Administration and Finance

Information and Technology Service

REQUEST FOR PROPOSALS

For

CYBERSECURITY ASSESSMENT AND PLAN

Timeline	
Wednesday, March 17, 2021 by 5:00 PM EST	RFP announcement in The Boston Globe
Friday, March 19, 2021 by 5:00 PM EST	RFP available online at www.bphc.org/RFP at 5:00 PM EST
Friday, April 2, 2021 by 5:00 PM EST	Questions about the RFP via email to: Jeffrey Beers Director of Technology Services JBeers@BPHC.org Subject Title: RFP Questions - Cybersecurity Risk Assessment and Plan
Friday, April 9, 2021 by 5:00 PM EST	Response to questions posted at www.bphc.org/RFP by 5:00 PM EST
Friday, April 23, 2021 by 5:00 PM EST	Submit response via email to: Jeffrey Beers Director of Technology Services JBeers@BPHC.org Subject Title: RFP Submission – Cybersecurity Risk Assessment and Plan

PLEASE SUBMIT ALL CORRESPONDENCE AND PROPOSALS
VIA E-MAIL DIRECTLY TO THE PROCUREMENT CONTACT LISTED ABOVE AND
INCLUDE 'IT CYBERSECURITY ASSESSMENT AND PLAN' IN THE SUBJECT LINE

The Boston Public Health Commission is soliciting proposals from firms for the provision of a comprehensive IT cybersecurity vulnerability assessment and plan.

A. BACKGROUND

The Boston Public Health Commission is looking to Improve Critical Infrastructure Cybersecurity and would like to take steps to enhance cybersecurity in BPHC facilities. These initiatives will greatly enhance the security and resiliency of this vitally important sector. Cybersecurity has been identified as a top priority for the Information Technology Services Department, which has responsibility for the Boston Public Health Commission.

This RFP establishes the terms, conditions, assurances, and certifications under which the Information Technology Services Department is seeking services under the Boston Public Health Commission. The Boston Public Health Commission is designated as a body politic and corporate and political subdivision of the Commonwealth and are subject to the Massachusetts Public Records Law and the designation of Health Insurance Portability and Accountability Act (HIPAA).

The Boston Public Health Commission (BPHC) is the local public health department for the City of Boston. BPHC's mission is to protect, preserve, and promote the health and well-being of all Boston residents, particularly the most vulnerable. To learn more about the Boston Public Health Commission, visit www.bphc.org.

The Information Technology Services Department maintains several enterprise and departmental software applications and platforms managed in-house, on premise, and in-cloud. The Information Technology Services Department manages these applications on Microsoft Windows servers and Microsoft SQL databases. The Information Technology Services Department also maintains enterprise class information technology infrastructure. The Information Technology Services Department has an in-house technical, functional, and business process staff.

The Boston Public Health Commission do intend to undertake a Cybersecurity Risk Assessment that will identify vulnerabilities in its information technology infrastructure, systems, policies and practices, and develop a prioritized plan to mitigate the risks identified. The Vulnerability Risk Assessment will utilize industry best practice methodologies to ensure a standardized risk mitigation approach that will offer the highest risk reduction potential.

The Boston Public Health Commission anticipates awarding a single contract to the selected vendor. The period of performance will be from the date of execution of a contract through June 31, 2021. All work must be completed by this date and final invoice must be submitted by 06/31/2021. The estimated cost to perform the work is between $50,000.00 to $80,000.00. The contract will include a Business Associate Agreement (HIPAA) (Exhibit A of Attachment B). Exhibit A must be signed by the same individual signing the contract for the selected firm.

The Boston Public Health Commission's Contract Terms and Conditions are included as Attachment B to this RFP. By submitting a Proposal, the Proposer represents that it has carefully read and agrees to be bound by the Boston Public Health Commission's Contract Terms and Conditions. Identify during the question submittal and response period, any sections you consider onerous, clarify why you consider these sections onerous, propose alternative language and describe why it is in the Boston Public Health Commission's best interests to adopt the alternative language. Conditioned proposals will be considered nonresponsive and will not be evaluated.

B. SCOPE OF SERVICES:

The Boston Public Health Commission will select a qualified certified security professional on a best value basis using a point-method of award, to undertake a comprehensive IT Cybersecurity Risk Assessment and Plan, thoroughly reviewing the current state of the Boston Public Health Commission's information technology security, develop a vulnerability plan, and prioritized road map of activities to enhance the Boston Public Health Commission's future Cybersecurity position.

