FUNDS AVAILABLE
$185 MILLION

Apply by November 15th, 2022
State and Local Cybersecurity Grant Program

GRANT HIGHLIGHTS

The State and Local Cybersecurity Grant Program (SLCGP) addresses cybersecurity risks and threats to information systems owned or operated by, or on behalf of, state, local and territorial governments. The program, which is being jointly managed by the Cybersecurity and Infrastructure Agency (CISA) and Federal Emergency Management Agency (FEMA), enables targeted cybersecurity investments aimed at improving the security of critical infrastructure and resilience of the services that state, local, and territorial governments provide to their communities. The SLCGP was created as part of the Infrastructure Investment and Jobs Act, which provides a total of $1 billion in dedicated funding for state and local cybersecurity over four years.

WHO CAN APPLY

All 56 states, territories and commonwealths are eligible to apply for SLCGP funds. The designated State Administrative Agency (SAA) for each state and territory is the only entity eligible to apply for SLCGP funding. A list of the funding allocation for each state and territory may be found on pp. 7-9 of the SLCGP Notice of Funding Opportunity (SLCGP NOFO). The SAA must pass-through at least 80% of the funds awarded under the SLCGP to local units of government, including at least 25% of funds to rural entities, within 45 calendar days of receipt of the funds. An SAA may partner with one or more other SAAs to form a multi-entity group.

FUNDING OBJECTIVES AND ALLOWABLE COSTS

The overarching goal of the SLCGP program is to assist state and local governments in managing and reducing systemic cyber risks. To accomplish this, CISA has established four discrete, but interrelated objectives:

- Governance and Planning: Develop and establish appropriate governance structures, as well as plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.
- Assessment and Evaluation: Identify areas for improvement in SLTT cybersecurity posture based on continuous testing, evaluation, and structured assessments.
- Mitigation: Implement security protections commensurate with risk (outcomes of Objectives 1 and 2), using the best practices as described in element 5 of the required 16 elements of the cybersecurity plans and those further listed in the NOFO.
- Workforce Development: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with their responsibilities as suggested in the National Initiative for Cybersecurity Education.

In the first year, the focus is on establishing a strong foundation on which to build a sustainable cybersecurity program. Initial priorities include the following, all of which are statutory conditions for receiving a grant:

- Establish a Cybersecurity Planning Committee that can lead entity-wide efforts.
- Develop a Cybersecurity Plan that addresses the entire jurisdiction and incorporates cybersecurity best practices.
- Conduct assessments and evaluations to identify gaps that can be mitigated by individual projects throughout the life of the grant program.

Allowable cost categories include planning, equipment, exercises, management and administration, organization, and training. Funding used for equipment must be consistent with FEMA's Authorized Equipment List.

MOTOROLA SOLUTIONS

HOW AND WHEN TO APPLY

The SAA must submit the full application by **November 15, 2022, 5 pm ET.** Applicants are encouraged to submit their initial application in Grants.gov at least seven days before this deadline.

The full application package should be submitted via FEMA's Non-Disaster Grants System.

ADDITIONAL PROGRAM DETAILS

Eligible entities must submit Cybersecurity Plans for review and approval as part of their grant application. These Plans are meant to guide development of cybersecurity capabilities across the state or territory and must be developed and approved by a Cybersecurity Planning Committee, the composition and scope of which is specified on pp. 62-64 of the NOFO. A Cybersecurity Plan Checklist may be found on pp. 66-72 of the NOFO and a Plan Template may be found here.

Applications may include up to four investment justifications, one for each of the SLCGP objectives (see above). Investments for objectives 1, 2 and 3 must have at least one project. Investments for objective 4 are optional for FY22 but that objective must still be addressed in the Cybersecurity Plan even if grant funds are not used to carry it out.

There is a 10% cost share/match required under this program which can be satisfied through a cash or third-party in-kind contribution. The performance period is four years.

Program documents, including FAQs, and other resources may be found here and here.

MOTOROLA SOLUTIONS OFFERS A PROVEN BASIS FOR YOUR APPLICATION

We offer a wide range of cybersecurity services, aligned to the National Institute of Standards and Technology (NIST) Cybersecurity Framework, that can help you detect, prevent and respond to cyber attacks including:

- Advisory Services - Identify vulnerabilities and develop a robust cybersecurity strategy with risk assessments, penetration testing and system recovery services.
- Managed Services - Protect your endpoints, network, cloud and mission-critical systems. As a managed security services provider (MSSP), we provide cost-effective solutions and expert assistance.
- Cybersecurity Training - Combat potential cybersecurity attacks with cybersecurity training. Our program ensures your workforce has the right skills and expertise to address any incident.
- Security Patching - Mitigate your cybersecurity risk with effective patching. Our security patching includes pre-testing, validation and anti-malware software updates aligned with industry standards. Grants System.

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 GovGrantsHelp.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: https://namrinfo.motorolasolutions.com/grants

---

JOIN THE PUBLIC SAFETY THREAT ALLIANCE

Public safety organizations need dedicated information and intelligence-sharing capabilities to protect against cyber threats, which are growing in scale and complexity. To provide them with the knowledge they need to defend against attacks, Motorola Solutions has established the Public Safety Threat Alliance (PSTA), a cyber threat Information Sharing and Analysis Organization (ISAO). Learn more on how you can join the PSTA.

ADDITIONAL RESOURCES

While cybersecurity requires a significant investment, it is imperative that agencies take measures to protect critical infrastructure from ransomware and other attacks. In partnership with the grant experts at Lexipol, we have compiled the top 10 strategies your organization's cybersecurity plan should include to help prevent data breaches and system compromises.

MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A. **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. © 2022 Motorola Solutions, Inc. All rights reserved. 09-2022 [BB03]