Administration
Information & Technology Service

BOSTON PUBLIC HEALTH COMMISSION
REQUEST FOR PROPOSALS (RFP)
No. ITS-003-23

Cybersecurity Risk Assessment

February 22, 2023

Issued by
Boston Public Health Commission
1010 Massachusetts Ave, 2nd Floor,
Boston, MA 02118

I. INTRODUCTION

The Boston Public Health Commission (the "BPHC") Boston Public Health Commission (BPHC) is requesting proposals from experienced and qualified organizations to provide a comprehensive cybersecurity vulnerability assessment of the BPHC's network. In addition, the assessment should provide information security guidance that is fully aligned with industry standards and best practices and methodologies outlined in National Institute for Standards and Technology (NIST), Cyber Security Framework (CSF), HIPAA, ISO/IEC, etc. The evaluation should include an information security roadmap to be used to develop a plan for remediation of any items identified.

The BPHC is currently seeking proposals for the Cybersecurity Risk Assessment.

Proposers interested in providing the Cybersecurity Risk Assessment Services are invited to respond to this request. It is the BPHC's intent to select the Proposer(s) that provides the best solution for the BPHC's needs.

The BPHC reserves the right to amend this RFP. The BPHC reserves the right to reject any or all of the proposals, or any part thereof, submitted in response to this RFP, and reserves the right to waive formalities, if such action is deemed to be in the best interest of the BPHC. The BPHC reserves the right to request additional information from any Proposer. While it is expected that a single award will result for this RFP solicitation, the BPHC reserves the right to award negotiated contracts to one or more Proposers. Proposals received shall be considered to remain in effect for no less than six (6) months and for no more than eighteen (18) months from the date of receipt.

IMPORTANT: APPLICATIONS THAT ARE NOT 100% COMPLETE AS SPECIFIED WITHIN THIS RFP, EXCEED THE SPECIFIED PAGE LIMITS, OR ARE NOT RECEIVED BY THE SPECIFIED DUE DATE AND TIME WILL NOT BE REVIEWED. ACCORDINGLY, PLEASE READ THE INSTRUCTIONS CAREFULLY SINCE CRITICAL INFORMATION IN THESE REGARDS MIGHT ONLY BE PRESENTED ONE TIME.

The BPHC will only contract with firms that do not discriminate against employees or applicants for employment because of race, creed, color, national origin, sex, age, disability, marital status, sexual orientation, citizenship status, or any other status protected by Commonwealth of Massachusetts and Federal laws.

As part of BPHC's efforts to have an equitable procurement process, BPHC will consider and encourage Certified Unrepresentative Businesses Enterprises(CUBE) that include; Minority-owned Business Enterprises (MBE), Women-owned Business Enterprises (WBE), Veteran-owned Business Enterprises (VBE), Disability-owned Business Enterprise (DOBE), Lesbian Gay Bisexual Transgender Business Enterprises (LGBTBE), Minority Non-Profit(MNPO), Women Non-Profit(WNPO), Minority Women Non-Profit (MWNPO) and local businesses to apply to this RFP.

II. PROPOSAL SCHEDULE & APPLICATION REQUIREMENTS

A. ANTICIPATED SCHEDULE OF PROPOSAL

The following schedule is for informational purposes only. The BPHC reserves the right to amend this schedule at any time.

February 22nd, 2023 - Issue RFP:
The RFP and related attachments can be found and downloaded at the Boston Public Health Commission website City of Boston Bids and RFPs.

March 8th, 2023, by 3:00 pm EST - Deadline for Written Questions to be Submitted:
Written Questions should be **sent by email** to ITSRFP@bphc.org. All questions need to be **received no later** than **March 8th, 2023, at 3:00 pm EST**. Be sure to include "**Question - RFP# Cybersecurity Risk Assessment - ITS-003-23**" as the Subject Line in your email. **Only questions received by email by March 8th, 2023, at 3:00 pm EST WITH THE ABOVE-REFERENCED SUBJECT LINE WILL RECEIVE A RESPONSE**. NO INDIVIDUAL responses will be sent in response to emailed questions.

March 15th, 2023 - Responses to RFP Questions will be Posted:
Responses to Questions received by email and by the deadline will be posted on or about **March 15th, 2023,** on the Boston Public Health Commission website City of Boston Bids and RFPs.

WEDNESDAY, March 29th, 2023 BY 3:00 PM EST - PROPOSAL DEADLINE

On or about April 5th, 2023 - Selection Made

Following all necessary BPHC approvals Contract Signed

By June 23rd, 2023, the risk assessment must be finalized.
At the end of this engagement, the service provider will have conducted a comprehensive cybersecurity assessment of BPHC's Information Technology Assets. The first deliverable will be a Risk Assessment Report by **June 23rd, 2023**. The Information Security Roadmap should be delivered by **June 23rd, 2023**.

