Request for Proposals for Cyber Range Services

RFP No. 2022-Cyber-03

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

Procurement Team Leader:	**Maxwell Fathy**
RFP Issued:	**3/29/2022**
Bidders' Q&A Zoom Call:	**4/14/2022 1PM EST**
Questions Due:	**4/15/2022**
Answers to Questions Posted:	**4/22/2022**
Responses Due:	**5/6/2022 by 3PM EST**

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 **Cyber Range Services** (RFP No.2022-Cyber-03) (the "RFP" or "RFP"). This RFP solicits responses from qualified vendors ("Respondents") to provide virtual cyber range services to Cybersecurity Centers of Excellence in the Massachusetts Cybersecurity Consortium. 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 the MassCyberCenter and potential CCEs 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, a division of MassTech, seeks 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 Overview of the Massachusetts Cybersecurity Consortium

The MassCyberCenter is supporting efforts to establish 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, Security Operations Center ("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 establish guidelines to advance the imperatives, support educational programs, advocate to public and private stakeholders, and allocate financial resources. Mass Tech Collaborative is currently supporting the establishment of the Consortium and the non-profit organization and has issued a Request for Proposals (RFP) for a Consultant to Establish the Massachusetts Cybersecurity Consortium Non-Profit (RFP No. 2022-Cyber-01).

Facilities offering SOC services, Cyber Range services, or both will be designated as "Cybersecurity Centers of Excellence" or "CCEs." The MassCyberCenter may support SOC and Cyber Range facilities who will become members of the Consortium as CCEs and has issued a Request for Responses (RFR) seeking expressions of interest and qualification from entities interested in establishing a Cyber Range facility and becoming a CCE as part of the Massachusetts Cybersecurity Consortium (RPR No. 2022-Cyber-02). Since there are several entities who have expressed interest in establishing a Cyber Range facility, MassCyberCenter is issuing this RFP to be able to provide cyber range services through the CCEs in advance of the establishment of the non-profit and Consortium.

2. SERVICES REQUIRED

2.1 Overview

A cyber range provides a safe place to allow training of personnel, testing of tools, and development of software, techniques, or hardware. As a membership benefit of the Massachusetts Cybersecurity Consortium, the non-profit is expected to manage a bundled cyber range license and make cyber range services available to the Consortium's Range CCEs. This RFP will establish a contract for the interim period between MassCyberCenter and a cyber range vendor in order to accelerate the establishment of Range CCEs.

Range CCEs 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 CCEs will recruit and establish fee structures with their customers.

While the Consortium is not yet fully established, there is an active interest in establishing range facilities now. Mass Tech Collaborative is issuing this RFP for a cyber range services vendor and will negotiate a contract with the selected respondent to provide range services to one or more of the future Consortium's Range CCEs. The contract may be assigned by MassTech to the new non-profit after its establishment.

2.2 Scope of Services

MassTech is seeking responses from Respondents able to provide the following services at each Range CCE for their customers:

	Service Offered	Description	Customers (business, Municipalities, State Agencies, Academic K-12, Academic Colleges, military)	Required vs. Preferred
1	Experiential	Use of the facility to demonstrate the nature of threat activity and experience cybersecurity actions	Businesses, municipalities, Academic, Military, State Agencies	Required
2	Certification of individual operators	A. Using range developed standards	Academic, Businesses, Municipalities, Military, State Agencies	Required
		B. Using custom standards	Academic, Businesses, Municipalities, Military, State Agencies	Required
3	Certification of team operators	A. Using range developed standards	Academic, Municipalities, Military, State Agencies	Required
		B. Using custom standards	Academic, Municipalities, Military, State Agencies	Required
4	Academic Credit	A. High School	Academic	Required
		B. College or university	Academic	Required
5	Network scenarios, malware, tools, and network configurations	A. Standard	Businesses, municipalities, Academic, Military, State Agencies	Required
		B. Tailored	Businesses, municipalities, Academic, Military, State Agencies	Required

6	Cyber Awareness Training	Offer cyber awareness trainings for users	Businesses, Municipalities, State Agencies	Required
7	Competitions	Competitions, such as Capture the Flag, for individuals or teams	Businesses, Academic	Preferred
8	Business Assessments	Conduct business assessments for third parties	Businesses, Municipalities	Preferred
9	Business Development	Use by entrepreneurs to test their products	Businesses	Preferred

Cyber range content should be inclusive of both scenarios and labs. Scenarios are prebuilt content designed to simulate both offensive and defensive enterprise security operations for information technology and operational technology using industry recognized tools and infrastructure. Labs are defined as self-paced individual experiences focusing on specific learning objectives.

