Notice of Funding Opportunity ("NOFO") for Entities Interested in Establishing Security Operations Centers

NOFO No. 2025-Cyber-03

Amendment 1

4/24/2025

1) The cover page is amended as follows:

Responses Due: 4/24/2025 by 3PM EST

is changed to

Responses Due: 5/1/2025 by 3PM EST

2) Section 3.2 Application Timeline is amended as follows:

Task	**Date:**
NOFO Released	March 24, 2025
Information Session	April 8, 2024 @ 3:00 p.m.
Questions Due	April 11, 2025 by 5:00 p.m.
Question and Answer File Posted	April 17, 2025
Applications Due	April 24, 2025 by 3:00 p.m.

Is changed to

Task	**Date:**
NOFO Released	March 24, 2025
Information Session	April 8, 2024 @ 3:00 p.m.
Questions Due	April 11, 2025 by 5:00 p.m.
Question and Answer File Posted	April 17, 2025
Applications Due	May 1, 2025 by 3:00 p.m.

Notice of Funding Opportunity ("NOFO") for Entities Interested in Establishing Security Operations Centers

NOFO No. 2025-Cyber-03

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

NOFO Team Leader:	**Maxwell Fathy**
NOFO Issued:	**3/24/2025**
Information Session:	**4/8/2025 (register here)**
Questions Due:	**4/11/2025**
Answers to Questions Posted:	**4/17/2025**
Responses Due:	**5/1/2025 by 3PM EST**

1. INTRODUCTION

1.1 Overview

Massachusetts Technology Collaborative ("MassTech"), on behalf of the MassCyberCenter, is issuing this Notice of Funding Opportunity (NOFO No. 2025-Cyber-03) (the "NOFO"). We are seeking applications ("Responses") from entities ("Respondents") interested in establishing and operating a Security Operations Center ("SOC") providing cybersecurity services to organizations serving the Defense Industrial Base (DIB) as a member of CyberTrust Massachusetts. Respondents may request funding for capital and/or operational expenditures associated with establishing such a facility.

Public higher education institutions and non-profits are eligible to respond to this solicitation. Additionally, this opportunity is only available to respondents in Massachusetts counties where there is not currently a CyberTrust Massachusetts SOC. Respondents located in the following Massachusetts counties are eligible to apply: Barnstable County, Berkshire County, Bristol County, Dukes County, Essex County, Frankin County, Hampden County, Middlesex County, Nantucket County, and Worcester County.

Mass Tech Collaborative will enter into a grant agreement (an Operating Funds Grant Agreement, or a Capital Funds Grant Agreement, or a combination of these, depending on funding being requested) with selected Respondents containing certain standard provisions (the "Agreement").

1.2 MassTech and 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. Mass Tech Collaborative has six primary divisions: the Innovation Institute, Massachusetts Broadband Institute, Massachusetts Cyber Center, Center for Advanced Manufacturing, NEMC Hub, and the Massachusetts e-Health Institute. For additional information about MassTech 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. The Grant

2.1 CyberTrust Massachusetts Overview

CyberTrust Massachusetts ("CTM") 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 that will 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. The goal of CyberTrust Massachusetts is to provide strategic planning and coordination to SOC and Range facilities that address the following needs of the Massachusetts cybersecurity ecosystem ("the Imperatives"):

- *Undersecurity* – Organizations across the Commonwealth, especially municipalities, small businesses, and non-profits, are challenged to find affordable resources to defend themselves against growing cybersecurity threats and maintain cyber resiliency.
- *Underemployment* – There is a supply shortage of trained workers available to meet the cybersecurity industry's workforce demands. Additionally, communities of color and women are underrepresented in the cybersecurity workforce and are frequently overlooked for employment due to a lack of experience.
- *Employee Training* – Businesses across the Commonwealth do not have a location to send their employees to receive cybersecurity training at an affordable rate.
- *Business/Economic Development* – There is a need to convene regional hubs for business development where cybersecurity entrepreneurs can establish and grow startups or where specific industry segments such as defense contractors can receive specialized support.

