MASSACHUSETTS
TECHNOLOGY
COLLABORATIVE

Request for Responses for Entities Interested in Establishing Cybersecurity Centers of Excellence

RFR No. 2022-Cyber-02

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

Procurement Team Leader:	**Maxwell Fathy**
RFR Issued:	**2/23/2022**
New **Live Zoom Q&A Call:**	**4/25/2022**
Revised **Questions Due:**	**4/26/2022**
Revised **Answers to Questions Posted:**	**5/3/2022**
Round 1 Responses Due:	**3/18/2022 by 3PM EST**
Round 2 Responses Due:	**5/20/2022 by 3PM EST**

*This amended version adds a live Q&A call with registration link and adds in new dates for questions and answers

1. INTRODUCTION

1.1 Overview

Massachusetts Technology Collaborative ("MassTech"), on behalf of the MassCyberCenter, is issuing this Request for Responses for Entities Interested in Establishing Cybersecurity Centers of Excellence (RFR No.2022-Cyber-02) (the "RFR"). We are seeking expressions of interest and qualification ("Responses") from entities ("Respondents") interested in establishing a Security Operations Center ("SOC") and/or a Cyber Range facility and becoming a Cybersecurity Center of Excellence ("CCE") as part of the Massachusetts Cybersecurity Consortium. Additionally, respondents submitting a request for funding whose responses meet the Imperatives outlined in section 2.1 and are ready to begin the process to establish a SOC or Cyber Range may be considered to receive funding for capital and/or operational expenditures associated with establishing a CCE.

This RFR will remain open for receipt of Responses for round one until March 18th and round two until May 20th or until it is withdrawn or modified pursuant to Section 5.1(f) below. The Mass Tech Collaborative will evaluate responses and enter into discussions with Respondents. Our decision to proceed to negotiate and award funding to a particular Respondent will be based on a best value judgment made in consideration of all relevant facts and circumstances as outlined in Section 4 below.

This RFR does not commit the Mass Tech Collaborative to select any entities, award any grants, or contract for any grants. The Mass Tech Collaborative reserves the right, in its sole discretion and in accordance with generally accepted good business practices, to accept or reject any or all submittals received, to negotiate with any or all qualified Respondents, to request modifications to proposals in accordance with such negotiations, to request supplemental or clarifying information from Respondents, or to cancel, amend or modify the RFR in any manner at any time.

1.2 MassTech and MassCyberCenter

MassTech is an independent public instrumentality of the Commonwealth of Massachusetts chartered by the Commonwealth to serve as a catalyst for growing its innovation economy. MassTech 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. MassTech's mission is to strengthen the competitiveness of the tech and innovation economy by driving strategic investments, partnerships, and insights that harness the talent of Massachusetts. For additional information about MassTech and its programs and initiatives, please visit our website at www.masstech.org.

The MassCyberCenter was launched in September 2017 with a vision to enhance opportunities for the Massachusetts cybersecurity ecosystem to compete as the national cybersecurity leader while strengthening the resiliency of the Commonwealth's public and private communities. The Center carries out this vision through its mission to enhance conditions for economic growth through outreach to the cybersecurity ecosystem of Massachusetts while fostering cybersecurity resiliency within the Commonwealth. Activities focus on convening the top public safety, technology, and municipal leaders across the state to grow programs that support our key institutions. For more information about MassCyberCenter and its programs and activities generally, please visit the web site at https://masscybercenter.org.

2. SERVICES REQUIRED

2.1 Overview of the Massachusetts Cybersecurity Consortium

The MassCyberCenter is issuing this RFR in support of the establishment of the Massachusetts Cybersecurity Consortium ("the Consortium") that will help provide solutions to municipalities, small businesses, and other organizations for protection against cyber threats, as well as grow and promote the diversity of the cybersecurity talent pipeline. Through the creation of, and engagement with, SOC and Range facilities, the Consortium aims to 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.