B. APPLICATION REQUIREMENTS

i. Each proposal shall be prepared simply and economically avoiding the use of elaborate promotional materials beyond what is sufficient to provide a complete, accurate and reliable presentation. An **eleven-point Font or larger**, **standard 8.5 inch by 11-inch paper**, **single-spaced with margins no smaller than 1 inch** are to be used for all materials (except for the Fonts, margins and paper size used on BPHC provided forms). **All documents are to include page numbers**.

ii. **PROPOSALS ARE TO BE PACKAGED AND ORDERED IN THE FOLLOWING MANNER:**
One **(1) original** shall be submitted in a **SEALED** package to Boston Public Health Commission, 1010 Massachusetts Ave, 2nd Floor, Boston, MA 02118. One **(1) digital copy** email to Procurement@bphc.org
Please **print single-sided** and do not staple.

1. **BPHC RFP Submission Package Checklist** (labeled as **Appendix A**).

2. **Application Cover Page** (labeled as **Appendix B**). The original must have an original signature of an authorized representative of the lead applicant organization.

3. **Vendor Profile**. The Vendor Profile is to be limited to **no more than four (4) pages. The Scoring Tool is included in this package (Appendix C) and should be reviewed in order to maximize your score.**

4. **Description of the proposed solution and work plan, including timeline and deliverables.** This requirement is limited to **no more than five (5) pages. The** Scoring Tool is included in this package (Appendix C) and should be reviewed in order to maximize your score.

5. **Responsible Bidder Attestation.**

6. **Disclosure of Employees or Officers of Boston Public Health Center**. A letter indicating the name, title and department of any employee or officer of Boston Public Health Commission within the 12 months immediately before the proposal. If none, indicate such in your letter.

7. **References.** A list of at least three (3) references from a Public Agencies organization with knowledge and experience with the specific services being offered.

8. **List of Prime Contractors and Subcontractors.** A list of prime contractors and subcontractors that the vendor does business with related to the services being offered in this RFP.

9. **Roles and Resumes of staff that will be assigned to this project.**

10. **Proposer Certification.** Include completed and signed Proposer Certification, with original signature, included as **Schedule A.**

11. **Response to Section B – Project and Long-Term Costs**. This should be submitted as a separate Section B.

C. HOW TO APPLY

To the extent feasible, please order your narrative content and the other proposal materials consistent with that indicated in **Section II B. Application Requirements**. If the ordering contradicts submission ordering directions in other sections of this RFP there will no penalty for any resultant document ordering discrepancies in your submission.

Submission of the proposals shall be directed to:

RFP# Cybersecurity Risk Assessment Service – No: ITS-003-23
Boston Public Health Commission
1010 Massachusetts Ave, 2nd Floor, Boston, MA 02118

All proposals must be delivered to the above office by March 29th, 2023 BY 3:00 PM. Proposals received after the above date and time will not be considered. Absolutely no exceptions will be made. The Boston Public Health Commission is under no obligation to return proposals.

1. NO COMMUNICATIONS OF ANY KIND WILL BE BINDING AGAINST THE BPHC, EXCEPT FOR THE INFORMATION TECHNOLOGY SERVICES FORMAL RESPONSES TO QUESTIONS, IF ANY, ADDRESSED ON THE WEBSITE.
2. Proposers may be required to give an oral presentation to the BPHC to clarify or elaborate on their written proposal. Those Proposers will be notified to arrange specific times.
3. No proposal will be accepted from, nor any agreement awarded to any Proposer that is in arrears upon any debt or in default of any obligation owed to the Boston Public Health Commission. Additionally, no agreement will be awarded to any Proposer that has failed to satisfactorily perform pursuant to any prior agreement with the Boston Public Health Commission.

4. **Optional:** In case of a Certified Minority Business Enterprise/Women's Business Enterprise (MBE/WBE) vendor. The proposers must include the Commonwealth of Massachusetts Supplier Diversity Office (SDO) Certification letter with their proposal.

5. **Optional:** In case the proposer is a Veteran-Owned Business, Proposer should include a letter indicating the company is 51% or more Veteran-owned.

Please note that BPHC will not review material beyond the specified page limits.

III. SCOPE OF PROFESSIONAL SERVICES REQUIRED

A. OBJECTIVE

The Boston Public Health Commission (BPHC) is requesting proposals from experienced and qualified organizations to provide a comprehensive cybersecurity vulnerability assessment of the BPHC's network. In addition, the assessment should provide information security guidance that is fully aligned with industry standards and best practices and methodologies outlined in National Institute for Standards and Technology (NIST), Cyber Security Framework (CSF), HIPAA, ISO/IEC, etc. The evaluation should include an information security roadmap to be used to develop a plan for remediation of any items identified.

B. GOAL

The goal of the assessment is to identify and validate weaknesses in the BPHC's information security architecture and posture from both an internal and external vantage point.

C. SCOPE OF WORK

The following tasks outline the functional areas in which the Service provider shall assess in this engagement.

Penetration Testing

The scope of the Penetrating testing should include the entire perimeter and any critical systems that may impact the security of the systems. This includes both the external perimeter (public-facing attack surfaces) and the internal perimeter (LAN to LAN attack surfaces).

Perimeter Testing

The service provider shall test BPHC's network perimeter both externally and internally. In addition, the test must include critical systems that could affect the security including security systems (e.g. firewalls, authentication servers,…, etc.) or any assets utilized by privileged users to support and manage the systems.

