



## TRANSIT SECURITY GRANT PROGRAM

FUNDS AVAILABLE

# \$93 MILLION

APPLY BY MAY 18, 2023

### GRANT HIGHLIGHTS

The Transit Security Grant Program (TSGP) provides funds to eligible public transportation systems (which include intra-city bus, ferries, and all forms of passenger rail) to protect critical transportation infrastructure and the travelling public from terrorism, and to increase transportation infrastructure resilience.

A cost share/match is not required under this program. The performance period is three years (four years for capital infrastructure projects).

### WHO CAN APPLY

Agencies eligible for the TSGP are determined based upon daily ridership and transit systems that serve historically eligible Urban Areas Security Initiative (UASI) jurisdictions.

In order to be eligible, transit agencies must have developed and/or updated their security plan within the last three years. Entities providing transit security (e.g. city/county police department, transit agency's own police department) for a public transportation agency must approve the security plan. Each public transportation agency receiving funds through this program must also participate in a Regional Transit Security Working Group.

A list of eligible transit agencies may be found on pp. 9-12 of the [TSGP Notice of Funding Opportunity](#). Eligibility does not guarantee grant funding.

### 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 receive a 20% increase to their scores.

Second-tier priorities addressing enduring security needs include: effective planning; training and awareness campaigns; equipment and capital projects; and exercises.

Priority projects under the Equipment and Capital projects category include Top Transit Asset List risk remediation and protection of other high-risk, high consequence areas or systems that have been identified through system-wide risk assessments. These include:

- Projects related to physical security enhancements at rail and bus stations in historically eligible UASI jurisdictions including security cameras, security screening equipment for people and baggage, and access control.
- Projects related to cybersecurity of access control, sensors, security cameras, badge/ID readers, ICS/SCADA systems, process monitors and controls, etc. or passenger/vehicle/cargo security screening equipment support. Cybersecurity assessments are allowable.

A comprehensive listing of all allowable equipment categories may be found on [Authorized Equipment List](#). The categories of equipment for which TSGP funds may be used include, among others, Interoperable Communications Equipment, Terrorism Incident Prevention Equipment, and Physical Security Enhancement Equipment.

**Emergency Communications:** Grantees and sub-grantees using TSGP funds to support emergency communications activities must comply with the most recent [SAFECOM Guidance for 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.

**Communications Towers:** Construction of communications towers is permitted subject to compliance with all applicable Environmental Planning and Historical Preservation requirements.

**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).

**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. 21-23 of the TSGP NOFO and pp.17-18 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 18, 2023, 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 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.
- **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.
- **License Plate Recognition (LPR)** — 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.
- **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.
- **School Safety & Protection** — Comprehensive and customizable mobile solutions for school safety, including emergency notification functionality, a one-click panic button, anonymous tip reporting, 9-1-1 integration, drill management and more to enable quick and efficient emergency response and coordination.
- **CBRS Private LTE (NITRO)** — Nitro from Motorola Solutions is a fixed private broadband wireless solution designed for critical infrastructure and enterprise. Nitro enables fast and secure transmission of voice and data to increase operational efficiencies of businesses and enterprises. Being a private closed network, Nitro system owners have complete control over coverage, access and usage. In the US, Nitro systems operate predominantly in the CBRS (3.5GHz) frequency band and are compatible with FCC certified user devices from many manufacturers.

## HOW TO APPLY

The initial submission to determine eligibility should be made through [www.grants.gov](http://www.grants.gov). The full application package, including investment justifications (IJ), detailed budgets and associated Memoranda of Understanding (MOU)/Memoranda of Agreement (MOA), should be submitted via the Non-Disaster Grants system at <https://portal.fema.gov>.

Agencies may submit IJs for projects related to law enforcement providers that are not part of the public transportation agency. Law enforcement providers may only submit projects that support a transit system's operational security capability and capacity.

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 FAQs, may be found [here](#). Applicants should take note of the application evaluation criteria on pp. 27-30 of the TSGP NOFO and Question 8 of the FAQs on what makes a strong IJ.

## 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](http://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](http://www.motorolasolutions.com/govgrants).