The Consortium's Imperatives will be coordinated and implemented through the creation of a non-profit organization that provides SOC and Cyber Range facilities assistance with strategic planning and coordination. The non-profit will have an Executive Director that reports to a Board of Directors which shall provide strategic oversight to programs and help identify funding sources. Mass Tech Collaborative is currently supporting the establishment of the Consortium and the non-profit organization.

Facilities offering SOC services, Cyber Range services, or both will be designated as "Cybersecurity Centers of Excellence" or "CCEs." CCEs must be members of the Consortium, committed to addressing the imperatives, and will be subject to paying membership dues to the non-profit and other membership requirements as established by the non-profit.

2.2 SOC Facilities

A SOC monitors network operations and provides a focal point for initial incident detection and response. Consortium SOC services will be provided to customers by a Managed Security Service Provider ("MSSP") in partnership with CCEs located statewide. The non-profit will pay for and hold the MSSP license and integrate SOC facilities at CCEs statewide. SOC services will be provided to municipalities, small business, and non-profit organizations for a fee. SOC facilities will recruit customers to join the Consortium in partnership with the non-profit.

SOC facilities will provide workforce and training opportunities for students affiliated with the entity operating the proposed CCE. Student employees will work as paid analysts/apprentices of the SOC in an on premise CCE providing the following services in partnership with an MSSP:

	Service Offered	Description
1	Threat Sharing	The SOC shares center's threat alerts with customers
2	Cyber Advisories	Sharing third party threat alerts with customers
3	Ongoing threat monitoring	Ongoing threat monitoring, initial triage and investigation, and notification to customer to investigate

4	Notification to customer to investigate	Additional incident investigation provided to customer
5	Cybersecurity Assessment	Perform cybersecurity assessments using various controls frameworks to identify opportunities to bolster cyber defenses
6	Security Awareness Training	Work with customer to raise awareness of cybersecurity threats
7	Monitoring phishing submissions	Customers can send reported phishing messages for further analysis by a SOC Team
8	Monitor internet accessible services	Customers with internet accessible services can rely on the SOC to look for risky services and make recommendations
9	Firewall Analysis and Reporting	Review firewall rules, logs, and serve as a resource to assist in identifying misconfigurations and work as a partner on continuous fine-tuning of the ruleset.
10	Vulnerability Assessment	Identify vulnerabilities and weaknesses in systems for remediation before threat actors can exploit the vulnerabilities
11	Threat Containment	SOC provides suggestions to customers on how to isolate suspicious activity
12	Threat hunting	Proactively reviewing events to detect malicious traffic
13	Deception programs	Formal actions taken to deceive attackers into performing actions that reveal location/intentions
14	DHS Cyber Hygiene	The Department of Homeland Security offers free “cyber hygiene” services to municipalities, state, and critical infrastructure.
15	Red team activities	Red Team activities within scoped rules of engagement

To address the Imperatives, SOC CCEs are encouraged to employ diverse students with some combination of the qualifications listed below as SOC employees:

Qualification	Description
Computer Networking	Understanding of how a collection of host computers work together with the sub-network or inter-network through which they can exchange data
Network Intrusions	An understanding of the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents.

Network Security	Understanding of how to protect information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity and availability
Operating Systems	An understanding of steps or measures used to protect the OS from threats, viruses, worms, malware or remote hacker intrusions
Information Assurance	An understanding of measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation
Cyber Ethics	An understanding of the code of responsible behavior on the internet
Cyber Adversary TTPs	An understanding of cyber adversary tactics, techniques, and procedures
Malware Techniques	An understanding of software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system (i.e., a virus, worm, Trojan Horse, or other code-based entity that infects a host)
Programming Languages (i.e. Python)	For example, Python
Systems Administration	Experience with the management, oversight and maintenance of a multiuser computing environment, such as a local area network (LAN)
Digital Forensics	An understanding of the application of computer science and investigative procedures involving the examination of digital evidence
Incident Response	An understanding of recommended practices for mitigating violations of security policies
Risk Management	An understanding of the process of managing risks to organizational operations, organizational assets, or individuals resulting from the operation of an information system
Non-Technical Criteria	Passion for Cybersecurity, willingness to learn, and teamwork skill

2.3 Cyber Range Facilities

A cyber range provides a safe place to allow training of personnel, testing of tools, and development of software, techniques, or hardware. The non-profit will manage a statewide cyber range contract with a vendor that offers cyber range services at the CCEs.