Activities must include, but may not be limited to:

1. Perform an in-depth cybersecurity vulnerability assessment and penetration testing of BPHC IT infrastructure of:

a. Internal network – all internal systems including routers, switches, physical and virtual servers, data storage infrastructure, and public computers and other connected IT devices: including all Demilitarized (DMZ) systems to include flow of controls from external and internal systems.

b. External network - all external public-facing systems including firewalls, FTP, web servers, and web service interface points.

2. Enumerate systems on the network and validate them against known systems. Identify any unknown or unexpected systems.
3. Scan network systems and mainframe for potential vulnerabilities. BPHC will provide the network ranges and any network/host exemptions to these scans.
4. Identify, analyze, and confirm vulnerabilities. It is expected that qualified service provider personnel will know how to look deeper into potential vulnerabilities for other security holes, misconfigurations, and other problems in order to follow the vulnerability to its end. It is expected that the service provider will share method and process (i.e., e-mail's screen shots, files, etc.) of successful penetration in addition to a list of open ports, missing patches, or possible vulnerabilities.

The security vendor will conduct security risk assessment scans on 5 critical applications.

All vulnerabilities reported as Critical/High shall be detailed in the 'Findings' section of the final deliverable. A complete list of vulnerabilities shall be provided in a separate appendix. Each vulnerability or risk identified shall be categorized as a Critical/High, Medium, or Low.

The service provider shall attempt to capture user credentials through the collection of the following vectors:

- Windows password hashes in-memory
- Keystroke logging
- Password and hash sniffing
- Collecting saved login credentials

User Privilege Escalation

Throughout the assessment, the service provider shall attempt to complete user privilege escalations in order to further compromise, or demonstrate the effectiveness of, the security of established controls within BPHC's environment.
This testing will assist in determining if access control systems are effectively enforcing user access and permission levels are configured correctly based on job function.

Segmentation Testing

The service provider shall test the segmentation controls of all segregated network segments from a sample of completely isolated/segmented networks (ensuring that each type of segmentation point is represented, such as firewalls, VLAN on switch, etc.).

Wireless Scanning (both private and guest)

The service provide shall identify rogue wireless devices and additional security architecture weaknesses related to the wireless networks.

Applications

• Provide authenticated application vulnerability scanning and penetration testing (At a minimum, the test should include OWASP Top 10). The security vendor will conduct security risk assessment scans on 5 external facing applications;

• Identify application security vulnerabilities and perform active exploit through identified vulnerabilities (Note: Exploit should stop at the point of proof of compromise but not causing any business interruption).

Database Assessment

We have approximately 16 database servers. In the database assessment phase, the service provider shall take the following actions:

• Assess the databases to look for common vulnerabilities such as buffer overflows, default accounts, or default permissions on database objects such as tables, views, and stored procedures.

• Look for erroneous configurations that may lead to information leaks, theft of data, or even intrusion and denial of service attacks.

• Examine several key functional areas that may include but not be limited to:

a. Authentication and Authorization to Control Database Access

b. Password Complexity Verification

c. Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities

d. Server Security

e. Database Connections

f. Table Access Control

g. Encryption Usage

h. Certificate Application

Brute Force Attack

The service provider shall conduct brute force attack to check for weak passwords. The objective of this test is to confirm whether passwords are meeting security best practices.

Social Engineering (Phone and E-mail)

During the Social Engineering phase of the assessment, the service provider shall attempt to impersonate and persuade BPHC/EMS employees via telephone and/or e-mail to disclose proprietary information. This information may allow the service provider to access sensitive information and/or exploit the integrity and/or availability of data. The sophisticated methods that may be utilized are, but not limited to, as follows:

• **Phishing/spear phishing Attacks** – Sending an e-mail to a user falsely claiming to be an established legitimate organization in an attempt to scam the user into surrendering

company sensitive/ information. The overall objective here is to measure end-user response to phishing, spear phishing, spam and other email threats.

• **Employee Impersonation** – Calling employees and attempt to convince them to release sensitive information (e.g. passwords of systems, unpublished e-mail addresses, names of other employees, names and virtual locations of systems).

• **Pretexting** – This method is the act of creating and using an invented scenario to persuade a targeted victim to release information or perform an action and is typically done over the telephone. It is more than a simple lie as it most often involves some prior research or set up and the use of pieces of known information (e.g. for impersonation: date of birth, Social Security Number, last bill amount or other specific company information to establish legitimacy in the mind of the target).

D. REQUIRED DELIVERABLES

1. Executive summary:

The executive summary should include high level overview of the assessment including the following:

a. Overall assessment results;

b. Overall risk ranking and key areas of risk;

c. Current maturity level score card against NIST cybersecurity framework;

d. Strategic recommendations and key areas of focus for remediation.

