Grant Executive Summary

Port Security Grant Program

Funds available

$90 Million

Apply by June 24, 2024

Grant highlights

The Port Security Grant Program (PSGP) provides funding to port authorities, facility operators, and State and local agencies for activities associated with implementing Area Maritime Security Plans (AMSPs), facility security plans, and other port- wide risk management efforts. The PSGP is focused on supporting increased port-wide maritime security risk management; enhancing maritime domain awareness; supporting maritime security training and exercises; and maintaining or reestablishing maritime security mitigation protocols that support port recovery and resiliency capabilities. PSGP investments must address U.S. Coast Guard (USCG) and Area Maritime Security Committee (AMSC) identified vulnerabilities in port security.

There is a cash or in-kind match requirement of at least 25 percent of the total project cost for each proposed project (50% for private, for-profit award recipients). Construction projects require a cash match. There is a process for requesting waivers.

The performance period is three years.

Who can apply

Eligible applicants must be subject to an Area Maritime Transportation Security Plan (AMSP) and include, but are not limited to: port authorities, facility operators, and state and local 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. This includes private, for-profit entities.

Only one application per eligible entity within each port area is permitted. No single application should propose projects intended to be implemented in multiple Port Areas. Separate applications must be submitted to fund projects in each Port Area.

Funding priorities and allowable costs

FEMA has identified enhancing cybersecurity and enhancing the protection of soft targets/crowded places as the areas of greatest concern and, therefore, projects that sufficiently address these national priorities will have their final review scores increased by a multiplier of 20 percent.

Second-tier priorities addressing enduring security needs include: effective planning; training and awareness campaigns; equipment and capital projects (e.g., physical security enhancement projects); and; exercises.

Among allowable equipment acquisition costs are:

- 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)
- Maritime security risk mitigation interoperable communications equipment
- Terrorism incident prevention and response equipment for maritime security risk mitigation
- Physical security enhancement equipment at maritime facilities (e.g., security cameras, access controls)
- 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.

A comprehensive listing of all allowable equipment categories may be found on Authorized Equipment List.

Emergency Communications: Grantees using PSGP funds to support emergency communications activities must comply with the most recent SAFECOM Guidance on Emergency Communication Grants.

Maintenance and Sustainment: Maintenance contracts, warranties, repairs, upgrades and user fees are allowable, but the coverage period of stand-alone contracts or extensions to an existing one must not exceed the performance period of the grant. The only exception is if the maintenance contract or warranty is purchased at the same time and under the same grant award as the original purchase of the system or equipment, then coverage may exceed the performance period.

Construction: Construction and renovation projects are allowable under the PSGP provided they address a specific vulnerability or need identified in AMSP or otherwise support the maintenance/sustainment of capabilities and equipment acquired through PSGP funding. Such projects include Maritime Command and Control Centers and Port Security Emergency Communications Centers.

Cybersecurity: Applicants are encouraged to propose projects to aid in implementation of all or part of the Framework for Improving Critical Infrastructure Cybersecurity developed by the National Institute of Standards and Technology (NIST). Although vulnerability assessments are generally not funded under the PSGP, the guidance specifically allows them to be funded as contracted costs given that cybersecurity is a relatively new and evolving program priority.

Prohibitions on Expending Grant Funds for Certain Telecommunications and Video Surveillance Equipment or Services: Effective August 13, 2020, DHS/FEMA grant recipients and subrecipients may not use grant funds for certain telecommunication and video surveillance equipment or services produced by certain Chinese companies identified by Congress in the National Defense Authorization Act for FY 2019. For more information see pp. 36 of the PSGP NOFO and pp. 13-14 of the FEMA Preparedness Grants Manual. Grant funds may be used to procure replacement equipment and services impacted by this prohibition, provided the costs are otherwise consistent with program requirements.

Buy America Requirements for Infrastructure Projects: Grant recipients planning to use award funds for infrastructure projects must comply with the Build America, Buy America Act unless they obtain a waiver from FEMA. For more information see pp. 78-80 of the PSGP NOFO and consult your legal department.

Application deadline

Eligible applicants must submit completed applications by **June 24, 2024, 5 pm ET**. Applicants are encouraged to submit their initial application in Grants.gov at least seven days before this deadline in order to have enough time to submit the final application via FEMA GO.