CTM members include academic and non-profit workforce training organizations in Massachusetts operating SOC and/or Cyber Range facilities, as well as private sector companies. The support of CTM leads to a coordinated and streamlined group of SOC and Range facilities working together to grow the pipeline of skilled, experienced, and diverse cyber workers; to enable students and workers at all career stages, from all backgrounds statewide, to access cyber education and training programs linked to cyber employers; and to help local governments, non-profits and small businesses manage their defenses and combat growing cyber threats with affordable cybersecurity services.

Organizations operating SOCs and Cyber Ranges are members of CTM, committed to addressing the imperatives, and subject to paying membership dues and maintaining status as a member in good standing.

2.2 CTM Security Operations Center

CTM has established and is managing a Security Operations Center providing cybersecurity services, including Managed Endpoint Detection and Response ("MDR") and cybersecurity assessments. MDR services monitor, detect, and respond to cybersecurity threats 24/7 on endpoints (laptops, cell phones, printers, servers, etc.) and are available for organizations as part of a paid subscription. Cybersecurity assessments provide vulnerability scans and health checks to help organizations understand their cyber posture and the specific shortfalls that create risk for them. CTM has focused on providing these services to municipal entities in Massachusetts since launching the SOC in January 2024.

CTM employs professional staff and manages contracts with technology and service providers that support the delivery of these services. CTM also employs students from its academic members to help provide these SOC services. Student SOC employees receive workforce training and development opportunities that prepare them to enter cybersecurity careers.

CyberTrust Massachusetts has operated the SOC since January 2024 remotely and is also now operating at physical SOC facilities at Bridgewater State University and Union Station in Springfield, Massachusetts. These SOC facilities serve as physical locations where students support the delivery of cybersecurity services under the supervision of CTM professional staff.

2.3 SOC Funding Eligibility

This solicitation provides an opportunity for interested academic institutions and non-profits to access funds to operate a SOC as a member of CyberTrust Massachusetts designed to protect the DIB. It also provides an opportunity to access capital funds to build or procure new and novel infrastructure, equipment, or resources that directly aid in the creation of SOCs. Funding requests for capital and/or operating expenditures may total no more than $300,000.

Only public higher education institutions and non-profits in Massachusetts counties where there is not currently a CyberTrust Massachusetts SOC are eligible to respond to this solicitation. Respondents

from the following Massachusetts counties are eligible: Barnstable County, Berkshire County, Bristol County, Dukes County, Essex County, Frankin County, Hampden County, Middlesex County, Nantucket County, and Worcester County.

Respondents must collaborate with CTM to develop a plan for their proposed SOC's operations prior to submitting a grant application. Our goal with this process is to ensure there is alignment between CTM and the Respondent's operating plans. This plan must then be submitted as part of the response to this NOFO per section 3.2. To begin discussing a plan for the development of a DIB-focused SOC, contact Peter Sherlock, the CEO of CyberTrust Massachusetts, at pete@cybertrustmass.org.

Note: Respondents must agree to operate the SOC as a member of Cyber Trust Massachusetts to be eligible to receive funding. Grants are not eligible to fund the cost of membership in CyberTrust Massachusetts.

2.4 Information Regarding Grant Funds - Use of Proceeds

Infrastructure grant funds to be provided by Mass Tech Collaborative must be used for funding capital projects that are an integral part of the overall project or initiative being undertaken by the Respondent. As part of their application, Respondents must submit the budget for their overall project, including operating expenses, capital expenses, and the portions of the project not funded by the Mass Tech Collaborative. In that overall budget, Respondents should specify which portions of the expenditures are proposed to be funded by the Mass Tech Collaborative. Any capital expenditure to be funded by the Mass Tech Collaborative under this program must be one that will be accounted for by the recipient in its financial records as a capital expenditure under Generally Accepted Accounting Principles ("GAAP"). Examples of such capital expenditures could include expenditures for the purchase of equipment and the development of new technology platforms or systems, the acquisition of land and existing facilities, construction of new buildings and the renovation of existing buildings. Such capital expenditures may in certain projects also include salaries of staff directly engaged in managing capital projects to the extent such expenditures are capitalizable under GAAP. Salaries of individuals engaged in operations, as well as other non-personnel operating costs, are not capital expenditures

3. APPLICATION PROCESS

3.1 Application and Submission Instructions

All Responses must be submitted electronically (.pdf or .doc) to proposals@masstech.org. Please state the following in the subject line: Proposal for Entities Interested in Establishing Security Operations Centers, NOFO No. 2025-Cyber-03.