2. Detailed report:

The detailed report should include detail of the assessment including the following:

a. Assessment methodology;

b. Detailed assessment results in a sortable spreadsheet, risk ranking and actionable recommendations for all areas within the assessment scope;

c. Detailed score card of current maturity level for each NIST subcategory

3. Road map:

This should include both tactical and strategic recommendations in a risk-based approach with consideration of business environment, technology, people and process.

a. **Tactical recommendations:** This should identify issues that are tactical in nature, simple to implement, and will have a positive impact to overall NIST alignment. Recommendations should be made and presented in a risk-ranked format along with technical, resource and process requirements.

b. **Strategic Recommendations**: This should identify issues that are strategic in nature, complex to implement, and require management decisions to fund, but will have a significant impact to the overall architecture program. Recommendations should be made and presented in a risk-ranked format along with technical, resource and process requirements.

c. Appropriate milestones and key performance indicators to enhance BPHC's information security posture and address key risk findings.

d. Identification of security projects based on individual or combined recommendations with detailed activities and action plans.

e. An assessment of how the implementation of each project would remediate risk and position BPHC with respect to industry best practices.

4. Prioritized project plan:

The project plan is developed to support the road map. At a minimum, the project plan should include the following elements:

a. Project description

b. Priority

c. Risk rank

d. Supported road map item #

e. Recommended solution

f. Level of complexity to implement

g. Resource requirement

5. Presentation deliverable:

The service provider should prepare and deliver an executive-level presentation of the assessment.

It is important to note that once Cybersecurity vulnerability assessment testing is completed, the Service provider must remove all agents, backdoors, any software used for the Cybersecurity risk assessment project, thus removing any trace of existence in the BPHC IT infrastructure.

A summary of BPHC's devices is listed in the table below:

BPHC Device	Approximate Count
Workstations	979
Servers	93
Data Centers	3
VLANs	95
Routers	3
Switches	105
Firewalls	2
Wireless locations	10
Access Points	137
UPS – Battery backups	64

E. PROPOSAL REQUIREMENTS

For Proposers to be considered for an award, the terms, conditions, and instructions contained in this RFP and attachments must be met. Any proposal which does not meet these criteria may be considered non-responsive. Your proposal should include two sections (A and B) and should be submitted in separate envelopes. **To maximize your score, please refer to the Scoring Tool in Appendix C.**

Section A: Technical and Organization

This section shall describe the approach and plans for accomplishing the work outlined in the Scope of Service section. Each proposal shall be prepared simply and economically, avoiding the use of elaborate promotional materials beyond what is sufficient to provide a complete, accurate, and reliable presentation.

1. RFP Coversheet

2. Vendor Profile (Maximum: Four Pages)
    a. Background
        i. Date Founded
            1. Organizational Structure
                a. ( ) Sole Proprietorship
                b. ( ) Partnership
                c. ( ) Corporation
            2. Ownership Status
                a. ( ) Independent
                b. ( ) Subsidiary (Include Name of Parent Organization)
            3. Company History
            4. Office Locations, Personnel, and Expertise
            5. Products and Services Offered
    b. What is the vendor's years of experience, background, and track record in conducting cybersecurity risk assessment?
    c. Provide a description of your firm's experience in performing similar work.
    d. Professional Conduct
        i. Describe any situation where a client has terminated a contract with vendor "for cause" claiming breach of contract.
    e. Service Delivery Model
        i. Any services delivered by off-shore (outside North America). If so, please provide details.
        ii. Any deliverables scoped, developed, tested, or supported by off-shore (outside North America) resources? If so, please provide details.

3. Provide a Description of the proposed service and work plan, including timeline and deliverables. (Maximum: Five Pages)

4. Demonstrate that the bidder is a "responsible bidder" by attesting that the bidder:

a. Complies with all laws prerequisite to doing business in the Commonwealth of Massachusetts.
b. Complies with U.S. Equal Opportunity Employer provisions.

5. If applicable, Certified Minority Business Enterprise/ Women's Business Enterprise (MBE/WBE) proposers should include the Commonwealth of Massachusetts Supplier Diversity Office (SDO) Certification letter with their proposal.

6. If applicable, Proposers who operate a Veteran-Owned Business should include a letter indicating their company is 51% or more veteran-owned with their proposal.

7. The name, title, and department of any employee or officer who was an employee or officer of the Boston Public Health Commission within the 12 months immediately before the proposal. If none, indicate such in your letter.

8. A list of at least three references from an organization with knowledge and experience with the specific services being offered.

9. A list of all prime contractors and subcontractors that their agency does business with related to the service in this RFP.

10. Roles and resumes of staff that will be assigned to this project.

11. Include the signed Proposer Certification (Schedule A.) with the original signature.

Section B – Project Costs

This section shall provide the direct and indirect costs for accomplishing the work outlined in the Scope of Service section. Please include a description, justification, and calculation for all budget lines.

Project Costs

1. Personnel Costs:
    a. Total and hourly salaries for all personnel on the project.
    b. Fringe Benefit-cost.
2. Travel (if applicable)
3. Equipment (if applicable)
4. Contractual (if applicable)
5. Other (if applicable)
6. Software Licenses

IV. STATEMENT OF RIGHTS

UNDERSTANDINGS

Please take notice, by submission of a proposal in response to this request for proposals, the Proposer agrees to and understands:

- That any proposal, attachments, additional information, etc., submitted pursuant to this Request for Proposals constitute merely a suggestion to negotiate with the Boston Public Health Commission.
- Submission of a proposal, attachments, and additional information shall not entitle the Proposer to enter into an agreement with the Boston Public Health Commission for the required services;
- By submitting a proposal, the Proposer agrees and understands that the Boston Public Health Commission is not obligated to respond to the proposal, nor is it legally bound in any manner whatsoever by submission of same;
- That any and all counter-proposals, negotiations, or any communications received by a proposing entity, its officers, employees or agents from the Boston Public Health Commission, its officers, employees or agents, shall not be binding against the Boston Public Health Commission, its officials, officers, employees or agents unless and until a formal written agreement for the services sought by this RFP is duly executed by both.