Range facilities can focus specifically on one customer sector or serve a combination of many types of customers, including: students in cybersecurity academic programs; adult learners transitioning careers; employees needing cybersecurity training, or specialized industry training for businesses needing credentials (i.e. defense). Range facilities will recruit and establish fee structures with their customers.

The statewide cyber range contract may provide the following services for Cyber Range facilities to offer to customers:

	Service Offered	Description	Customers (business, Municipalities, State Agencies, Academic K-12, Academic Colleges, military)
1	Experiential	Use of the facility to demonstrate the nature of threat activity and experience cybersecurity actions	Businesses, municipalities, Academic, Military, State Agencies
2	Certification of individual operators	A. Using range developed standards	Academic, Businesses, Municipalities, Military, State Agencies
		B. Using custom standards	Academic, Businesses, Municipalities, Military, State Agencies
3	Certification of team operators	A. Using range developed standards	Academic, Municipalities, Military, State Agencies
		B. Using custom standards	Academic, Municipalities, Military, State Agencies
4	Academic Credit	A. High School	Academic
		B. College or university	Academic
5	Network scenarios, malware, tools, and network configurations	A. Standard	Businesses, municipalities, Academic, Military, State Agencies
		B. Tailored	Businesses, municipalities, Academic, Military, State Agencies
6	Cyber Awareness Training	Offer cyber awareness trainings for users	Businesses, Municipalities, State Agencies
7	Competitions	Competitions, such as Capture the Flag, for individuals or teams	Businesses, Academic
8	Business Assessments	Conduct business assessments for third parties	Businesses, Municipalities

9	Business Development	Use by entrepreneurs to test their products	Businesses

2.4 Funding Eligibility

Respondents may be eligible to receive grant funding for the following capital and/or operational expenditures involved with operating a CCE, based on rationale presented in the response. Other expenditures not listed here may be considered.

	Expense	Description
Capital Expenditures	**Facility Renovation**	Remodeling of facility to code; electrical upgrades
	Cyber Suite Tenant Work	Design of Range/SOC area in facility/building; arrangement of rooms; internet connection and dimmable light
	Initial Equipment Investment	Computers, mobile devices, terminals, desks, chairs, monitors, tables, big screen TVs, rolling IT carts, video conferencing technology, printers
	Upfront Range Costs	Upfront setup costs for Range license (i.e. perimeter firewall, servers)
	Build Out Total	Dry wall to build private offices, conferences, classroom, kitchen
	Contingency (Design and Install)	Building code licenses; Architects; Designer to oversee contractor
Operational Expenditures	**CBT App**	Computer Based Training Application for Security Awareness Trainings
	Instructors	Coordinator or instructor for individual Range events; provided by license
	Trainers (Staff)	Extra trainers beyond what the Range/SOC license provides (i.e. faculty, grad assistants, interns)
	Staff Salaries	I.e. Range Manager, Business Development, and Tech Support
	Marketing	Expenses associated with advertising Range and SOC services to be expended by business development
	Occupancy Costs	Landlord fees, electrical, water, sewer, elevator, common area cleaning

	Communications Connectivity	Internet, VOIP
	Guest Network	Mobile, guests, IPTV, video conferencing
	Security	Secured and logged entry/exit
	Replacement Reserve Equipment	Costs to replace equipment over time (i.e. broken terminals, chairs, etc.)
	Consumables	Supplies
	Legal and Insurance	Legal and Insurance Fees

Note: CCEs are not eligible to receive funding for individual range licenses as the non-profit intends to negotiate a bundled license for the CCEs.