In addition to offering the services listed above, the vendor is expected to submit proposals that consider the following requirements:

- Pre-packaged content ready to be integrated into curriculum for key cybersecurity topics including, but not limited to, cryptography, network security, computer security, software security, offensive security, defensive security, digital forensics on network traffic and digital devices, and incident response.
- Scenarios which support municipal cybersecurity are a high priority. These scenarios could promote general cybersecurity awareness, incident response across local government or team training events focused on emergency services, schools, or utilities are a special interest for this RFP.
- Cyber range exercises must vary in length and complexity as to be suited for different audiences and skill levels.
- Provides support for faculty and/or instructors to use the scenarios and labs. This may include faculty/instructor guides or other documentation for each scenario or lab which should include learning objectives, study questions, and sample quizzes.
- Capability to have concurrent range scenarios and/or labs running at any given time at one facility or across multiple facilities.
- Allows participants on-premises and remote to access any given scenario and labs simultaneously.
- Labs and scenarios are aligned with the current standards (i.e. National Initiative for Cybersecurity Education (NICE) Workforce Framework, MITRE ATT&CK, and National Security Agency Center of Academic Excellence (CAE) Knowledge Units (KUs) including CAE-CD 2020 KUs and CAE-CO 2021 KUs).
- Provides training and support for range administrators.
- Ability to provide range participants with overviews of the range scenarios and labs and formal performance feedback, including correct answers and hints at the conclusion of range scenarios and labs.
- Provides instrumentation for individual and team performance assessments.

- Ability for the cyber range to integrate with learning management systems.

The following requirements are preferred:

- A cloud hosted cyber range and not an on-premises deployment. Bidders may offer a hybrid model in their response for consideration.
- Capability to develop custom content.
- Ability for faculty/instructors to tailor content to meet the needs of curriculum development.
- Ability to add new content in the future, as well as an ability to collaborate with selected faculty/instructors to build new content.

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. Required Submissions- All Applications must include the items listed below:

- Application Cover Sheet (Attachment A)
- Application, which shall include:
    - A cover letter describing the Respondent and their qualifications to perform the Scope of Services, including any experience providing these services to academic or public sector institutions;
    - Bios and resumes for all individuals associated with the Respondent providing the services;
    - **Services**
        a. Describe which of the services listed in section 2.2 the Respondent's range solution is capable of providing to customers and the proposed approach to providing them in alignment with this RFP.
        b. Describe any capabilities the range has for assisting in achieving compliance with the Cybersecurity Maturity Model Certification (CMMC) or other industry certifications.
    - **Pre-Packaged Content Overview, including Scenarios and Labs**
        a. Describe the cybersecurity topics addressed in the range's content (i.e. cryptography, network security, computer security, etc.).
        b. Provide a catalogue which includes a complete list and description of cyber range scenarios, labs, including the required software and hardware specifications needed to run each scenario or lab. The descriptions of scenarios and labs should include any student pre-requisites or skills necessary for the scenario and lab along with detailed information, such as background information of involved topics, overview of project structure, connection of different components, referenced solutions, maximum number of students at one time, etc.
        c. Describe how cyber range exercises varying in length and complexity to be suited for different audiences and skill levels are supported.

d. Specify licensing model for scenarios and labs, including those that are in high-demand.
e. Specify release cadence for new content (i.e. release frequency of new scenarios and labs).
f. Describe the alignment of scenarios and labs with recognized industry standards (i.e. NICE Framework, MITRE ATT&CK, and CAE KUs including CAE-CD 2020 KUs and CAE-CO 2021 KUs, etc.).
g. Describe support the Respondent provides to faculty/instructors for use of the scenarios and labs.
h. Describe efforts and processes for growing the Range Learning Management System to account for changes in cybersecurity training, education, and workforce development.

- **Customizable Content**
  a. Describe the ability of faculty/instructors to tailor content to meet the needs of curriculum development.
  b. Articulate the technical requirements and qualifications of range administrators to create and develop custom content for the range.
  c. Address the possibility of collaborating with faculty/instructors to build new content, its procedures, the expected cost, and the copyright issue of the content.
  d. Outline the application levels on top of the basic Range Learning Management System bring together the technology and service components of the Cyber Range.
- **Assessments**
  a. Identify capabilities to provide range participants with overviews of the range scenarios and labs.
  b. Describe how formal performance feedback is provided to range participants, including correct answers and hints at the conclusion of range scenarios and labs.
  c. Identify instrumentation the range provides for individual and team performance assessments.
- **Technical Requirements**
  a. Identify whether the cyber range services are cloud hosted or requires an on-premises deployment, or whether the cyber range can offer a hybrid cloud/on-premise deployment.
     i. Note any equipment required for services that must be accessed on-premises. maintenance orquipment, software,
  b. Specify all technical requirements for an individual to participate in range activities (i.e. workstation requirements, applications, protocols, etc.).
  c. Indicate whether the range can support participants in each of the following settings:
     i. On-premises (i.e. in a classroom at the range facility).
     ii. Remote (i.e. students who are not physically located at the range facility).
     iii. On-premises and remote (i.e. simulaneously supporting students on premise and students who are remote).
  d. Articulate any limits on the number of simultaneous participants in any given scenario or lab activity.
  e. Convey the total capacity in terms of concurrent range scenarios and/or labs running at any given time. For example, can the range run two different scenarios with different populations of students concurrently?

f. Describe the cyber range's ability to integrate with learning management systems.

