Notice of Funding Opportunity for Cyber Resilient Massachusetts

NOFO No. 2026-Cyber-01

Massachusetts Technology Collaborative
75 North Drive
Westborough, MA 01581-3340
http://www.masstech.org

Procurement Team Leader:	**Maxwell Fathy**
Date Issued:	March 18, 2026
Applications Due:	Rolling

1. INTRODUCTION

1.1 Overview

The Mass Cyber Center, a division of the Massachusetts Technology Collaborative ("Mass Tech Collaborative" or "MassTech"), is issuing this Notice of Funding Opportunity for the Cyber Resilient Massachusetts Grant Program to solicit responses from municipalities, small businesses, and non-profits interested in receiving grants to fund Security Operations Center (SOC) services, including Managed Detection and Response (MDR) and other related services. Grants will position municipalities, small businesses, and non-profits to remediate cybersecurity vulnerabilities and defend against cybersecurity threats. Respondents will be competing against each other for grant funding and the submissions of all Respondents shall be compared and evaluated pursuant to the evaluation criteria set forth in this NOFO.

Mass Tech Collaborative will be the contracting entity on behalf of the Mass Cyber Center for the purposes of this NOFO, and (except where the specific context warrants otherwise), the Mass Cyber Center and Mass Tech Collaborative are collectively referred to as Mass Tech Collaborative or MassTech. Mass Tech Collaborative will enter into grant agreement with selected Respondents.

1.2 Mass Tech Collaborative and the MassCyberCenter

Mass Tech Collaborative is an independent public instrumentality of the Commonwealth of Massachusetts chartered by the Commonwealth to serve as a catalyst for growing its innovation economy. Mass Tech Collaborative brings together leaders from industry, academia, and government to advance technology-focused solutions that lead to economic growth, job creation, and public benefits in Massachusetts. For additional information about Mass Tech Collaborative and its programs and initiatives, please visit our website at www.masstech.org.

The **MassCyberCenter** has a vision for a diverse, vibrant, and competitive Massachusetts cybersecurity ecosystem that enhances resiliency for public and private entities, provides workforce development opportunities, and elevates public cybersecurity awareness. The Center carries out this vision through its mission to convene the Massachusetts cybersecurity ecosystem to improve cybersecurity resiliency, workforce development, and public awareness within the state by developing cutting edge programs, organizing engaging events, and leading collaborative working groups. For more information about MassCyberCenter and its programs and activities generally, please visit the web site at https://masscybercenter.org.

2. Grant Overview

The MassCyberCenter has modified the Cyber Resilient Massachusetts Grant Program released on May 7, 2024, to enable municipalities, small businesses, and non-profits, to receive grants of up to $25,000 for SOC services, including MDR and other related services, from CyberTrust Massachusetts. Eligible respondents under this NOFO are **municipalities, small businesses, and non-profits** in Massachusetts.

Joint applications between municipal entities (i.e. local governments and school districts) are encouraged. Regional school districts may apply separately from local governments. Additionally, regional entities, including those that are non-profits, are eligible to apply if municipalities are the end-beneficiary of funds.

Eligible small businesses are those that meet the U.S. Small Business Administration definition of a small business (see Table of Small Business Size Standards).

The MassCyberCenter will prioritize applications from Massachusetts-based small businesses and non-profits that represent the following sectors:

- Artificial Intelligence / Machine Learning
- BlueTech
- ClimateTech
- Defense & Aerospace
- FinTech
- Entrepreneurial-support Organizations
- Health Care and Digital Health
- Manufacturing
- Microelectronics
- Robotics
- Quantum

Grants to municipalities will be forward funded. Grants to small businesses and non-profits will be funded on a reimbursement basis.

Services Eligible for Grant Funding

Municipalities, small businesses, and non-profits in Massachusetts are eligible to receive a grant of up to $25,000 to fund SOC services, including MDR and other related services, from CyberTrust Massachusetts for up to three years. CyberTrust Massachusetts is a non-profit organization working closely with the MassCyberCenter and is currently supported with grant funding to provide governance to SOC and Cyber Range facilities located at colleges and universities across the Commonwealth that grow and promote the diversity of the cybersecurity talent pipeline, as well as help provide solutions to municipalities, small businesses, and other organizations for protection against cyber threats. SOC services are provided to customers as part of a paid subscription.