In addition to the foregoing, by submitting a proposal, the Proposer also understands and agrees that the Boston Public Health Commission has the right, and may at its sole discretion exercise, the following rights, and options with respect to this Request for Proposals:

- To reject any or all proposals;
- To issue amendments to this RFP;
- To issue additional solicitations for proposals
- To waive any irregularities in proposals received after notification to Proposers affected;
- To select any proposal as the basis for negotiations of a contract, and to negotiate with one or more of the Proposers for amendments or other modifications to their proposals;
- To conduct investigations with respect to the qualifications of each Proposer;
- To exercise its discretion and apply its judgment with respect to any aspect of this RFP, the evaluation of proposals, and the negotiations and award of any contract;
- To enter into an agreement for only portions (or not to enter into an agreement for any) of the services contemplated by the proposals with one or more of the Proposers;
- To select the proposal that best satisfies the interests of the BPHC and not necessarily on the basis of price or any other single factor;
- To interview the Proposer(s);
- To request or obtain additional information the Boston Public Health Commission deems necessary to determine the ability of the Proposer;
- To modify dates;
- All proposals prepared in response to this RFP are at the sole expense of the Proposer, and with the express understanding that there will be no claim, whatsoever, for reimbursement from the Boston Public Health Commission for the expenses of preparation. The Boston Public Health Commission assumes no responsibility or liability of any kind for costs incurred in the preparation or submission of any proposal;
- The Boston Public Health Commission is not responsible for any internal or external delivery delays which may cause any proposal to arrive beyond the stated deadline. To be considered,

proposals MUST arrive at the place specified herein and be time-stamped prior to the deadline.

Proposal Costs

Each Proposer shall be solely responsible for all costs and expenses associated with the preparation and/or submission of its proposal, and BPHC shall have no responsibility or liability whatsoever for any such costs and expenses. Neither BPHC nor any of its directors, officers, employees or authorized agents shall be liable for any claims or damages resulting from the solicitation or collection of proposals.

BPHC assumes no responsibility or liability for costs incurred by respondents to the Request for Proposal, including any requests for additional information, interviews, or negotiations.

By submitting a proposal, Proposer expressly waives (i) any claim(s) for such costs and expenses, and (ii) any other related claims or damages.

Disposition of Proposals

All proposals submitted in response to this RFP become the property of BPHC once they are opened.

Other Considerations

BPHC reserves the right to request additional information as may be required and to further investigate proposer's qualifications to make this determination.

EVALUATION

The following criteria, not necessarily listed in order of importance, will be used to review the proposals. The Boston Public Health Commission reserves the right to weigh its evaluation criteria in any manner it deems appropriate:

- Proposer's demonstrated capability to provide the services;
- Evaluation of the professional qualifications, background and resume(s) of individuals involved in providing services;
- Proposer's experience to perform the proposed services;
- Proposer's financial ability to provide the services;
- Evaluation of the proposed cost/s. It should be noted that while cost is not the only consideration, it is an important one;
- A determination that the Proposer has submitted a complete and responsive proposal as required by this RFP;
- An evaluation of the Proposer's projected approach and plans to meet the requirements of this RFP;
- The Proposer's presentation at and the overall results of any interview conducted with the Proposer;
- Proposers MUST sign the Proposal Certification attached hereto as "Schedule A". Unsigned proposals will be rejected;
- If applicable, Certified Minority Owned Business Enterprises and Women-Owned Business Enterprises (MBE/WBE) by the Commonwealth of Massachusetts – Supplier Diversity Office (SDO) ;
- Proposers may be required to give an oral presentation to the Boston Public Health Commission to clarify or elaborate on the written proposal; and
- No proposal will be accepted from nor any agreement awarded to any Proposer that is in arrears upon any debt Additionally, no agreement will be awarded to any Proposer that has failed to satisfactorily perform pursuant to any prior agreement with the Boston Public Health Commission.

CONTRACT

After the selection of the successful Proposer, a formal written contract will be prepared by the Boston Public Health Commission and will not be binding until signed by both parties and, approved by the Boston Public Health Commission - Office of the General Counsel.