Responses are due on April 24, 2025. After receipt of responses, Mass Tech Collaborative will contact respondents to discuss their application and funding request based on their alignment with criteria listed in section 4.

3.2 Information Required in Submission:

Entities must include the following information in their response to be considered by Mass Tech Collaborative to receive funding support for capital and/or operational expenses to establish a SOC.

(a) Response Cover Sheet (Attachment A)
(b) Authorized Application Signature and Acceptance Form (**Attachment B**)
(c) Respondent's W-9
(d) Description of Respondent
- Identify the lead respondent and their qualifications
- Identify partners to the lead respondent (academic, corporate, or other)
- Provide qualifications of lead respondent and partners for hosting a SOC and becoming a member of CyberTrust Massachusetts

- Identify individuals serving as project leads for the proposed SOC and their qualifications

(e) SOC Overview

- Describe the proposed SOC, including whether it will utilize an existing facility or require construction of a new facility
- Provide a timeline for the opening of the SOC
- Describe how the proposed SOC would operate as a member of CyberTrust Massachusetts:
    i. *Required:* Provide a letter of support from CyberTrust Massachusetts endorsing the respondent's proposed SOC.
- Describe how the SOC would support the DIB and advance the Imperatives;
- Provide a list potential customers:
    i. *Optional:* Provide letters of support for any potential customers.
- Describe outreach plan to secure potential customers
- Provide an estimate of the number of students eligible to serve as SOC employees
    i. *Note*: SOC employees must be US Citizens or Permanent Legal Residents only

(f) Economic Model

- List expenses for the proposed SOC, including capital and operational expenses, for the first three years of operations
- Identify all sources of funding for the proposed SOC for the first three years of operations
    i. *Optional:* Provide letters of commitment to provide funding from non-MassTech sources
- Detail how the facility will become financially self-sustainable within three years

(g) Funding Request

- Identify the capital and/or operating expenses you are requesting funding for and why they are necessary
- Provide a timeline for the expenditure of funds requested

(h) Exceptions to the applicable Grant Agreement posted with this NOFO (an Operating Funds Grant Agreement, or a Capital Funds Grant Agreement, or a Combined Operating Funds and Capital Funds Grant Agreement, depending on funding being requested) if any

By executing the Authorized Respondent's Signature and Acceptance Form and submitting a response to this NOFO, Respondents certify that they (1) are in compliance with the terms, conditions and specifications contained in this NOFO, (2) acknowledge and understand the procedures for handling materials submitted to the Mass Tech Collaborative as set forth below, (3) agree to be bound by those procedures, and (4) agree that the Mass Tech Collaborative shall not be liable under any circumstances for the disclosure of any materials submitted to the Mass Tech Collaborative pursuant to this NOFO or upon the Respondent's selection.

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 and shall be subject to public disclosure. As a public entity, the Mass Tech Collaborative is subject to the Massachusetts Public Records Law (set forth at Massachusetts General Laws Chapter 66). There are very limited and narrow exceptions to disclosure under the Public Records Law. If a Respondent wishes to have the Mass Tech Collaborative treat certain 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. fourteen (14) business days prior to the required date of Application submission set forth in Section 3.2 below. 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 ten (10) 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.

3.2 Application Timeframe

The application process will proceed according to the following schedule. The target dates are subject to change. Therefore, Respondents are encouraged to check Mass Tech Collaborative's website frequently for updates to the schedule.