The consultant's approach will utilize industry best practice methodologies to ensure a standardized risk mitigation approach that will offer the highest risk reduction potential. The approach will complement the 'Framework for Improving Critical Infrastructure Cybersecurity' developed by the National Institute for Standards and Technology (NIST) in response to Presidential ExecutiveOrder13636 (attached). Additionally, the approach shall consider the OpSec (Operations Security) Five Step Process (http://www.opsecprofessionals.org/process.html) as it pertains to Cybersecurity.

The assessment is to include, but not be limited to:

a) Review existing security as it relates to Advanced Persistent Threats (APTs) such as viruses, malware, Trojan horses, botnets and other targeted attack exploits. Evaluate the Boston Public Health Commission's current threat posture including antivirus and Intrusion Detection and Prevention (IDP) capabilities.
b) Review wireless network system components for security vulnerabilities, validating system-specific configurations and known exploits.
c) Review system-specific configurations and review for known exploits. This includes firewalls, switches and routers, Microsoft Active Directory, email and file servers, web servers, wireless routers, VPN, VoIP and CCTV systems.
d) Assess VoIP network system components for security vulnerabilities, validating system-specific configurations and reviewing for known exploits.
e) Review existing IT policies and procedures and make recommendations for changes and/or additional policy and procedure development.

The overall engagement will be managed by the vendor, with a defined scope, schedule and budget. Project activities will be appropriately managed, and project risks and task progress will be formally communicated. The Boston Public Health Commission will assign a Project Manager to act as a focal point for vendor communications.

Services will be provided at the Boston Public Health Commission's direction and discretion and may be provided in collaboration with ITS Department staff or third-party support vendors. Services may be provided onsite or remotely, at the Boston Public Health Commission's discretion.

C. DELIVERABLES:

Deliverables will include:

System Security Plan (SSP): Establishes the desired security state (target profile) of the business. The target profile aligns with the NIST Cybersecurity Framework and is based on CIS Critical Security Controls. The target profile identifies the desired cybersecurity outcomes of organization.

Cyber Risk Assessment: Identifies the current security state of the business (current profile) based on alignment with the NIST Cybersecurity Framework and CIS Controls. The Risk Assessment results indicate which outcomes from the SSP are currently being achieved.

Gap Analysis / Plan of Action and Milestones (POA&M): The current profile and the target profile are compared to determine gaps. Based on the gaps identified, a prioritized action plan is developed to address the gaps. The action plan includes the resources necessary to address the gaps.

The Gap Analysis / Plan of Action and Milestones (POA&M) includes:

- Weaknesses or deficiencies in deployed security controls and source of the identified weakness
- Severity of the identified security control weaknesses or deficiencies
- Scope or affected assets of the weakness in components within the environment.
- Proposed risk mitigation approach to address the identified weaknesses or deficiencies in the security control implementations (e.g., prioritization of risk mitigation actions and allocation of risk mitigation resources).

Cybersecurity Program Executive Report: Establishes a baseline of the current and desired cybersecurity program maturity. Highlights the strengths, weaknesses, and overall maturity of the BPHC cybersecurity program.

Project Management Deliverables: Work Breakdown Schedule (WBS) including tasks, schedule and dependencies; Weekly Status Reports including risks and progress reports.

D. RFP ELEMENTS & EVALUATION CRITERIA:

Proposals should present information in a straightforward and concise manner, while ensuring complete and detailed descriptions of the Firm's/Team's abilities to meet the requirement of this RFP. Emphasis will be on completeness of content. The written proposals should be prepared in the sequential order as outlined below.

Proposals are limited to 12 numbered pages (8 ½ by 11 inch) **including** the cover letter and all appendices. All pages shall be in portrait orientation with 1-inch margins. Font size shall be 11 point or larger. Proposals that do not follow this format will not be reviewed.

The cover letter shall include the RFP Title and Number, Name, Title, Email Address, Phone Number and Addresses of the Proposing Team's main contact and include the following information:

- Describe any claim submitted by any client against the firm within the past two years related to the services provided by the firm or its key personnel. For purposes of this request, "claim" means a sum of money in dispute in excess of 5% of the firm's fee for the services provided.
- Any real or perceived conflicts of interests for team members, inclusive of the prime, sub-consultants and key team members.