Initial Funding Eligibility

Since the Consortium is not yet fully established but there is an interest in initiating the establishment of one or more CCE's, grants may be awarded to support expenditures listed above to accelerate the commencement of operations at the proposed facility before it joins the Consortium as a CCE. Respondents may indicate in their response the immediate funding needs required to begin to establish and operationalize the proposed CCE before the Consortium is established.

3. SUBMISSION OF QUESTIONS AND RESPONSES

Questions regarding this RFR may be submitted by electronic mail to proposals@masstech.org. Please include the RFR number in the subject heading of the email.

Zoom Questions and Answers Call: To be held April 25, 2022

Please register:
https://us02web.zoom.us/meeting/register/tZEsdeGtrjMiHtYDkvl1a_eWnK7MYFTD_AHh

Additional Questions Due: April 26, 2022

Answers Posted: May 3, 2022

3.1 Instructions for Submission of Responses:

All Responses must be submitted electronically (.pdf or .doc) to proposals@masstech.org. Please state the following in the subject line: Proposal for Cybersecurity Centers of Excellence, RFR No. 2022 Cyber-02.

Responses received by Mass Tech Collaborative on or before March 18, 2022 at 3PM EST will be considered for round one funding. Responses received after March 18, 2022 and before May 20, 2022 at 3PM EST will be considered for round two funding. After the response deadline for each round, Mass Tech Collaborative will contact respondents to discuss their expression of interest and regarding potential grants requested to support capital and/or operating expenditures for CCEs based on their alignment with the imperatives, as well as other criteria listed in section 4. Grants may be awarded to begin programs at the proposed CCE before the Consortium is established.

3.2 Information Required in Submission:

Entities must include the following information in their response to be considered by Mass Tech Collaborative to become a CCE and receive funding support for capital and/or operational expenses (if requested).

(a) Response Cover Sheet (Attachment A)

(b) 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 CCE and becoming a member of the Massachusetts Cybersecurity Consortium;
- Identify individuals serving as project leads for the proposed CCE and their qualifications;
- Describe the organizational structure, including management and staffing, for the proposed CCE;

(c) CCE Overview

- Identify the type of CCE proposed (SOC facility, Range facility, or both);
- Describe the proposed CCE, including whether it will utilize an existing facility or require construction of a new facility;
- Provide a timeline for the opening of the CCE;

(d) Services

- *For Proposed SOC Facilities:* Describe how the proposed CCE would utilize a statewide MSSP license providing the SOC services listed in section 2.2;
- *For Proposed Range Facilities:* Describe how the proposed CCE would utilize a bundled statewide range license providing the Cyber Range services listed in section 2.3;

(e) Customers *(SOC Facilities)*

- List potential customers of SOC facility;
    i. *Optional:* Provide letters of support for any potential customers.
- Describe outreach plan to secure potential customers;

(f) Customers (*Range Facilities*)

- Identify potential users/operators of the proposed Range facility (students, employees, etc.), as well as their use cases and expected frequency of use;
- List potential customers of Range facility and identify which are potential customers versus committed customers;
    i. *Optional:* Provide letters of support for any potential or committed customers.
- Describe outreach plan to secure potential customers;

(g) Imperatives

- Identify how the proposed CCE would advance the imperatives of the Consortium (undersecurity, underemployment, employee training, business/economic development) or other needs of the Massachusetts cybersecurity ecosystem;
- *For Proposed SOC Facilities:* Provide an estimate for the number of students eligible to serve as employees of the SOC facility in the proposed CCE considering the SOC employee qualifications listed in section 2.2;
    i. Provide an estimate of the training cost per student.
- *For Proposed Range Facilities:* Quantify how many students and employees will be trained per year at the proposed Range facility;
    i. Provide an estimate of the training cost per student.

(h) Economic Model

- List expenses for the proposed CCE, including capital and operational expenses, for the first three years of operations;
- Identify existing sources of funding for the proposed CCE for the first three years of operations;
- Detail how the facility will become financially self-sustainable within three years;

(i) Funding Request *(Optional)*

To the extent the Respondent is ready to establish the CCE and begin to operationalize the plan provided in its submission, the Respondent may also submit a funding request:

- Describe additional funding the Respondent requires to establish the proposed CCE;
  i. Provide a list of expenses and totals.
- Provide a timeline for the expenditure of funds requested;
  ii. Identify any immediate funding needs required to establish operations at the proposed facility before the Consortium is operational.