INDEMNIFICATION AND INSURANCE

The Proposer accepts and agrees that language in substantially the following form will be included in the contract between the Proposer and the Boston Public Health Commission:

> "In addition to, and not in limitation of the insurance requirements contained herein the Consultant agrees:
>
> (a) that except for the amount, if any, of damage contributed to, caused by or resulting from the negligence of the Boston Public Health Commission, the Consultant shall indemnify and hold harmless the Boston Public Health Commission, its officers, employees, and agents from and against any and all liability, damage, claims, demands, costs, judgments, fees, attorneys' fees or loss arising directly or indirectly out of the acts or omissions hereunder by the Consultant or third parties under the direction or control of the Consultant; and
>
> (b) to provide defense for and defend, at its sole expense, any and all claims, demands or causes of action directly or indirectly arising out of this Agreement and to bear all other costs and expenses related thereto
>
> Upon execution of any contract between the Proposer and the Boston Public Health Commission, the Proposer will be required to provide proof of the insurance coverage described in "Schedule B."
>
> Insurance coverage in amount and form shall not be deemed acceptable until approved by the Boston Public Health Commission."

INTELLECTUAL PROPERTY RIGHTS

The Proposer accepts and agrees that language in substantially the following form will be included in the contract between the Proposer and the Boston Public Health Commission:

> All deliverables created under this Agreement are to be considered "works made for hire.". If any of the deliverables do not qualify as "works made for hire," the Consultant hereby assigns to the Boston Public Health Commission all right, title and interest (including ownership of copyright) in such deliverables and such assignment allows the BPHC to obtain in its name copyrights, registrations and similar protections which may be available. The Consultant agrees to assist the BOSTON PUBLIC HEALTH COMMISSION, if required, in perfecting these rights. The Consultant shall provide the BOSTON PUBLIC HEALTH COMMISSION with at least one copy of each deliverable.
>
> The Consultant agrees to indemnify and hold harmless the BOSTON PUBLIC HEALTH COMMISSION for all damages, liabilities, losses, and expenses arising out of any claim that a deliverable infringes upon an intellectual property right of a third party. If such a claim is made, or appears likely to be made, the Consultant agrees to enable the BOSTON PUBLIC HEALTH COMMISSION's continued use of the deliverable, or to modify or replace it. If the BOSTON PUBLIC HEALTH COMMISSION determines that none of these

alternatives is reasonably available, the deliverable will be returned.

All records compiled by the Consultant in completing the work described in this Agreement, including but not limited to written reports, source codes, studies, drawings, blueprints, negatives of photographs, computer printouts, graphs, charts, plans, specifications, and all other similar recorded data, shall become and remain the property of the BOSTON PUBLIC HEALTH COMMISSION. The Consultant may retain copies of such records for its own use.

NON-COLLUSION

The Proposer, by signing the proposal, does hereby warrant and represent that any ensuing agreement has not been solicited, secured or prepared directly or indirectly, in a manner contrary to the laws of the Commonwealth of Massachusetts and the rules of Boston Public Health Commission, and that said laws have not been violated and shall not be violated as they relate to the procurement or the performance of the agreement by any conduct, including the paying or the giving of any fee, commission, compensation, gift, gratuity or consideration of any kind, directly or indirectly, to any BOSTON PUBLIC HEALTH COMMISSION employee, officer or official.

CONFLICT OF INTEREST

All Proposers must disclose with their proposals the name of any officer, director or agent who is also an employee of the Boston Public Health Commission. Further, all Proposers must disclose the name of any BPHC employee who owns, directly or indirectly, an interest of ten percent or more in the firm or any of its subsidiaries or affiliates.

There shall be no conflicts in existence during the term of any contract with the BOSTON PUBLIC HEALTH COMMISSION. The existence of a conflict shall be grounds for termination of a contract.

COMPLIANCE WITH LAWS

By submitting a proposal, the Proposer represents and warrants that it is familiar with all federal, state, and local laws and regulations and will conform to said laws and regulations. The preparation of proposals, selection of Proposers, and the award of contracts are subject to provisions of all Federal, State, and BOSTON PUBLIC HEALTH COMMISSION laws, rules and regulations.

CONTENTS OF PROPOSAL

The federal Freedom of Information Act and the Massachusetts Public Records Law, mandates public access to government records.

APPENDIX A:
BPHC SUBMISSION PACKAGE CHECKLIST
RFP# ITS-003-23

Cybersecurity Risk Assessment Services

Proposer Name: _____

Place a check in the first column to indicate that each item is contained in your application package. Materials should be compiled in the following order.

	APPENDIX A: RFP Submission Package Checklist
	APPENDIX B: Cover Page
	Vendor Profile (Maximum Four (4) pages)
	Description of the proposed solution and work plan, including timeline and deliverables. (Maximum Five (5) Pages)
	Responsible Bidder Attestation
	Commonwealth of Massachusetts - Supplier Diversity Office (SDO): MBE/WBE Certification Letter (if applicable)
	Veteran-Owned Business Letter (if applicable)
	Disclosure of Employees Boston Public Health Commission
	References
	List of Prime Contractors and Subcontractors
	Roles and Resumes of Staff assigned to this project
	Proposer Certification
	Section B: Project Costs

APPENDIX B

COVER PAGE INSTRUCTIONS

BOSTON PUBLIC HEALTH COMMISSION **Cybersecurity Risk Assessment Services** **RFP # ITS-003-23** **Appendix B: PROPOSER COVER PAGE FORM - APPLICANT INFORMATION** **Instructions for completing Appendix B**	
Organization Name	Please list the official name of your organization.
Mailing Address	Please list the official address of your organization for mailing purposes; include city and ZIP code information.
Primary RFP Contact	Please provide name, telephone number, FAX number, email address and, complete mailing address if different than the organizational mailing address above, for the primary contact for this proposal. Should you have a change in this information after submitting your application, please be sure to provide the updated information to ITSRFP@bphc.org
Alternate RFP Contact	Please provide name, telephone number, FAX number, email address and, complete mailing address if different than organization mailing address above, for an alternate contact for this proposal. Should you have a change in this information after submitting your application, please be sure to provide the updated information to ITSRFP@bphc.org .
Leadership	Please list the name of your organization's Executive Director, President or Chief Executive Officer. If your organization has interim leadership, please list "Interim" in parentheses.