Grants are eligible to fund the following CyberTrust Massachusetts services:

Managed Detection and Response (MDR)

- Managed endpoint detection and response using a SentinelOne technology stack: 24/7 monitoring of endpoints, threat insights, proactive notifications, consultations on handling threats and false positives, and threat response
- Active threat hunting, based on cyber threat intelligence, malicious actor tactics, and known bad resources, identifies new and unique threats
- Network Discovery: visibility of all devices connected to a network and scanning to identify and manage connected devices
- Vulnerability Management: a dashboard showing applications aggregated by version with several ways to filter application and vulnerability information
- Application and Asset Inventory: visibility into infrastructure, to include endpoints, servers, and software

Extended Detection and Response (XDR) — broader monitoring across key systems

- Extends existing SentinelOne EDR with cross-source detection across identity, email, and firewall — no new platform required
- Monitors a defined set of critical integrated log sources, including Active Directory, Entra ID, email security, and firewall; additional integrations available as needs grow
- Correlates activity across sources to detect additional threats, such as phishing-related compromise, account takeover, and lateral movement
- Automated detection and alerting, with analyst review and escalation to your team on high-confidence incidents
- Supports cyber insurance requirements, compliance reviews, and incident investigations through consolidated activity records across monitored systems

Application Control and Zero Trust

- Control over which applications can run on your systems, using the ThreatLocker technology stack
- Containment of unauthorized software and programs
- Reduced attack surface and lateral movement opportunities
- Can be applied broadly across all assets, or selectively across high-value assets and users

Note: Grants may not fund CyberTrust Massachusetts Advisory Services.

CyberTrust Massachusetts is also employing students from its academic members to help provide these SOC services under the supervision of industry experts while receiving workforce training and development opportunities that will prepare them to enter cybersecurity careers.

CyberTrust Massachusetts was formed in 2022 through a grant from the Massachusetts Cybersecurity Innovation Fund, which is administered by the MassCyberCenter. In December of 2023, the Massachusetts Legislature passed legislation that allows political subdivisions of the Commonwealth, including but not limited to municipalities, to enter into a contract for cybersecurity and related services with "an organization that was established, in whole or in part, through a grant from the Massachusetts Cybersecurity Innovation Fund" without a public procurement process. *See* 2023 Mass. Chapter 77, Section 195. Municipalities may therefore contract directly with CyberTrust Massachusetts for cybersecurity and related services without a public procurement process.

For more information about CyberTrust Massachusetts, visit https://www.cybertrustmass.org/.

2.2 Grant Requirements and Guidance

Respondents must first receive a scope of work from CyberTrust Massachusetts for services. The scope of work may be for up to three years of services and total no more than $25,000. Respondents must include this scope of work as part of their application per section 3.1 of this NOFO.

To develop a scope of work, interested municipal respondents should contact muni@cybertrustmass.org; interested small business and non-profit respondents should contact smb@cybertrustmass.org.

2.3 Evaluation Process and Criteria

Selection of a Respondent to receive funding as set forth within this NOFO may be based on criteria that include but are not limited to:

- Projects that provide SOC services, including MDR and other related services, from CyberTrust Massachusetts
- Applications that leverage non-MassTech sources of funding

Mass Tech Collaborative shall evaluate each Application that is properly submitted. As part of the selection process, Mass Tech Collaborative may invite Respondents to answer questions regarding their Application in person or in writing. In its sole discretion, Mass Tech Collaborative may also choose to enter into a negotiation period with a Respondent and then ask the Respondent to submit additional information.

Lack of debarment status by either the state or federal government is also required.

The order of these factors does not generally denote relative importance. The goal of this NOFO is to select and enter into a grant agreement with the Respondent that will most closely align with MassTech Collaborative's goals in the publication of this NOFO. Mass Tech Collaborative reserves the right to consider such other relevant factors as it deems appropriate.