- **Technical Support**
  a. Document methods for technical support and guidance for faculty/instructors and range participants.
     i. Specify the time to resolve issues once the range vendor is notified.
  b. Describe how the Respondent will provide training and support for range administrators.
- **Range Implementation**
  a. Provide a project plan and proposed timetable outlining the methodology to go-live with the cyber range at two or more Range CCEs on September 1, 2022 *(note: this date is subject to change).*
  b. Identify and articulate all technical requirements for the implementation of the range at Range CCEs.
  c. Provide clearly established timelines, milestones, and resource requirements for a range facility to implement the range.
- **Pricing**
  a. Provide a detailed breakdown of costs necessary to complete the Scope of Services per facility.
     i. Include a cost structure for each service requested in the table in section 2.2. If possible, provide the cost per service requested.
     ii. Pricing for services provided shall be detailed by implementation fees, integration fees, annual license fees, software fees, hardware costs, equipment, consulting fees, and estimated travel costs.
     iii. Provide pricing estimates for 2-4 facilities and 5-6 facilities for a contract lasting 12-18 months.
  b. Provide a pricing and contracting structure that allows Range CCEs to have access to the Range's services. Explain how the number of facilities utilizing the Range contract affects the per facility and total cost of the contract.
  c. Pricing should include any discounts provided to public sector or educational clients.
  d. Specify cost to add new content, such as scenarios or labs, in the future.
  e. If sub-contracting support services, provide names and address of all sub-contractors, the services that they will be providing, their qualifications and expertise in providing such services, and the expected amount of money each will receive.
  f. If there are other fees, costs, or billable expenses associated with the execution of this project, please describe in detail, and list the costs.
- **Samples**
  a. Submit samples of student feedback, assessments, faculty guides and if available, video examples of a scenario and student interaction.
- **References**
  a. Provide three references—one business, one academic, and a third of the vendor's choice—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 c. 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.

- Respondents must indicate whether they are willing to enter into an agreement to provide range services that is assignable to another entity.

- Please include and explain any additional information that is not requested in this Request for Proposals that would assist the Mass Tech Collaborative in evaluating the proposal.

b. Applications **must** be delivered as follows:

Electronic version submitted to-

proposals@masstech.org (please include the RFP number in the subject heading).

c. 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	**3/29/2022**
Bidders' Q&A Zoom Call	**4/14/2022 @ 1PM EST**
Questions Due	**4/15/2022 @ 5 PM EST**
Question and Answer File Posted	**4/22/2022 @ 5 PM EST**
Applications Due	**5/6/2022 @ 3 PM EST**

3.3 Questions

Written questions regarding this RFP must be submitted by electronic mail to proposals@masstech.org with the following Subject Line: "Questions – RFP No. 2022-Cyber-03". All questions must be received by 5:00 p.m. EST on 4/15/2022. Responses to all questions received will be posted on or before 5:00 p.m. on 4/22/2022 to Mass Tech Collaborative and Comm-Buys website(s).

3.4 Bidders' Q&A Zoom Call

A bidders' Zoom call will be held on 4/14/2022 at 1PM EST to give potential respondents an opportunity to ask members of the Mass Tech Collaborative team questions about this RFP. All potential Respondents interested in participating in the bidders' Zoom call must register here in order to obtain the call information. Mass Tech Collaborative will post summary responses to procedural questions and issues addressed at the bidders' call on the Mass Tech Collaborative's and the Comm-Buys websites.

4 EVALUATION PROCESS AND CRITERIA

4.1 Process

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:

- Quality of proposal and services offered;
- Thoroughness of project plan, methodology and timeliness for Range implementation;
- Alignment of proposal with requirements listed in Section 2.2;
- Pricing;
- Ability to meet the proposed timeline of going live with the cyber range at two or more Range CCEs on September 1, 2022, as well as accelerated schedules;
- Scalability to multiple Range CCEs;
- Performance with existing clients based upon References;
- Experience providing cyber range solutions to academic and public sector institutions;
- Ability to integrate with CCEs; and
- Quality of samples provided by Respondent.

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 Services 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: _____