

Maryland Local Cybersecurity Support Fund (LCSF) Program

Objective

This document provides a high-level overview of the [Maryland Local Cybersecurity Support Fund \(LCSF\) Program](#), administered by the Maryland Department of Emergency Management. This program will support “local governments” including local school systems, local school boards, municipalities, and local health departments to improve their cybersecurity preparedness.

Program Summary

This program may be used to adopt or enhance cybersecurity best practices, strengthen cybersecurity workforce development, address specific cybersecurity needs, or apply for federal cybersecurity preparedness grants. Funding may also be used to fund an entity's completion of a Cybersecurity Capabilities Assessment through a vendor approved by the Maryland Department of Information Technology (DoIT). See “Eligible Uses” below for more information.

This award is 'Reimbursable', meaning eligible entities must [submit for reimbursement](#) of approved project expenses. Documentation should clearly demonstrate an allowable purchase, directly related to the scope of work from an approved proposal and include both proof of purchase and the proof of payment. Reimbursement requests and documentation must be emailed to: lcsf.mdem@maryland.gov.

In order to apply for projects to be completed with Local Cybersecurity Support Funds (LCSF), a local government entity shall either provide proof of a Cybersecurity Capabilities Assessment in the previous 12 months OR undergo a free Cybersecurity Capabilities Assessment through DoIT OR complete the assessment through a vendor approved by DoIT within 12 months of application. Refer to pages 4-5 of the [NOFO](#) for more information on this requirement.

The Maryland Department of Emergency Management (MDEM) manages LCSF on behalf of the State of Maryland, provides administrative oversight, and serves as the main point of contact for eligible applicants. Once projects are awarded, MDEM helps recipients by processing reimbursement requests and making sure all state requirements are met.

Application
Deadline

Applications must be submitted by **August 28, 2026, by 11:59 p.m.**

EST. Grant applications are submitted by emailing completed forms to lcsf.mdem@maryland.gov.

Applications will only be considered if applicants can provide proof of a Cybersecurity Capabilities Assessment through DoIT or an

	<i>approved vendor, OR proof that an approved assessment will be completed within 12 months of application.</i> Refer to pages 3-4 of the NOFO for more information on how to apply and documents necessary for application.
Eligible Uses	» Completion of Cybersecurity Capabilities Assessments through an approved vendor » Adoption or enhancement of cybersecurity best practices, such as updating current devices, purchasing new software to improve cybersecurity preparedness, implementing and maintaining integrators or other similar intelligence-sharing infrastructure » Cybersecurity workforce development, such as recruiting and hiring IT staff focused on cybersecurity or paying outside vendors for cybersecurity training » Addressing specific cybersecurity needs such as supporting the security of local wastewater treatment plants by acquiring or implementing cybersecurity-related upgrades » Applying to federal cybersecurity preparedness grants » Management and administration expenses associated with the project types listed above. Funding for this category may not exceed 5% of the total project cost
Cost Sharing Requirements	» No cost share or cost match is required
Priority Populations	» No priority populations are listed

FY26 Local Cybersecurity Support Fund Application Status

The [Maryland Local Cybersecurity Support Fund Program](#) is soliciting applications until **August 28, 2026**. If you have any questions about the LCSF program, please email lcsf.mdem@maryland.gov.