



PORT SECURITY GRANT PROGRAM

FUNDS AVAILABLE

\$100 MILLION

APPLY BY JUNE 20, 2018

GRANT HIGHLIGHTS

The Port Security Grant Program (PSGP) is a competitive program that provides funds for transportation infrastructure security activities to implement Area Maritime Transportation Security Plans and facility security plans among port authorities, facility operators, and state and local government agencies required to provide port security services.

The purpose of the PSGP is to improve port-wide maritime security risk management; enhance maritime domain awareness; support maritime security training and exercises; and maintain or reestablish maritime security mitigation protocols that support port recovery and resiliency capabilities.

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.

Only one application per eligible entity within each port area is permitted. Applicants with projects in multiple port areas may submit only one application per port area based on the implementation location of the proposed projects. Eligibility does not guarantee grant funding.

FUNDING PRIORITIES AND ALLOWABLE COSTS

In addition to the two overarching program priorities of risk-informed funding and regional security cooperation, the following six priorities have been identified as selection criteria for all PSGP applicants:

- Marine Domain Awareness (MDA)
- Port Resiliency / Continuity of Operations
- Training and Exercises
- Cybersecurity Capabilities
- Improvised Explosive Device (IED) and Chemical, Biological, Radiological, Nuclear and Explosives (CBRNE) capabilities
- Physical Security

Allowable uses of PSGP funds include equipment that will be used in direct support of maritime security risk mitigation and that supports developing or sustaining one or more core capabilities such as:

- 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
- Equipment in support of resiliency such as interoperable communications, intrusion prevention/detection, physical security enhancements, and software and equipment needed to support essential functions during a continuity situation

A comprehensive listing of all allowable equipment categories may be found on [Authorized Equipment List](#).

Emergency Communications: Grantees and sub-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 program priority.

APPLICATION DEADLINE

Eligible applicants must submit completed applications by June 20, 2018. Applicants are encouraged to submit their initial application in Grants.gov at least seven days before this deadline.

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:

- **Interoperable Communications** — The need for improved coordination with port partners, local and regional public safety agencies, particularly during emergency conditions, is critical to prevent, protect, respond to and recover from attacks and natural disasters. WAVE Work Group Communications create simple, secure, and reliable Push-To-Talk communications between radios and devices outside the radio system, such as smartphones, tablets, and laptops.
- **Intelligence Led Public Safety (ILPS) Solutions** — Exceed new expectations for safety and efficiency by transforming big data into actionable intelligence with CommandCentral. Analyze more data, faster, to help you uncover new insights. Then deliver this information, in the right context to improve situational awareness across your operation.
- **CommandCentral Aware** — As you invest in technologies to more effectively aid those in the field, various disconnected systems overloading your agency with information may be making it difficult to provide true impact. Support the field with more meaningful, real-time intelligence by extracting deeper insights from integrated voice, video and data.

- **CommandCentral Inform** — A single piece of information can often make the difference in making the most intelligence-led decisions. Yet, ensuring everyone has access to the information and can quickly understand its relevance can be difficult. Keep everyone informed and in sync with a map-based common operating picture available anywhere they are, on any device.
- **CommandCentral Analytics** — In an increasingly scrutinized world, the more agency initiatives are based on facts and results can be quantified, the better. Unfortunately, the crime analysis required for making sense of your data is oftentimes a manual, time-consuming process. Easily turn strategic planning into measured tactical action by automating the most advanced crime data analysis.
- **Cybersecurity Professional Services** — Motorola provides network security monitoring, pre-tested software security updates, risk assessments and other security services to protect against cyber threats to mission-critical radio networks and real-time information sources, particularly as such information is shared across agencies.
- **Video Surveillance** — A recent Motorola Solutions acquisition, Avigilon, offers advanced video surveillance and analytics solutions, from high-definition cameras to artificial intelligence and machine learning software.

HOW TO APPLY

Eligible applicants will apply directly to FEMA for funding under this program. All applicants will submit their PSGP grant application, investment justifications and associated MOUs/MOAs, if required through <https://portal.fema.gov> prior to the application deadline date and time. 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 Non-Disaster Grants system at <https://portal.fema.gov>.

Find [specific grant guidance](#) for the PSGP.

Applicants should use the Sample Budget Detail Worksheet found on pages 51-54 of the PSGP NOFO and the Investment Justification template found on www.grants.gov.

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.

