MASSACHUSETTS
TECHNOLOGY
COLLABORATIVE

Request for Proposals for RFP for Market Analysis on the Viable Alternatives and Launch Plan/Go-To-Market Strategy for potential statewide cyber range and security operations center facilities

RFP No. 2021-Cyber-02

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

Procurement Team Leader:	**Maxwell Fathy**
RFP Issued:	**July 2, 2021**
Questions Due:	**July 12, 2021**
Answers to Questions Posted:	**July 14, 2021**
Responses Due:	**July 19, 2021 by 3PM**

1. INTRODUCTION

1.1 Overview

Massachusetts Technology Collaborative ("Mass Tech Collaborative" or "MassTech"), on behalf of the MassCyberCenter is issuing this Request for Proposals for a **Market Analysis on the Viable Alternatives and Launch Plan/Go-To-Market Strategy for potential statewide cyber range and security operations center ("SOC") facilities** (RFP No.2021-Cyber-02) (the "RFP" or "RFP") to solicit responses from qualified contractors ("Respondents") with experience in **market analysis and understanding of cyber range and SOC service provider vendors**. Respondents will be competing against each other for selection to provide the services set forth herein (the "Services"). The submissions of all Respondents shall be compared and evaluated pursuant to the evaluation criteria set forth in this RFP, and a single Respondent may be selected.

Mass Tech Collaborative will be the contracting entity on behalf of MassCyberCenter for the purposes of this RFP, and (except where the specific context warrants otherwise), MassCyberCenter and Mass Tech Collaborative are collectively referred to as Mass Tech Collaborative or MassTech. Mass Tech Collaborative will enter into a Services Agreement and Statement of Work with selected Respondents containing certain standard provisions (the "Agreement"), located **HERE**.

1.2 Mass Tech Collaborative 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. For additional information about Mass Tech Collaborative and its programs and initiatives, please visit our website at www.masstech.org.

The MassCyberCenter ("Center") 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.

1.3 Potential Statewide Cyber Range and Security Operations Center Facilities

The Massachusetts cybersecurity ecosystem is facing challenges in four key areas: undersecurity, underemployment, employee training, and business development.

- **Undersecurity**: Organizations across the Commonwealth, especially municipalities 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. Colleges and universities could provide students with additional operational skills to secure entry level employment in the cybersecurity industry. Additionally, communities of color are underrepresented in the cybersecurity workforce and are frequently overlooked for employment due to a lack of experience.
- **Training**: Businesses across the Commonwealth do not have a location to send their employees to receive cybersecurity training at an affordable rate.

- **Business Development**: There is a need to convene regional hubs for business development where cybersecurity entrepreneurs can establish and grow startups.

To address these four challenges, the MassCyberCenter has convened a working group to assess the feasibility of implementing sustainable statewide cyber range and/or security operations center facilities. The working group assessment will be presented to the Secretary of Housing and Economic Development (EOHED) for the Commonwealth of Massachusetts.

2. SERVICES REQUIRED

2.1 Overview

The MassCyberCenter is seeking a consultant to conduct a market analysis on the Viable Alternatives and Launch Plan/Go-To-Market Strategy for statewide cybersecurity range and security operations center facilities. The selected Respondent will deliver a written summary of their findings as well as a presentation which summarizes the final report. The Center is seeking proposals for the Services described herein, for 1) **cyber range**: gap analysis of services; cost analysis; cyber range providers; customer demand; and go-to-market strategy; and 2) **security operations centers**: gap analysis of services; cost analysis; cyber range providers; customer demand; and go-to-market strategy. Both deliverables are described in more detail below. Applicants *must apply for and be capable of performing both market analysis for cyber range and SOC facilities*; incomplete applications applying for one portion of Services alone will not be considered. Applicants may meet the provider criteria by submitting applications that utilize a prime/subcontractor relationship.

2.2 Scope of Services

Applicants are required to describe their approach for the following Services. Additionally, Applicants are invited to propose alternative(s) which provide substantially better or more cost-effective performance than achievable under the stated RFP scope of services.

<u>Cyber Range</u>

The National Institute of Standards and Technology (“NIST”) defines cyber ranges as “interactive, simulated representations of local networks, systems, tools, and applications that are connected to a simulated Internet level environment. Cyber ranges provide safe, legal environments to gain hands-on cyber skills and a secure environment for product development and security posture testing. A cyber range may include actual hardware and software or may be a combination of actual and virtual components. The Internet level piece of the range environment includes not only simulated traffic, but also replicates network services such as webpages, browsers, and email as needed by the customer.”[1]

The potential statewide cyber range customers may include academic institutions (K-12 and institutions of higher education), businesses, municipalities, state agencies and military. For the purpose of the analysis, assume the potential cyber range facilities could provide customers with services established in Table 1.

Respondents will assess the cyber range providers in the Commonwealth of Massachusetts in the following areas:

1) *<u>Perform a gap analysis of range services:</u>* Identify companies or organizations currently in the market that provide the services that the potential statewide range(s) intends to provide. Additionally, identify the services that market competitors are not currently providing.
2) *<u>Perform a cost analysis for range services:</u>* Based on the list of services (provided below), perform a cost analysis of the services provided, in order to assess what is a typical range service provider fee structure or cost bases (i.e. cost per service or size of customer).

