards or is flagged for any integrity record submission. FEMA may also pose additional questions to the applicant to aid in conducting the pre-award risk review. Therefore, application evaluation criteria may include the following risk-based considerations of the applicant:

i. Financial stability.

ii. Quality of management systems and ability to meet management standards.

iii. History of performance in managing federal award.

iv. Reports and findings from audits.

v. Ability to effectively implement statutory, regulatory, or other requirements.

c. Supplemental Financial Integrity Criteria and Review

Prior to making a federal award where the anticipated total federal share will be greater than the simplified acquisition threshold, currently $250,000:

i. FEMA is required by 41 U.S.C. § 2313 and 2 C.F.R. § 200.206(a)(2) to review and consider any information about the applicant, including information on the applicant's immediate and highest-level owner, subsidiaries, and predecessors, if applicable, that is in the designated integrity and performance system accessible through the System for Award Management (SAM), which is currently the Federal Awardee Performance and Integrity Information System (FAPIIS).

ii. An applicant, at its option, may review information in FAPIIS and comment on any information about itself that a federal awarding agency previously entered.

iii. FEMA will consider any comments by the applicant, in addition to the other information in FAPIIS, in making a judgment about the applicant's integrity, business ethics, and record of performance under federal awards when completing the review of risk posed by applicants as described in 2 C.F.R. § 200.206.

2. Review and Selection Process

Following the USCG COTP-led Field 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 two National Priorities (enhancing cybersecurity or enhancing the protection of soft targets/crowded places) 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 the national priority.

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 FY 2024 PSGP will take into consideration the ability of the revised project to address the National Priorities 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.

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. The analysis includes threats from domestic violent extremists, international terrorist groups, and individuals inspired by terrorists abroad. 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.

F. Federal Award Administration Information

1. Notice of Award

Before accepting the award, the AOR and recipient should carefully read the award package. The award package includes the instructions on administering the grant award and the terms and conditions associated with responsibilities under federal awards. **Recipients must accept all conditions in this NOFO and the Preparedness Grants Manual as well as any specific terms and conditions in**

the Notice of Award to receive an award under this program.

See the Preparedness Grants Manual for information on Notice of Award.

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 email notification of the award package will be sent through FEMA's grant application system to the AOR that submitted the application.

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

Funds will remain on hold until the recipient accepts the award through the FEMA GO system 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.

2. Administrative and National Policy Requirements

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

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

- Environmental Planning and Historic Preservation (EHP) Compliance
- FirstNet
- National Incident Management System (NIMS) Implementation
- SAFECOM

a. DHS Standard Terms and Conditions

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

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

b. Ensuring the Protection of Civil Rights

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

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

The DHS Standard Terms and Conditions include a fuller list of the civil rights provisions that apply to recipients. These terms and conditions can be found in the DHS Standard Terms and Conditions. Additional information on civil rights provisions is available at https://www.fema.gov/about/offices/equal-rights/civil-rights.

Monitoring and oversight requirements in connection with recipient compliance with federal civil rights laws are also authorized pursuant to 44 C.F.R. Part 7 or other applicable regulations.

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

c. Environmental Planning and Historic Preservation (EHP) Compliance

See the Preparedness Grants Manual for information on EHP compliance.

d. National Incident Management System (NIMS) Implementation

See the Preparedness Grants Manual for information about NIMS implementation.

e. Mandatory Disclosures

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

Please note applicants and recipients may report issues of fraud, waste, abuse, and mismanagement, or other criminal or noncriminal misconduct 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.

3. Reporting

Recipients are required to submit various financial and programmatic reports as a condition of award acceptance. Future awards and funds drawdown may be withheld if these reports are delinquent.

See the Preparedness Grants Manual for information on reporting requirements.

4. Monitoring and Oversight

The regulation at 2 C.F.R. § 200.337 provides DHS and any of its authorized representatives with the right of access to any documents, papers, or other records of the recipient [and any subrecipients] that are pertinent to a federal award in order to make audits, examinations, excerpts, and transcripts. The right also includes timely and reasonable access to the recipient's or subrecipient's personnel for the purpose of interview and discussion related to such documents. Pursuant to this right and per 2 C.F.R. § 200.329, DHS may conduct desk reviews and make site visits to review project accomplishments and management control

systems to evaluate project accomplishments and to provide any required technical assistance. During site visits, DHS may review a recipient's or subrecipient's files pertinent to the federal award and interview and/or discuss these files with the recipient's or subrecipient's personnel. Recipients and subrecipients must respond in a timely and accurate manner to DHS requests for information relating to a federal award.

See the Preparedness Grants Manual for information on monitoring and oversight.