_____ _____

Chief Executive Officer Signature (as identified above) Date

_____

Printed Name and Title

APPENDIX B:

COVER PAGE

BOSTON PUBLIC HEALTH COMMISSION **Cybersecurity Risk Assessment** **RFP # ITS-003-23** **APPENDIX B: AGENCY COVER PAGE - APPLICANT INFORMATION** **Please refer to the instructions within the RFP for completing Appendix B.** **(This is to be the top sheet for the entire application package.)**	
Organization Name:	
Mailing Address:	
Primary RFP Contact:	
Alternate RFP Contact:	
Leadership:	

_____ _____

Chief Executive Officer Signature (as identified above) Date

_____

Printed Name and Title

APPENDIX C

BOSTON PUBLIC HEALTH COMMISSION SCORING TOOL

Cybersecurity Risk Assessment Services

RFP# ITS-003-23

Ranking	Description	Score
Not Acceptable	Non-responsive, fails to meet RFP specification. The approach has no probability of success. If a mandatory requirement, this score will result in disqualification of the proposal.	0
Poor	Below average, falls short of expectations, is substandard to that which is the average or expected norm, and has a low probability of success in achieving objectives per RFP.	1
Fair	Has a reasonable probability of success; however, some objectives may not be met.	2
Average	Acceptable, achieves all objectives in a reasonable fashion per RFP specification. This will be the baseline score for each item, with adjustments based on the interpretation of the proposal by Evaluation Committee members.	3
Above Average	Very good probability of success, better than that which is average or expected as the norm. Achieves all objectives per RFP requirements and expectations.	4
Exceptional	Exceeds expectations, is very innovative, and clearly superior to that which is average or expected as the norm. Excellent probability of success in achieving all objectives and meeting RFP specifications.	5

List	Evaluation Criteria	Weight
A.	**Completeness of Response:** Responses to this RFP must be complete. Responses that do not include the proposal content requirements identified within this RFP will be considered incomplete, be rated a Fail in the Evaluation Criteria and will receive no further consideration.	Pass/Fail
B.	**Bid Form Response :** The points for the Bid Form response will be based on the following three areas. 1. Understanding the Requirements: Are all the requirements understood accurately and reflected in the solution? 2. Completeness and appearance of the Proposal: This focuses on the Scope of Service itself. Are all aspects of the project addressed appropriately in the proposal? Does it leave questions about the project unanswered? 3. Deliverables: Has the proposer demonstrated that it understands the deliverables the BPHC expects it to provide?	20
C.	**Vendor Profile:** Proposals will be evaluated against the RFP specifications and the questions below: 1. Background and Experience: Do the Vendor's background and experience indicate that they are capable of performing the Scope of Services? 2. Staff: Does the Vendor's staff that will be assigned to this project have experience on similar projects?	40

D.	**Solution and Work Plan:** 1. Feasibility: Is the workplan feasible to meet all timelines? How well has the proposer identified pertinent issues and potential problems related to the project? 2. Solution**:** Does the platform the vendor will have the required features requested in the scope of service?	30
E.	**M/WBE Certification (If Applicable):** Does the agency receive MBE/WBE Certification from the Commonwealth of Massachusetts – Supplier Diversity Office (SDO)?	10
F.	**Project and Long-Term Costs** (to be evaluated for highest ranked proposal(s)) Is the budget, complete, reasonable and provide sufficient justification for costs? Are the Long-Term costs provided, reasonable and provide sufficient justification for costs?	20

Section Scores:

Completeness of Response: _____
Bid Form Response: _____
Vendor Profile: _____
Solution and Work Plan: _____
MBE/WBE: _____
Total Score: _____

Comments/Potential follow-up questions for the agency:

RFP# ITS-003-23
BPHC EXECUTIVE APPROVAL OF SCORING TOOL

_____
Chief Information Officer

_____
Date

Appendix E - Privacy Policy

Privacy Statement

Effective Date:

Table of Contents

Introduction

The [Boston Public Health Commission] [does x in BPHC].

[Boston Public Health Commission] understands that you are aware of and care about your own personal privacy interests, and we take that seriously. This Privacy Notice describes the policies and practices regarding the collection and use of your personal data, and sets forth your privacy rights. We recognize that information privacy is an ongoing responsibility, and so we will from time to time update this Privacy Notice as we undertake new personal data practices or adopt new privacy policies.