Proposals are to address, and will be evaluated upon, the following criteria:

INITIAL EVALUATION PHASE

1. Qualifications & Experience 40 PTS

   - Describe, in detail, the history of the firm submitting the proposal, including: length of time in business; business history including patterns of growth, mergers or acquisitions; number of staff; number of customers; market/vertical specializations; office locations; length of time offering services similar to those proposed; etc.
   - Describe, in detail, the experience and qualifications of the Consultants proposed to work on this project, including relevant certifications, length of time working in a cybersecurity field, areas of specialization, experience with the Boston Public Health Commission's preferred methodologies, etc.

2. Proposed Approach 40 PTS

   - Describe in detail the approach proposed to undertake the project, including proposed best practice methodologies, scorecard measurement methodologies, proposed areas of focus, proposed tools, etc.
   - Provide detailed descriptions of three recently completed projects similar in scope to the Boston Public Health Commission's project, including a definition of the projects' goals, scope, deliverables, cost and success.

3. Work Approach 20 PTS

   - Assumptions and Risks: Define the assumptions made regarding accomplishing the Scope of Services. Define the factors the consultant believes are risks to the successful completion of the project and proposed mitigation strategies. Describe any factors that that you believe may constrain your firm's ability to undertake the scope of work described.
   - Innovative Ideas: Include a summary of innovative ideas and suggestions for enhancing the scope of services
   - Coordination & Communication: Provide a plan for communications and coordination between the Consultants team and the Information Technology Services Department staff.
   - Project Management: Describe the consultants experience in the formal project management of projects such as that defined in this RFP.

Failure to discuss the following items with some detail will result in a Proposer's response being determined as NOT RESPONSIVE. This item will not be included in the scoring evaluation of the Proposer's response.

   - Work Location: Describe the consultants' considerations for onsite or remote access performance of project tasks.

4. Compensation 20 PTS

Compensation information MUST be provided separately from the proposal, in an individual PDF document.

   - Include on the Rate Sheet (Attachment C) the labor category and hourly rate of each member of the proposed team, or of each specific project role.

All rates and costs/fees quoted shall be:

   - **Fully burdened, including, but not limited to, per diem, administrative overhead, travel, lodging, and transportation (all direct/indirect expenses included);**
   - Quoted in US Dollars.

- Full cost inclusive; and
- Valid throughout the contract period unless otherwise amended and agreed to by both parties in writing.

5. References ..... 20 PTS

Ensure completion of a **minimum of 3 references** submitted using Attachment D. All references must be received by the Boston Public Health Commission by the Proposal due date. The Boston Public Health Commission will evaluate the reference checks to assess the proposed team's overall performance and success of previous, similar work. Reference checks will also be utilized to validate information contained in the proposal. The Boston Public Health Commission may contact submitted reference sites directly to accomplish this.

FINAL EVALUATION PHASE (if applicable)

6. Interviews 100 PTS

If an award is not made based on the written evaluations alone, interviews will be conducted with the three top-ranked proposers. Failure to participate in the interview process will result in the Proposer's disqualification from further consideration. If interviews and software demonstrations are conducted, they will be held at the Boston Public Health Commission, Boston, MA. Travel costs will not be reimbursed for the interview. Interviews may be conducted via video conferencing at the Boston Public Health Commission's discretion.

ATTACHMENT A – INSTRUCTIONS FOR PROPOSING

ATTACHMENT B – STANDARD CONTRACT/TERMS AND CONDITIONS

ATTACHMENT C – RATE SHEET

ATTACHMENT D – REFERENCE QUESTIONAIRE

ATTACHMENT A – INSTRUCTIONS FOR PROPOSING

All status updates on the solicitation timeline will be announced on the Boston Public Health Commission's website for this solicitation.

VENDOR OBLIGATION

Boston Public Health Commission Requests for Bids, Requests for Proposals and Requests for Qualifications can be accessed on the Boston Public Health Commission's website, www.bphc.org under 'RFPs and BIDS'.

COMMUNICATION / INQUIRES

Proposers who, relative to this scope of services, contact any individuals or Commission members representing the Boston Public Health Commission, other than the Procurement Representative listed on the RFP shall be disqualified from consideration.

Written questions about the meaning or intent of the Solicitation Documents shall only be submitted to the Information Technology Services Department, jbeers@bphc.org ("**XXXXX Information Technology Cybersecurity Assessment and Plan"** in the subject line)

Proposers who may have questions about provisions of these documents are to email their questions by the date listed above. The ITS Department staff will respond to all written questions submitted by this deadline.

ADDENDA

The Boston Public Health Commission may make changes to this Solicitation. Oral or other interpretations, clarifications or submittal instructions will be without legal effect. Any information modifying a solicitation will be furnished in a formal, written addendum. Addenda will be posted to the Boston Public Health Commission's web site and conveyed to those potential submitters.