Task	Date:
NOFO Released	March 24, 2025
Information Session	April 8, 2024 @ 3:00 p.m.
Questions Due	April 11, 2025 by 5:00 p.m.
Question and Answer File Posted	April 17, 2025
Applications Due	May 1, 2025 by 3:00 p.m.

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. 2025-Cyber-03". All questions must be received by 5:00 p.m. EST on April 11, 2025. Responses to all questions received will be posted on April 17, 2025 to Mass Tech Collaborative and COMMBUYS website(s).

4. EVALUATION PROCESS AND CRITERIA

The MassCyberCenter will employ evaluation criteria in evaluating responses. The criteria assessed may include, without limitation, the following:

- Alignment of proposed SOC with the CyberTrust Massachusetts operating plan
- Commitment of respondent to operating the SOC as a member in good standing of CyberTrust Massachusetts
- Scale of impact of SOC on the cybersecurity resiliency of organizations serving the DIB in Massachusetts
- Scale of impact of the proposed SOC on the cybersecurity workforce in Massachusetts
- Demonstrated experience of respondent in advancing cybersecurity resiliency and/or workforce development
- Timeline for launch of proposed SOC and delivery of services to customers
- Quantity of committed and/or potential customers
- Expressions of commitment to the proposed SOC by partners, especially entities related to the DIB, academic partners, corporations, or community partners
- Economic feasibility of proposed SOC and likelihood of becoming financially self-sustainable within three years
- Clarity and thoroughness of the application, and
- Quality and experience of project team leads

The order of these factors does not generally denote relative importance. Mass Tech Collaborative and the MassCyberCenter reserve the right to consider such other factors as they deem appropriate.

5.0 GENERAL CONDITIONS

5.1 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 firm(s), award any contracts 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 NOFO 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 NOFO 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 NOFO 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.

i) Mass Tech Collaborative reserves the right to amend the Agreement at any time prior to execution. Respondents should review the Agreement as they are required to specify any exceptions to the Agreement and to make any suggested counterproposal in their Application. A failure to specify exceptions and/or counterproposals will be deemed an acceptance of the Agreement's general terms and conditions, and no subsequent negotiation of such provisions shall be permitted.

5.2 Posting of Modifications/Addenda to NOFO

This NOFO has been distributed electronically using the Mass Tech Collaborative and COMMBUYS websites. If the 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 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
Response Cover Sheet

<table>
<tr><td colspan="4">Name of Respondent</td></tr>
<tr><td>Mailing Address</td><td>City/Town</td><td>State</td><td>Zip Code</td></tr>
<tr><td>Telephone</td><td>Fax</td><td colspan="2">Web Address</td></tr>
<tr><td colspan="2">Primary Contact for Clarification</td><td colspan="2">Primary Contact E-mail Address</td></tr>
<tr><td colspan="2">Authorized Signatory</td><td colspan="2">Authorized Signatory E-mail Address</td></tr>
<tr><td colspan="2" rowspan="2">Legal Status/Jurisdiction (e.g., a Massachusetts corporation)</td><td colspan="2">Respondent’s EIN:
_____</td></tr>
<tr><td colspan="2">Respondent’s UEI No.:</td></tr>
</table>

Attachment B
Massachusetts Technology Collaborative
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 of the terms and conditions of the NOFO are mandatory, and that Respondent's response is compliant with such requirements.

The Respondent understands that, if selected by the Mass Tech Collaborative, the Respondent and the Mass Tech Collaborative will execute an Agreement specifying the mutual requirements of participation. The undersigned has either (*please check one)*:

☐ specified exceptions and counter-proposals to the terms and conditions of the applicable grant agreement posted with this NOFO, or
☐ agrees to the terms and conditions set forth therein

The undersigned acknowledges and agrees that the failure to submit exceptions and counter-proposals with this response shall be deemed a waiver, and the Agreement shall not be subject to further negotiation.

Respondent agrees that the entire Application response will remain valid for sixty (60) days from receipt by the Mass Tech Collaborative.

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 C
Budget Template

SEE ASSOCIATED EXCEL SPREADSHEET