Privacy Officer

Boston Public Health Commission is headquartered in 1010 Massachusetts Avenue, Boston, MA 02118, in the United States. Boston Public Health Commissioner has appointed a Privacy Officer for you to contact if you have any questions or concerns about personal data policies or practices. If you would like to exercise your privacy rights, please direct your query to Privacy Officer. Boston Public Health Commission privacy officer's name and contact information are as follows:

[Include the appropriate name and contact information here]

How we collect and use (process) your personal information

Boston Public Health Commission collects personal information about its website visitors and customers. With a few exceptions, this information is generally limited to:

- [List data collected here]

We use this information to provide prospects and customers with services.

We do not sell personal information to anyone and only share it with third parties who are facilitating the delivery of our services.

Use of the [APP NAME]

As is true of most other mobile applications, [Boston Public Health Commission mobile app name] collects certain information automatically and stores it in log files. The information may include internet protocol (IP) addresses, the region or general location where your computer or device is accessing the internet, browser type, operating system, and other usage information about the use of [BPHC mobile app name], including a history of the pages you view. We use this information to help us design our site to better suit our users' needs. We may also use your IP address to help diagnose problems with our server and to administer our website, analyze trends, track visitor movements, and gather broad demographic information that assists us in identifying visitor preferences.

[BPHC] has a legitimate interest in understanding how members, customers, and potential customers use the [BPHC mobile app name]. This assist [BPHC] with providing more relevant products and services, with communicating value to our sponsors and corporate members, and with providing appropriate staffing to meet member and customer needs.

Sharing information with third parties

The personal information [BPHC] collects from you is stored in one or more databases hosted by third parties located in the United States. These third parties do not use or have access to your personal information for any purpose other than cloud storage and retrieval.

[BPHC] does not otherwise reveal your personal data to non-[BPHC] persons or businesses for their independent use.

Transferring personal data to the U.S.

[BPHC] has its headquarters in the United States. Information we collect about you will be processed in the United States. By using [BPHC] services, you acknowledge that your personal information will be processed in the United States. The United States has not sought nor received a finding of "adequacy" from the European Union under Article 45 of the GDPR. Pursuant to Article 46 of the GDPR, CCNY & its affiliates are providing for appropriate safeguards by entering binding, standard data protection clauses, enforceable by data subjects in the EEA and the UK. These clauses have been enhanced based on the guidance of the European Data Protection Board and will be updated when the new draft model clauses are approved.

For more information or if you have any questions, please contact us at [Insert appropriate contact details here].

Data Subject rights

The European Union's General Data Protection Regulation (GDPR) and other countries' privacy laws provide certain rights for data subjects. Data Subject rights under GDPR include the following:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right of data portability
- Right to object
- Rights related to automated decision-making including profiling

This Privacy Notice is intended to provide you with information about what personal data [BPHC] collects about you and how it is used.

If you wish to confirm that [BPHC] is processing your personal data, or to have access to the personal data & its affiliates may have about you, please contact us.

For questions or complaints concerning the processing of your personal data, you can email [BPHC] at [Insert appropriate contact details here].

Data storage and retention

Your personal data is stored by the [BPHC] on its servers, and on the servers of the cloud-based database management services the [BPHC] engages, located in the United States. The [BPHC] retains service data for the duration of the customer's business relationship with the [BPHC] and for a period of time thereafter, to analyze the data for [BPHC's] own operations, and for historical and archiving purposes associated with [BPHC's] services. [BPHC] retains prospect data until such time as it no longer has business value and is purged from [BPHC] systems. All personal data that [BPHC] controls may be deleted upon verified request from Data Subjects or their authorized agents. For more information on where and how long your personal data is stored, and for more information on your rights of erasure and portability, please contact us at [insert appropriate contact details here].

Questions, concerns or complaints

If you have questions, concerns, complaints, or would like to exercise your rights, please contact us at:

[Insert appropriate contact information here]

SCHEDULE A: PROPOSER

CERTIFICATION

The undersigned agrees and understands that this proposal and all attachments, additional information, etc. submitted herewith constitute merely an offer to negotiate with the Boston Public Health Commission. Submission of this proposal, attachments, and additional information shall not obligate or entitle the proposing entity to enter into a service agreement with Boston Public Health Commission for the required services. The undersigned agrees and understands that the Boston Public Health Commission is not obligated to respond to this proposal nor is it legally bound in any manner whatsoever by the submission of same. Further, the undersigned agrees and understands that any and all proposals and negotiations shall not be binding or valid against the Boston Public Health Commission, its directors, officers, employees or agents unless an agreement is signed by a duly authorized officer of the Boston Public Health Commission and, if necessary, approved by the BPHC Office of General Counsel.

It is understood and agreed that the Boston Public Health Commission reserves the right to reject consideration of any and all proposals including, but not limited to, proposals which are conditional or incomplete. It is further understood and agreed that the Boston Public Health Commission reserves all rights specified in the Request for Proposals.

It is represented and warranted by those submitting this proposal that except as disclosed in the proposal, no officer or employee of the BPHC is directly or indirectly a party to or in any other manner interested in this proposal or any subsequent service agreement that may be entered into.

By: _____
Proposer Signature

_____
Printed Name and Title

Date: _____