3. APPLICATION PROCESS

3.1 Application and Submission Instructions

Respondents are cautioned to read this NOFO carefully and to conform to its requirements. Failure to comply with the requirements of this NOFO may serve as grounds for rejection of an Application.

a. All applications must be submitted HERE
b. Application shall include:
    a. An overview of the Respondent, including
        i. For municipalities: population of the municipality, number of employees, and description of any participation in cybersecurity collaborations in Massachusetts.
        ii. For small businesses: a description of the business, number of employees in Massachusetts, and annual revenue.
        iii. For non-profits: a description of the non-profit and number of employees.
    b. Scope of Work for SOC Services:
        i. The scope of work from CyberTrust Massachusetts for SOC services.
        ii. A non-confidential description of how SOC services will assist the respondent in developing a mature cybersecurity program (250 words maximum).
    c. The total not-to-exceed costs funded by the grant for SOC services in the Budget Template (Attachment B). Grants may not exceed $25,000. List additional fees, overhead charges, or reimbursable expenses, if any. As a general policy, the Mass Tech Collaborative does not pay mark-ups on reimbursables or out-of-pocket expenses. Mass Tech Collaborative also does not pay for word processing or meals. For travel costs, the Mass Tech Collaborative pays the IRS rate per mile.
    d. Authorized Application Signature and Acceptance Form (Attachment A), which contains specified certifications by Respondent. Please read the certifications carefully before signing.
    e. A copy of the respondent's W-9

c. Please note that as a public entity, Mass Tech Collaborative is subject to the Massachusetts Public Records Law (set forth at Massachusetts General Laws Chapter 66) and thus all documents and other materials made or received by Mass Tech Collaborative and/or its employees are subject to public disclosure upon request. While there are very limited and narrow exceptions to disclosure under the Public Records Law, subclause (n) of the first paragraph of clause Twenty-Six of chapter 7 of the Massachusetts General Laws exempts vulnerability assessments relating to cybersecurity, the disclosure of which is likely to jeopardize public safety or cybersecurity. **Therefore any vulnerability assessment relating to cybersecurity submitted in response to this NOFO will be presumptively treated as a confidential document**. **Please label it as such**. If a Respondent wishes to have Mass Tech Collaborative treat any additional information or documentation as confidential, the Respondent must submit a written request to the Mass Tech Collaborative's General Counsel's office no later than 5:00 p.m. ten (10) business days prior to the required date of Application submission. The request must precisely identify the information and/or documentation that is the subject of the request and provide a detailed explanation supporting the application of the statutory exemption(s) from the public records cited by the Respondent. The General Counsel will issue a written determination within five (5) business days of receipt of the written request. If the General Counsel approves the request, the Respondent shall clearly label the relevant information and/or documentation as "**CONFIDENTIAL**" in the Application. Any statements in an Application reserving any confidentiality or privacy rights that is inconsistent with these requirements and procedures will be disregarded.
d. Any and all responses, Applications, data, materials, information and documentation submitted to Mass Tech Collaborative in response to this NOFO shall become Mass Tech Collaborative's property.

3.2 Application Timeframe

MassTech will review applications on a rolling basis. Awards will be issued until all program funds are expended.

Grants may only fund expenses incurred after an application is submitted to MassTech. *Note: submission of an application is not a guarantee of receiving an award from MassTech*, *and applicants must assume all project costs if the application is not selected for an award.*

3.3 Questions

Questions regarding this NOFO must be submitted by electronic mail to proposals@masstech.org with the following Subject Line: "Questions – NOFO No. 2026-Cyber-01". Questions will be reviewed on a rolling basis and responses will be posted to Mass Tech Collaborative and Commbuys website(s).