G. DHS Awarding Agency Contact Information

1. Contact and Resource Information

a. Program Office Contact

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.

b. FEMA Grants News

FEMA Grants News is a non-emergency comprehensive management and information resource developed by FEMA for grants stakeholders. 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. When necessary, recipients will be directed to a federal point of contact who can answer specific programmatic questions or concerns. FEMA Grants News can be reached by e-mail at fema-grants-news@fema.dhs.gov OR by phone at (800) 368-6498, Monday through Friday, 9:00 AM – 5:00 PM ET.

c. Grant Programs Directorate (GPD) Award Administration Division

GPD's Award Administration Division (AAD) provides support regarding financial matters and budgetary technical assistance. Additional guidance and information can be obtained by contacting the AAD's Help Desk via e-mail at ASK-GMD@fema.dhs.gov.

d. Equal Rights

The FEMA Office of Equal Rights (OER) is responsible for compliance with and enforcement of federal civil rights obligations in connection with programs and services conducted by FEMA and recipients of FEMA financial assistance. All inquiries and communications about federal civil rights compliance for FEMA grants under this NOFO should be sent to FEMA-CivilRightsOffice@fema.dhs.gov .

e. Environmental Planning and Historic Preservation

GPD's EHP Team provides guidance and information about the EHP review process to recipients and subrecipients. All inquiries and communications about GPD projects under this NOFO or the EHP review process, including the submittal of EHP review materials, should be sent to gpdehpinfo@fema.dhs.gov.

2. Systems Information

a. FEMA GO

For technical assistance with the FEMA GO system, please contact the FEMA GO Helpdesk at femago@fema.dhs.gov or (877) 585-3242, Monday through Friday, 9:00 AM – 6:00 PM ET.

H. Additional Information

GPD has developed the Preparedness Grants Manual to guide applicants and recipients of grant funding on how to manage their grants and other resources. Recipients seeking guidance on policies and procedures for managing

preparedness grants should reference the Preparedness Grants Manual for further information. Examples of information contained in the Preparedness Grants Manual include:

- Actions to Address Noncompliance
- Audits
- Case Studies and Use of Grant-Funded Resources During Real-World Incident Operations
- Community Lifelines
- Conflicts of Interest in the Administration of Federal Awards and Subawards
- Disability Integration
- National Incident Management System
- Payment Information
- Period of Performance Extensions
- Procurement Integrity
- Record Retention
- Termination Provisions
- Whole Community Preparedness
- ·Financial Assistance Programs for Infrastructure
- Report issues of Fraud, Waste, and Abuse
- Hazard Resistant Building Codes
- Other Post-Award Requirements

1. Termination Provisions

FEMA may terminate a federal award in whole or in part for one of the following reasons. FEMA and the recipient must still comply with closeout requirements at 2 C.F.R. §§ 200.344-200.345 even if an award is terminated in whole or in part. To the extent that subawards are permitted under this NOFO, pass-through entities should refer to 2 C.F.R. § 200.340 for additional information on termination regarding subawards. Note that all information in this Section H.1 “Termination Provisions” is repeated in the Preparedness Grants Manual.

a. Noncompliance

If a recipient fails to comply with the terms and conditions of a federal award, FEMA may terminate the award in whole or in part. If the noncompliance can be

corrected, FEMA may first attempt to direct the recipient to correct the noncompliance. This may take the form of a Compliance Notification. If the noncompliance cannot be corrected or the recipient is non-responsive, FEMA may proceed with a Remedy Notification, which could impose a remedy for noncompliance per 2 C.F.R. § 200.339, including termination. Any action to terminate based on noncompliance will follow the requirements of 2 C.F.R. §§ 200.341-200.342 as well as the requirement of 2 C.F.R. § 200.340(c) to report in FAPIIS the recipient's material failure to comply with the award terms and conditions. See also the section on Actions to Address Noncompliance in the Preparedness Grants Manual

b. With the Consent of the Recipient

FEMA may also terminate an award in whole or in part with the consent of the recipient, in which case the parties must agree upon the termination conditions, including the effective date, and in the case of partial termination, the portion to be terminated.

c. Notification by the Recipient

The recipient may terminate the award, in whole or in part, by sending written notification to FEMA setting forth the reasons for such termination, the effective date, and in the case of partial termination, the portion to be terminated. In the case of partial termination, FEMA may determine that a partially terminated award will not accomplish the purpose of the federal award, so FEMA may terminate the award in its entirety. If that occurs, FEMA will follow the requirements of 2 C.F.R. §§ 200.341-200.342 in deciding to fully terminate the award.

2. Program Evaluation

Federal agencies are required to structure NOFOs that incorporate program evaluation activities from the outset of their program design and implementation to meaningfully document and measure their progress towards meeting agency priority goal(s) and program outcomes.