4. EVALUATION PROCESS AND CRITERIA

The MassCyberCenter will employ evaluation criteria in determining which Respondents may become CCEs and be eligible to receive awards for capital and/or operational expenses. The criteria assessed may include, without limitation, the following:

- Alignment of proposed CCE with the Imperatives;
- Scale of impact of CCE on the cybersecurity workforce and resiliency in Massachusetts;
- Demonstrated experience of respondent in advancing cybersecurity resiliency and/or workforce development;
- Timeline for launch of proposed CCE and delivery of services to customers;
- Quantity of committed and/or potential customers (for Range facilities);
- Expressions of commitment to the proposed CCE by partners, especially academic partners, corporations, or community partners;
- Economic feasibility of proposed CCE 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. The Mass Tech Collaborative and the MassCyberCenter reserve the right to consider such other factors as they deem appropriate in order to identify potential CCEs.

5.0 GENERAL CONDITIONS

5.1 General Information

(a) All responses, proposals, related documentation and information submitted in response to this RFR are subject to the Massachusetts Public Records Law, M.G. L. c. 66, §10, and to M.G.L. c. 4, §7(26), regarding public access to such documents. Any statements reserving any confidentiality or privacy rights in submitted responses or statements otherwise inconsistent with these statutes will be void and disregarded. All materials and documentation submitted to MassTech in response to this RFR shall become MassTech property and may be subject to public disclosure under the Massachusetts Public Records Law.

(b) Further, any selected Respondent must recognize that in the performance of the Agreement it may become a holder of personal data (as defined in M.G.L. c. 66A) or other information deemed confidential by the Commonwealth. Respondent shall comply with the laws and regulations relating to confidentiality and privacy, including any rules or regulations of the Mass Tech Collaborative. Any questions concerning issues of confidentiality, the submission of materials to the Mass Tech Collaborative, or any other questions related to these matters, please contact Jennifer Saubermann, General Counsel, (saubermann@masstech.org) at MassTech.

(c) It is the policy of MassTech that contracts are awarded only to Respondents who fully conform to RFR requirements. In order to qualify as responsive, the Respondent must respond to all requirements of the RFR in a complete and thorough manner. Any response determined to be non-responsive to this RFR, including instructions governing the submission of responses, will be disqualified without evaluation subject to the right of MassTech to waive minor irregularities in responses submitted under the RFR and/or provide respondents with an opportunity to cure such minor irregularities.

(d) Respondent's submitted Response shall be treated by MassTech 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 rejection of the Response and/or of any resulting contract.

(e) MassTech will not be responsible for any costs or expenses incurred by Respondents in responding to this RFR.

(f) If MassTech determines that it is necessary to modify any part of this RFR, Respondents will receive an addendum by email. It is the responsibility of Respondents to review any addenda or modifications to a RFR to which they intend to respond. MassTech, the Commonwealth of Massachusetts, and its divisions accept no liability and will provide no accommodation to Respondents who submit a Response based on an out-of-date RFR.

ATTACHMENT A
Response Cover Sheet

Name of Respondent			
Mailing Address	City/Town	State	Zip Code
Telephone	Fax	Web Address	
Primary Contact for Clarification	Primary Contact E-mail Address		
Authorized Signatory	Authorized Signatory E-mail Address		
Legal Status/Jurisdiction (e.g., a Massachusetts corporation)	Respondents DUNS No.		
List category(s) of Services for which you wish to be considered.			

The undersigned is a duly authorized representative of the Respondent listed below. The Respondent has read and understands the RFR requirements.

I hereby certify that:

Respondent is in compliance with all corporate filing requirements and State tax laws.

The statements made in this Response to the RFR, 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

Optional Budget Template

See Excel Attachment