4.0 GENERAL CONDITIONS

4.1 General Information

a) If an Application fails to meet any material terms, conditions, requirements or procedures, it may be deemed unresponsive and disqualified. The Mass Tech Collaborative reserves the right to waive omissions or irregularities that it determines to be not material.

b) This NOFO, as may be amended from time to time by Mass Tech Collaborative, does not commit Mass Tech Collaborative to select any organization(s), award any grant funds pursuant to this NOFO, or pay any costs incurred in responding to this NOFO. Mass Tech Collaborative reserves the right, in its sole discretion, to withdraw the NOFO, to engage in preliminary discussions with prospective Respondents, to accept or reject any or all Applications received, to request supplemental or clarifying information, to negotiate with any or all qualified Respondents, and to request modifications to Applications in accordance with negotiations.

c) On matters related solely to this NOFO that arise prior to an award decision by the Mass Tech Collaborative, Respondents shall limit communications with the Mass Tech Collaborative to the Procurement Team Leader and such other individuals as the Mass Tech Collaborative may designate from time to time. No other Mass Tech Collaborative employee or representative is authorized to provide any information or respond to any questions or inquiries concerning this NOFO. Respondents may contact the Procurement Team Leader for this NOFO in the event this NOFO is incomplete.

d) The Mass Tech Collaborative may provide reasonable accommodations, including the provision of materials in an alternative format, for Respondents with disabilities or other hardships. Respondents requiring accommodations shall submit requests in writing, with supporting documentation justifying the accommodations, to the Procurement Team Leader. The Mass Tech Collaborative reserves the right to grant or reject any request for accommodations.

e) Respondent's Application shall be treated by the Mass Tech Collaborative as an accurate statement of Respondent's capabilities and experience. Should any statement asserted by Respondent prove to be inaccurate or inconsistent with the foregoing, such inaccuracy or inconsistency shall constitute sufficient cause for Mass Tech Collaborative in its sole discretion to reject the Application and/or terminate of any resulting agreement.

f) Costs that are not specifically identified in the Respondent's response and/or not specifically accepted by Mass Tech Collaborative as part of the agreement will not be compensated under any contract awarded pursuant to this NOFO.

g) Mass Tech Collaborative's prior approval is required for any subcontracted services under any agreement entered into as a result of this NOFO. The selected Respondent will take all

appropriate steps to assure that minority firms, women's business enterprises, and labor surplus area firms are used when possible. The selected Respondent is responsible for the satisfactory performance and adequate oversight of its subcontractors. Subcontractors are required to meet the same requirements and are held to the same reimbursable cost standards as the selected Respondent.

h) Submitted responses must be valid in all respects for a minimum period of sixty (60) days after the deadline for submission.

4.2 Posting of Modifications/Addenda to NOFO

This NOFO has been distributed electronically using the Mass Tech Collaborative and Commbuys websites. If Mass Tech Collaborative determines that it is necessary to revise any part of this NOFO, or if additional data is necessary to clarify any of its provisions, an addendum will be posted to the websites. It is the responsibility of each potential Respondent to check the Mass Tech Collaborative, the Innovation Institute and Commbuys websites for any addenda or modifications to the NOFO. The Mass Tech Collaborative accepts no liability and will provide no accommodation to Respondents who submit a response based on an out-of-date NOFO.

Attachment A
Authorized Respondent's Signature and Acceptance Form

The undersigned is a duly authorized representative of the Respondent listed below. The Respondent has read and understands the NOFO requirements. The Respondent acknowledges that all the terms and conditions of the NOFO are mandatory, and that Respondent's response is compliant with such requirements. The Respondent specifically acknowledges the application of the procedures regarding submission of information under the MA Public Records Law set forth in Section 3.1 c) of the NOFO, and specifically agrees that it shall be bound by those procedures.

Respondent agrees that the entire proposal will remain valid for sixty (60) days from receipt by MassTech.

I certify that Respondent is in compliance with all corporate filing requirements and state tax laws.

I further certify that the statements made in this response to the NOFO, including all attachments and exhibits, are true and correct to the best of my knowledge.

Respondent: _____
(Printed Name of Respondent)

By: _____
(Signature of Authorized Representative)

Name: _____

Title: _____

Date: _____

Attachment B
Budget Template

SEE ASSOCIATED EXCEL SPREADSHEET