PRE-PROPOSAL CONFERENCE

The Boston Public Health Commission will not conduct a pre-proposal conference for this procurement. To obtain answers to any questions or for further clarifications, submit all questions as noted above.

SUBMITTAL PROCESS

Proposals must be received via email on or before the date and time outlined on the front page of this RFP. Send your electronic submittal to:

JBeers@bphc.org
Name of Firm, IT Cybersecurity Assessment and Plan (Subject Line)

Please submit one electronic copy in Adobe Acrobat PDF format, including all appendices. Submittals need to be limited to **9 MB in total email size**. It is the Consultant's responsibility to verify the receipt of the submittal. Electronic verification will be provided upon request.

***Late proposals will not be accepted by the Boston Public Health Commission. Proposals received after the stated date and time will not be reviewed and shall be deemed non-responsive.**

All proposals submitted shall be valid and binding on the submitting firm for a period of ninety days following the Proposal submittal deadline and for any extension of time granted by the submitting firm.

EVALUATION AND AWARD PROCESS

An evaluation team will review each proposal and evaluate all responses received based upon the criteria listed herein. The Boston Public Health Commission may request clarifications or additional information, if needed. After the evaluation team individually scores each proposal, the scores are tallied, and the firms are ranked based on the scores.

A selection may be made based on the proposals and initial evaluation criteria alone. Alternatively, the evaluation team may create a short list of the top ranked firms and invite the short-listed firms in for interview and/or check references. Scores for reference checks and interviews will be tallied and added to the short-listed firm's initial evaluation scores. Final selection will be based on reference checks and interviews.

The Boston Public Health Commission intends to select the Proposer who represents the best value to the Boston Public Health Commission and begin the negotiation and award process based on the evaluated scores.

The selected Consultant will be invited to enter contract negotiations with the Boston Public Health Commission. Should the Boston Public Health Commission and the selected firm(s) not reach a mutual agreement, the Boston Public Health Commission will terminate negotiations and move to the next highest ranked firm and proceed with negotiations.

The Boston Public Health Commission reserves the right to accept or reject any or all information in its entirety or in part and to waive informalities and minor irregularities and to contract as the best interest of the Boston Public Health Commission may require. The Boston Public Health Commission reserves the right to reject any or all Proposals submitted as non- responsive or non-responsible.

Procedure When Only One Proposal is received

In the event that a single responsive proposal is received, the Proposer shall provide any additional data required by the Boston Public Health Commission to analyze the proposal. The Boston Public Health Commission reserves the right to reject such proposals for any reason.

GENERAL INFORMATION

News releases pertaining to this RFP, the services, or the project to which it relates, shall not be made without prior approval by, and then only in coordination with, the Boston Public Health Commission.

COSTS BORNE BY PROPOSERS

All costs incurred in the preparation of a Proposal and participation in this RFP and negotiation process shall be borne by the proposing firms.

SMALL BUSINESS AND DISADVANTAGED BUSINESS OPPORTUNITIES

The Boston Public Health Commission encourages Certified Underrepresented Business Enterprises (CUBEs) to respond to this RFP. CUBE's are identified as; Disability-owned Business Enterprise (DOBE), Lesbian Gay Bisexual Transgender-owned Enterprise (LGBTBE), Minority-owned Business Enterprise (MBE), Small Local Businesses Enterprise (SLBE), Women-owned Business Enterprise (WBE), Veteran-owned Business Enterprise (VBE).

PUBLIC DISCLOSURE

Proposals submitted under this Solicitation will be considered public documents and, with limited exceptions, will become public information and may be reviewed by appointment by anyone requesting to do so following the conclusion of the evaluation, negotiation, and award process. This process is concluded when a signed contract is completed between the Boston Public Health Commission and the selected Consultant.

If a firm considers any portion of its response to be protected under the law, the vendor shall clearly identify each such portion with words such as "CONFIDENTIAL," "PROPRIETARY" or "TRADE SECRET" on each page for which the protection is sought. If a request is made for disclosure of such portion, the Boston Public Health Commission will notify the vendor of the request and allow the vendor not less than ten (10) days to seek a protective order from the Courts or other appropriate remedy and/or waive the claimed confidentiality. Unless such protective order is obtained and provided to the Boston Public Health Commission by the stated deadline, the Boston Public Health Commission will release the requested portions of the Proposals. By submitting a response, the vendor assents to the procedure outlined in this paragraph and shall have no claim against the Boston Public Health Commission on account of actions taken under such procedure.