[1] https://www.nist.gov/system/files/documents/2018/02/13/cyber_ranges.pdf

3) *Identify range partners:* The analysis will assess which, if any, of the identified service providers/alternatives the range(s) could establish partnerships with.
4) *Assess customer demand for range services:* Municipalities, academic institutions, small and medium sized business (SMBs), the military, and state agencies are potential customers for range services. The analysis will determine whether these potential customers would subscribe to the range at a competitive or reduced cost.
5) *Go-To-Market Strategy for range*: The analysis will identify a Go-To-Market (GTM) strategy for engaging potential customers of the range(s). The GTM strategy will include recommendations for marketing the suggested services to meet the imperatives of the range(s) and suggestions to most effectively engage target customers to ensure maximum participation.

Table 1: Working Group's suggested cyber range services.

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

Security Operations Center (SOC)

Gartner defines a security operations center "…as a team, often operating in shifts around the clock, and a facility dedicated to and organized to prevent, detect, assess and respond to cybersecurity threats and incidents, and to fulfill and assess regulatory compliance."[2]

The potential statewide SOC(s) could address a key concern of undersecurity by providing cybersecurity services to municipal, academic, and non-profit clients at an affordable rate. In addition, to address the challenges of underemployment and training, college students, particularly those from underrepresented populations and communities of color, may staff the SOC as part time employees, working under the direction of private sector cybersecurity professionals, to gain the real world experience and hands-on cybersecurity skills not currently available through college training. The potential SOC will equip these students with skills enabling them to obtain a cybersecurity job, shrinking the talent gap, while raising the overall level of security in the Commonwealth. For the purpose of the analysis, assume the potential SOC would provide customers with services established in Table 2.

Respondents will assess the SOC service providers in the Commonwealth of Massachusetts in the following areas

1) *Perform a gap analysis of SOC services:* Identify companies or organizations currently in the market providing the services that the potential statewide SOC(s) intends to provide. Additionally, identify the services that market competitors are not currently providing.
2) *Perform a cost analysis for SOC services:* Based on the list of services (provided below), perform a cost analysis of the services provided, in order to assess what is a typical SOC service provider fee structure or cost bases (i.e. cost per service or size of customer).
3) *Identify SOC Partners:* The analysis will assess which, if any, of the identified market competitors/alternatives the SOC(s) could establish partnerships with.
4) *Assess customer demand for SOC services:* Municipalities, academic institutions, and nonprofit organizations are potential customers for SOC services. The analysis will determine whether these potential customers would subscribe to the SOC services at a free or low cost. The analysis will also determine whether customers would subscribe to the SOC based on different possible operating hours, including: 24 hours per day, 7 days per week; 10 hours per day, 7 days per week; and 10 hours per day, 7 days per week with on call service when the SOC is not staffed.
5) *Go-To-Market Strategy for SOC*: The analysis will identify a Go-To-Market (GTM) strategy for engaging potential customers of the SOC(s). The GTM strategy will include how the suggested services can be marketed to meet the imperatives of the SOC(s) and how to most effectively engage target customers to ensure that they subscribe.

Table 2: Working Group's suggested SOC services.

	Service Offered	**Description**	**Customers (Academic – Higher Ed, Municipalities, Non-Profits)***	**Phase Offered**
1	Threat Sharing	The SOC shares center's threat alerts with customers	All customer types	1
2	Cyber Advisories	Sharing third party threat alerts with customers	All customer types	1
3	Ongoing threat monitoring	Ongoing threat monitoring, initial triage and investigation, and notification to customer to investigate	All customer types	1

[2] https://www.gartner.com/en/newsroom/press-releases/2017-10-12-security-operations-centers-and-their-role-in-cybersecurity

4	Notification to customer to investigate	Additional incident investigation provided to customer	All customer types	1
5	Threat Containment	SOC provides suggestions to customers on how to isolate suspicious activity	All customer types	1
6	Threat hunting	Proactively reviewing events to detect malicious traffic	All customer types	1
7	Monitoring phishing submissions	Customers can send reported phishing messages for further analysis by a SOC Team	All customer types	1
8	Monitor internet accessible services	Customers with internet accessible services can rely on the SOC to look for risky services and make recommendations	All customer types	1
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.	All customer types	1
10	Vulnerability Assessment	Identify vulnerabilities and weaknesses in systems for remediation before threat actors can exploit the vulnerabilities	All customer types	1
11	Cybersecurity Assessment	Perform cybersecurity assessments using various controls frameworks to identify opportunities to bolster cyber defenses	All customer types	1
12	Security Awareness Training	Work with customer to raise awareness of cybersecurity threats.	All customer types	1
13	Deception programs	Formal actions taken to deceive attackers into performing actions that reveal location/intentions	All customer types	2
14	DHS Cyber Hygiene	The Department of Homeland Security offers free “cyber hygiene” services to municipalities, state, and critical infrastructure.	All customer types	2
15	Red team activities	Red Team activities within scoped rules of engagement	All customer types	2

**state agencies may contract for SOC services by exception*

<u>Additional insights:</u>

The analysis will provide any additional insights concerning the creation of statewide range(s) and

SOC(s).

