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" as the area of greatest concern and, therefore, projects that sufficiently address the Cybersecurity National Priority will have their final review scores increased by a multiplier of 20 percent.

Second-tier priorities addressing enduring security needs include: enhancing the protection of soft targets/crowded places (e.g., security cameras, access controls); addressing emerging threats (e.g., transnational criminal organizations, weapons of mass destruction, unmanned aerial systems, etc.); 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 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 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 pages 21-22 of the PSGP NOFO and page 19 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.

APPLICATION DEADLINE

Eligible applicants must submit completed applications by **May 14, 2021, 5 pm ET**. 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 Two-Way Radios and Networks** — Enable or augment communications 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.
- **Public Safety LTE** — The LEX L11 Mission Critical LTE Device is designed with first responders in mind. Every feature and function is thoughtfully considered, from the rugged, easy to operate design to the always loud and clear audio to the advanced end-to-end secure mobile platform and the enhanced accessibility provided by a suite of accessories. Chiefs who may not be on the front lines can use the LEX L11 to stay in touch using instant push-to-talk. Rugged and durable yet streamlined and slim, you can count on the LEX L11 to perform when it's needed most.
- **CommandCentral Software** — CommandCentral is an end-to-end software suite that provides users with a unified, intuitive experience and intelligent capabilities designed specifically for the needs of public safety and schools. It includes integrated call handling, command and control and records and evidence solutions.
- **Dispatch Solutions** — Computer-aided dispatch solutions enhance 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.
- **WAVE PTX: Broadband Push-to-Talk** — Create simple, secure, and reliable Push-To-Talk communications between radios and devices outside the radio system, such as smartphones, tablets, and laptops.
- **Radio Alert** — Instantly receive video analytic and access control alerts directly to your two-way radio via text message and text-to-voice alert including license plate recognition, breaches, loitering and presence detection.
- **Video Security & Analytics** — Avigilon, a Motorola Solutions company, offers advanced video security and analytics solutions, from high-definition cameras to artificial intelligence and machine learning software.
- **Access Control** — The Avigilon access control platform scales to the changing needs of your business, with flexible solutions that range from our Access Control Manager (ACM) enterprise system to our entry-level ACM Embedded Controller™ system.
- **Body-Worn and In-Car Cameras** — WatchGuard, part of Motorola Solutions, provides mobile video solutions for law enforcement, supplying in-car video systems and body-worn cameras along with evidence management software to approximately one-third of all law enforcement agencies in the United States and Canada.
- **License Plate Recognition (LPR)** — Vigilant Solutions, part of Motorola Solutions, offers an LPR platform with powerful analytics that help complete the investigative triangle of person, plate and location. All of the data and analytics received from LPR detections across the nation are stored in Vigilant's Cloud, LEARN, to help law enforcement develop leads and close cases.
- **CBRS Private LTE (NITRO)** — Private broadband to share multimedia and data across facilities using a private data network managed via a cloud-based portal.
- **Managed Services —** Build an emergency management program to monitor and resolve threats to system performance so your teams can do their job effectively and you can have peace of mind.

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 Non-Disaster Grants system at https://portal.fema.gov.

Applicants should refer to the FEMA Preparedness Grants Manual for more information on submitting an application. This Manual includes an Investment Justification template as well as Supplemental Emergency Communications Guidance.

Other program documents, including the PSGP Notice of Funding Opportunity and FAQs, may be found here. Applicants should take note of the application evaluation criteria on pp. 26-28 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 W. Monroe Street Chicago, IL 60661 U.S.A. 800-367-2346 **MotorolaSolutions.com**

MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. © 2021 Motorola Solutions, Inc. All rights reserved.