Motorola Solutions offers a proven basis for your application

We offer a wide range of solutions to improve transportation infrastructure security activities and help create safer cities and thriving communities, including:

- **Cybersecurity Services** — Secure and protect your critical infrastructure by always knowing your cyber security risk posture. Motorola Solutions Cybersecurity Professional Services offer a comprehensive assessment of an agency's attack surface profile by applying the best practices of the NIST Cybersecurity Framework. Detailed remediation recommendations can then guide the agency to an appropriate solution, such as Security Monitoring or Security Update Services.
- **Land Mobile Radio Communications** — Communications in urban areas can be enabled or augmented with Project 25-compliant, mission-critical-grade infrastructure to provide expanded coverage, reliability, capacity and security for emergency responders. Mobile and portable radios are designed specifically for the needs of first responders and provide interoperability on Project 25 networks, legacy Smartnet/Smartzone or conventional networks, and across multiple frequency bands for unparalleled interoperability through a single device. Connectivity between disparate or neighboring standalone communications networks can be achieved via IP-based gateways, consolidated P25 networks or hosted cloud solutions.
- **Body-Worn and In-Car Cameras** — Motorola Solutions provides mobile video solutions for law enforcement, supplying in-car video systems and bodyworn cameras along with evidence management software to approximately one-third of all law enforcement agencies in the United States and Canada.
- **Digital Evidence Management System** — Combine all of your digital evidence and management workflows with CommandCentral Evidence. Preserve evidence confidently and easily manage large quantities of content by storing all of it together in a single, secure place. Leverage smart data correlation from across systems to automatically organize content so that people and cases keep moving.
- **Voice & Computer-Aided Dispatch Solutions** — Computer-aided dispatch solutions suite enhances incident management by automating workflows and data retrieval from the PSAP to the field. Coordinate your team with a seamless flow of information from the moment a call comes in, to when responders arrive - enabling the quickest, safest response.
- **Command Center Software** — Our command center software features end-to-end solutions that provide users with a unified, intuitive experience and intelligent capabilities designed specifically for the needs of public safety and schools. It includes integrated software solutions from call to case closure, including emergency call management, dispatch, real-time intelligence, field response & reporting and records & evidence management solutions.
- **WAVE PTX Broadband Push-to-Talk Communications** — Create simple, secure, and reliable Push-To-Talk communications between radio and devices outside the radio system, such as smartphones, tablets, and laptops.
- **Video Security & Access Control** — Motorola Solutions offers fixed video, access control and software solutions to help you find, analyze and share information so you can respond to events with speed and decisiveness to keep your people and property safe. Our fixed video security systems include Avigilon, IndigoVision, Ava, and Pelco. Our access control systems and security include Openpath.
- **Mass Notification and Critical Incident Management** — Enable organizations and communities to quickly and effectively send emergency alerts and share critical information to their entire audience through multiple channels including, SMS, email, voice, desktop, IPAWS, push notifications, social media and more. Supercharge notifications with tactical incident management for both planned and unplanned events to make sure every task is completed using automated communications, dynamic task management, event-specific resources and extensive reporting.

How to apply

The initial submission to determine eligibility should be made through www.grants.gov. The full application package, including investment justifications, detailed budgets, and associated MOUs/MOAs if required, should be submitted via the FEMA GO Portal at https://go.fema.gov.

Applicants should refer to the FEMA Preparedness Grants Manual for more information on submitting an application.

The Investment Justification template is located at the grants.gov entry for this program. For more information on emergency communications guidance, please review page 41-42 of the PSGP NOFO.

FAQs may be found here.

Contact your SAA for specific details and their application timelines. Find a list of SAA contacts here.

Applicants should take note of the application evaluation criteria on pp. 65-70 of the PSGP NOFO and Question 9 of the FAQs on what makes a strong Investment Justification.

We can help you

The grant application process can be challenging to navigate. To help you, Motorola Solutions has partnered with the grant experts at PoliceGrantsHelp.com. Their team of funding experts can help your agency identify which areas you are eligible for, answer questions and offer insights on how to write an effective application.

Additional information and resources can be found on our website: www.motorolasolutions.com/govgrants.

MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A.