Cyber Resilient Massachusetts Grant Program Informational Webinar

NOFO No. 2024-Cyber-01

May 23, 2024

MassCyberCenter at MassTech

Cyber Resilient Massachusetts Grant Program Overview

Summary: The Cyber Resilient Massachusetts Grant Program will provide grants of up to $25,000 to municipalities to fund narrowly focused cybersecurity technology upgrades identified through a cybersecurity vulnerability assessment.

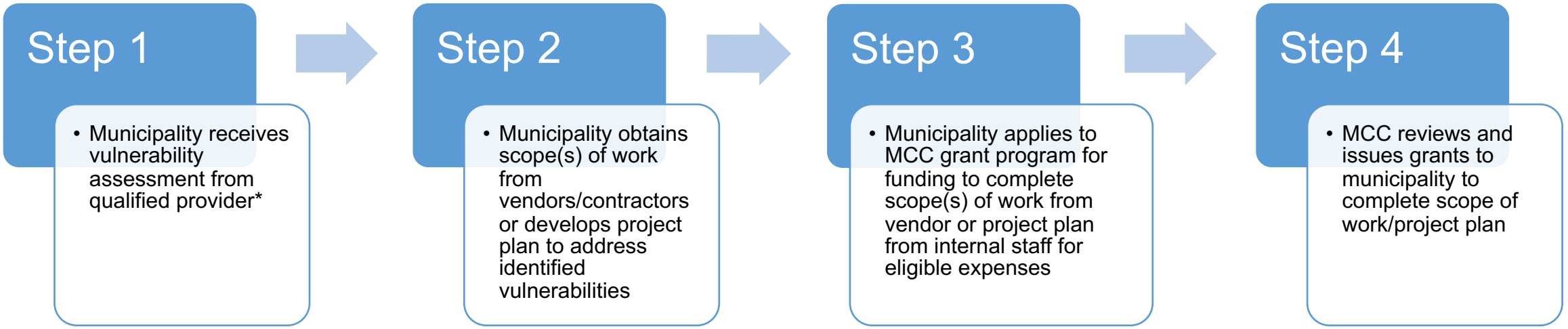
Goal: Grants will position municipalities to remediate cybersecurity vulnerabilities and be better positioned to defend against cybersecurity threats. Grants will also enable municipalities to integrate with a Security Operations Center (SOC) which may include the CyberTrust Massachusetts SOC. *(note: joining the CyberTrust Massachusetts SOC is not a requirement to receive funding)*

Eligible Applicants: Municipal entities. Joint applications between municipal entities (i.e. local governments and school districts) are encouraged. Regional school districts may apply separately from local governments.

Notice of Funding Opportunity: https://masscybercenter.org/notice-funding-opportunity-cyber-resilient-massachusetts-grant-program

MassCyberCenter at MassTech

Grant Process for Municipality



***Qualified Providers of Vulnerability Assessments**

- CyberTrust Massachusetts (more info here)
- EOTSS Office of Municipal and School Technology – Health Check Program (more info here)
- Commonwealth Fusion Center – Vulnerability and Threat Intelligence Project (sign up here)
- CISA – Cyber Hygiene Scan or Penetration Test
- Vendor providing support to a municipality or internal municipal staff completing the Nationwide Cybersecurity Review as part of a Municipal Local Cybersecurity Grant Program application

MassCyberCenter at MassTech

Uses of Grant Funds

Eligible Uses of Funds	Ineligible Uses of Funds
• Capital equipment, technology, and infrastructure for cybersecurity • Vendors/contractors or IT-related staff costs of municipality performing the services	• Costs of the original vulnerability assessment conducted by a qualified provider; • Improvements that may be funded under the Municipal Local Cybersecurity Grant Program; and • Scopes of work from CyberTrust Massachusetts to provide cybersecurity upgrades identified through a vulnerability assessment from a qualified provider.

Potential Project Examples

- Implementing Microsoft best practices in O365 or Google best practices in Google Workspace
- Purchasing a new firewall certificate
- Purchasing a firewall or other smart switches/routers to integrate within a municipal network

Application Requirements

- Respondent overview, including a description of any participation in cybersecurity collaborations in Massachusetts.
- Copy of the vulnerability assessment completed no later than six months before the response by a qualified provider that identifies recommended cybersecurity improvements.
- A non-confidential description of the cybersecurity investment efforts the Respondent will be making based on the assessment and how the improvements will assist the respondent in developing a mature cybersecurity program (250 words maximum).
- List of which of the 18 CIS Critical Security Controls are associated with those vulnerabilities being mitigated.
- The scope of work from a vendor or a project plan to be performed by IT-related staff of the municipality to address cybersecurity vulnerabilities to implement the cybersecurity upgrades based on the assessment
- Funding request and project budget (Note: funding requests may not exceed $25,000 though improvement projects may cost more)

Apply here.

Grant Evaluation Criteria

- Projects that will address cybersecurity vulnerabilities identified as part of an assessment and reduce the cybersecurity risk of the respondent
- Likelihood that the improvements will assist the respondent in developing a mature cybersecurity program
- Participation of the respondent in statewide cybersecurity collaborations in Massachusetts
- Considerations of geographic and economically equitable outcomes

Reporting Requirements

Grantees will be required to report to the MassCyberCenter on:

- The number of vulnerabilities closed as a result of the grant;
- Type of vulnerabilities closed as a result of the grant (short narrative);
- List which of the 18 CIS Critical Security Controls are associated with those vulnerabilities being mitigated;
- Total dollars (including non-MassTech funds) expended as part of improvement projects; and
- Project status (on track; some obstacles or project delays but will be overcome; off track/project in jeopardy).

See grant reporting template here.

Timeline

Task	Date
NOFO Issued, Applications Open	May 7
Informational Webinar	May 23
Questions Due	May 30
Answers to Questions Posted	June 6
Application review begins*	July 1 by 5 pm

**Applications will be accepted and reviewed on a rolling basis beginning July 1 until all program funds are expended*

MassCyberCenter at MassTech

Questions?

Questions regarding this NOFO must be submitted by email to proposals@masstech.org with the following Subject Line:
"Questions – NOFO No. 2024-Cyber-01"

MassCyberCenter at MassTech