Work schedule:

The vendor should submit a proposed schedule for the study, assuming a 2 August 2021 start date.

3 APPLICATION PROCESS

3.1 Application and Submission Instructions

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

a. All Applications must be submitted electronically.
b. Required Submissions- All Applications must include the items listed below:

- Application Cover Sheet (Attachment A)

- Application, which shall include:

  - A description of the firm responding to the RFP (including descriptions of proposed subcontractors, if any) and the firm's qualifications to perform the Services including sufficient information to evaluate the criteria set forth in section 4.2 below.
  - The proposed approach to providing the Services. Additionally, Respondents are invited to propose alternative(s) which provide substantially better or more cost-effective performance than achievable under the stated RFP scope of services.
  - Provide the total not-to-exceed costs for providing the Services based on projected hours, proposed hourly rates, as well as any other appropriate costs, in the Budget Template (Attachment C). 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. The Mass Tech Collaborative also does not pay for word processing, overtime or meals. For travel costs, the Mass Tech Collaborative pays the IRS rate per mile.
  - Three references for work previously performed by the Respondent that is substantially similar to the Services. References should include a contact person, address and phone number.

- Authorized Application Signature and Acceptance Form (Attachment B). **By executing the Authorized Respondent's Signature and Acceptance Form and submitting a response to this RFP, Respondents certify that they (1) are in compliance with the terms, conditions and specifications contained in this RFP, (2) acknowledge and understand the procedures for handling materials submitted to the Mass Tech Collaborative as set forth in subsection d. 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 RFP or upon the Respondent's selection.**

- Exceptions to the *Services Agreement and Statement of Work*, located at **HERE**, if any.

c. Applications must be submitted to proposals@masstech.org (please include the RFP number in the subject heading).

d. Any and all responses, Applications, data, materials, information and documentation submitted to Mass Tech Collaborative in response to this RFP 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 4.2 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 and **shall only include the confidential material in the hard copy of 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:**
RFP Released	July 2, 2021
Questions Due	July 12, 2021 **@ 5 PM EST**
Question and Answer File Posted	July 14, 2021 **@ 5 PM EST**
Applications Due	July 19, 2021 **@ 3 PM EST**

3.3 Questions

Questions regarding this RFP must be submitted by electronic mail to proposals@masstech.org with the following Subject Line: "Questions – RFP No. 2021-Cyber-02"). All questions must be received by 5:00 p.m. EST on July 12, 2021. Responses to all questions received will be posted on or before 5:00 p.m. on July 14, 2021 to Mass Tech Collaborative and Comm-Buys website(s).

4 EVALUATION PROCESS AND CRITERIA

4.1 Process

The Mass Tech Collaborative shall evaluate each Application that is properly submitted. As part of the selection process, Mass Tech Collaborative may invite finalists 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 one or more finalist Respondent(s) and then ask the Respondent(s) to submit a best and final offer.

4.2 Criteria

Selection of a Respondent to provide the services sought herein may be based on criteria that include but are not limited to:

- Familiarity with cybersecurity services industry in Massachusetts;
- Demonstrated experience analyzing ecosystems;

- Familiarity with cyber ranges and Security Operations Centers;
- Interaction with municipalities and academic programs is a plus;
- Ability to provide actionable recommendations to support a determination around the feasibility of a statewide SOC/range with a combination of state/federal/philanthropic/and fee based customers;
- Familiarity of technologies involved with SOC and Range;
- Examples of previous market analyses;
- Clarity of, and thought put in, the application;
- Quality of suggested approach on how the analysis will be conducted;
- Demonstrated ability to provide depth and breadth of information in a timely manner; and
- Overall pricing and rates proposed.

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 RFP is to select and enter into an Agreement with the Respondent that will provide the best value for the Services to achieve MassTech Collaborative's goals. Mass Tech Collaborative reserves the right to consider such other relevant factors as it deems appropriate in order to obtain the "best value."

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 RFP, 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 for services pursuant to this RFP, or pay any costs incurred in responding to this RFP. Mass Tech Collaborative reserves the right, in its sole discretion, to withdraw the RFP, 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, all to the same extent as if this were a Request for Information.

c) On matters related solely to this RFP 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 RFP. Respondents may contact the Procurement Team Leader for this RFP in the event this RFP 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 RFP.

g) Mass Tech Collaborative’s prior approval is required for any subcontracted services under any Agreement entered into as a result of this RFP. 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 RFP

This RFP 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 RFP, 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, MassCyberCenter and COMMBUYS websites for any addenda or modifications to the RFP. The Mass Tech Collaborative accepts no liability and will provide no accommodation to Respondents who submit a response based on an out-of-date RFP.

Attachment A
Application 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, LLC, LLP, etc.)	Respondents DUNS No.		

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 RFP requirements. The Respondent acknowledges that all of the terms and conditions of the RFP 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 Agreement; 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 bid 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 RFP, 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 EXCEL SPREADSHEET