OMB Memorandum M-21-27, Evidence-Based Policymaking: Learning Agendas and Annual Evaluation Plans, implementing Title I of the Foundations for Evidence-Based Policymaking Act of 2018, Pub. L. No. 115-435 (2019) (Evidence Act), urges federal awarding agencies to use program evaluation as a critical tool to learn, improve equitable 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).

As such, recipients and subrecipients are required to participate in a DHS-, Component, or Program Office-led evaluation if selected, which may be carried out by a third-party on behalf of the DHS, its component agencies, or the Program Office. Such an evaluation may involve information collections including but not limited to surveys, interviews, or discussions with individuals who benefit from the federal award program operating personnel, and award recipients, as specified in a DHS-, component agency-, or Program Office-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). Recipients and subrecipients are also encouraged, but not required, to participate in any additional evaluations after the period of performance ends, although any costs incurred to participate in such evaluations are not allowable and may not be charged to the federal award.

3. Financial Assistance Programs for Infrastructure

a. Build America, Buy America Act

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

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

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

For FEMA's official policy on BABAA, please see FEMA Policy 207-22-0001: Buy America Preference in FEMA Financial Assistance Programs for Infrastructure available at https://www.fema.gov/sites/default/files/documents/fema_build-america-buy-america-act-policy.pdf To see whether a particular FEMA federal financial assistance program is considered an infrastructure program and thus required to include a Buy America preference, please see Programs and Definitions: Build America, Buy America Act | FEMA.gov. and https://www.fema.gov/sites/default/files/documents/fema_build-america-buy-america-act-policy.pdf

b. Waivers

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

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

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

more than 25%.

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

c. Definitions

For BABAA specific definitions, please refer to the FEMA Buy America website at: "Programs and Definitions: Build America, Buy America Act | FEMA.gov."

Please refer to the applicable DHS Standard Terms & Conditions for the BABAA specific term applicable to all FEMA financial assistance awards for infrastructure.

4. Report issues of fraud, waste, abuse

Please note, when applying to this notice of funding opportunity and when administering the grant, applicants may report issues of fraud, waste, abuse, and mismanagement, or other criminal or noncriminal misconduct 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.

5. Appendices

- PSGP Sample Memorandum of Understanding/Agreement (MOU/MOA)
  The sample MOU/MOA below 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.

Memorandum of [Understanding / Agreement]

Between [provider of layered security] and [recipient of layered security]

Regarding [provider of layered security's] Use of Port Security Grant Program Funds

1. **PARTIES**. The parties to this Agreement are the [Provider of Layered Security] and the [Recipient of security service].

2. **AUTHORITY**. This Agreement is authorized under the provisions of [applicable Area Maritime Security Committee (AMSC) authorities and/or other authorities].
3. **PURPOSE**. The purpose of this Agreement is to set forth terms by which [Provider of security service] shall expend Port Security Grant Program project funding in providing security service to [Recipient of security service]. Under requested PSGP grant, the [Provider of security service] must provide layered security to [Recipient of security service] consistent with the approach described in an approved grant application.

4. **RESPONSIBILITIES**: The security roles and responsibilities of each party are understood as follows:
   (1) [Recipient of security service]

   Roles and responsibilities in providing its own security at each MARSEC level

   (2) [Provider of security service]

   [-An acknowledgement by the facility that the applicant is part of their facility security plan.]

   [-The nature of the security that the applicant agrees to supply to the regulated facility (waterside surveillance, increased screening, etc.).]

   [-Roles and responsibilities in providing security to [Recipient of security service] at each MARSEC level.]

5. **POINTS OF CONTACT**. [Identify the POCs for all applicable organizations under the Agreement; including addresses and phone numbers (fax number, e-mail, or internet addresses can also be included).]
6. **OTHER PROVISIONS**. Nothing in this Agreement is intended to conflict with current laws or regulations of [applicable State] or [applicable local Government]. If a term of this agreement is inconsistent with such authority, then that term shall be invalid, but the remaining terms and conditions of this agreement shall remain in full force and effect.

7. **EFFECTIVE DATE**. The terms of this agreement will become effective on [EFFECTIVE DATE].
8. **MODIFICATION**. This agreement may be modified upon the mutual written consent of the parties.
9. **TERMINATION**. The terms of this agreement, as modified with the consent of both parties, will remain in effect until the grant end dates for an approved grant. Party upon [NUMBER] day's written notice to the other party may terminate this agreement.

APPROVED BY: Organization and Title

Footnotes

1. Homeland Security Act of 2002: Report Together with Minority and Dissenting Views 222, Select Committee on Homeland Security: 107th Congress, U.S. House of Representatives (2002) (H. Rpt. 107-609).
2. Strategic Intelligence Assessment and Data on Domestic Terrorism, Federal Bureau of Investigation and Department of Homeland Security, June 2023.