Grant Summary

The State and Local Cybersecurity Grant Program

Funds available

$280 Million

Apply by December 3, 2024

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. 15-17 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 school districts), with at least 25% of funds going 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. To be eligible for FY 2024 SLCGP funding, each entity is required to have established a Cybersecurity Planning Committee and must have submitted and received approval of their Cybersecurity Plan and projects.

Deadlines and submission information

The SAA must submit the full application by **December 3, 2024 , 5 pm ET.**

The full application package should be submitted via FEMA's Grants Outcomes System (FEMA GO).

MOTOROLA SOLUTIONS

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:

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:

1. 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.
2. Assessment and Evaluation: Identify areas for improvement in SLTT cybersecurity posture based on continuous testing evaluation, and structured assessments.
3. 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.
4. Workforce Development: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with their responsibilities as suggested in the National Initiative for Cybersecurity Education.

Applicants are required to address at least one of these objectives in their applications. For those eligible applicants that did not apply in FY 2022, FY 2023, or for FY 2022 SLCGP recipients that were unable to meet the requirements, must refer to both Appendix A and B for more information on how to meet those requirements for this 2024 solicitation.

In FY 2024, applicants should be focused on building upon FY22 and FY23 and continuing to invest in projects aligned with their Cybersecurity Plan and priorities from the FY23 program, including:

- Implement security protections commensurate with risk.
- Support organizational personnel commensurate with responsibility in the organization.

Allowable cost categories include planning, equipment, exercises, management and administration, organization, and training. More information can be found on pp. 37-38 and Appendix D of the NOFO.

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. 38-40 of the NOFO. Grant funds may be used to procure replacement equipment and services impacted by this prohibition, provided the costs are otherwise consistent with program requirements.

Emergency Communication: Grantees (including sub-recipients) who receive awards under the SLCGP that wholly or partially provide funding for emergency communication projects and related activities should comply with the most recent version of the SAFECOM Guidance on Emergency Communications Grants.

Additional program details

No more than four Investment Justifications (IJ) may be submitted with the application. The IJ and Project Worksheet (PW) templates can be found on the FY 2024 SLCGP page on grants.gov.

There is a 30% cost share/match (20% for multi-entity projects) required under this program which can be satisfied through a cash, contributions of the reasonable value of property or services, or (with prior approval) unrecovered indirect costs.

The performance period is four years.

All applicants with a CISA approved Cybersecurity Plan must submit their current Cybersecurity Plan to CISA via the FEMA SLCGP Inbox at FEMA-SLCGP@fema.dhs.gov no later than January 30, 2025, and annually thereafter on the same date throughout the grant's period of performance.

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, incident response planning and other professional services.
- **Managed Security Services** — Protect your mission-critical systems with integrated Managed Detection and Response (MDR) services for emergency call handling (ECH), land-mobile radio (LMR) systems and computer-aided dispatch (CAD). 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.

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.

MOTOROLA SOLUTIONS

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