BOSTON PUBLIC HEALTH COMMISSION

Information Technology Services

REQUEST FOR PROPOSALS

IT Security Infrastructure and Governance Improvement Program

RFP# BPHC-ITS-2026-03

Issuing Department	Information Technology Services (ITS)
Issue Date	May 8, 2026
Questions Due	May 14, 2026
Proposal Due Date	June 8, 2026
Contract Period	July 1, 2026 through November 30, 2026

1. INTRODUCTION AND PURPOSE

1.1 Overview

The Boston Public Health Commission (BPHC), through its Information Technology Services (ITS) department, is soliciting proposals from qualified vendors that are based in the United States to provide professional services across five (5) discrete IT security and infrastructure improvement projects. These projects are designed to strengthen BPHC's security posture, improve operational processes, and ensure alignment with industry standards and regulatory requirements.

1.2 Organizational Background

BPHC serves the residents of Boston through public health programs and services. The ITS department supports approximately 1,300 employees across eight workplace organizations, managing the technology infrastructure, applications, and data systems that enable the Commission's mission-critical operations.

Commitment to Equitable Procurement: BPHC is dedicated to fostering equitable procurement practices and encourages submissions from Certified Underrepresented Business Enterprises (CUBE). This includes Minority-owned Business Enterprises (MBE), Women-owned Business Enterprises (WBE), Veteran-owned Business Enterprises (VBE), Disability-owned Business Enterprises (DOBE), Lesbian, Gay, Bisexual, and Transgender Business Enterprises (LGBTBE), Minority Non-Profit Organizations (MNPO), Women Non-Profit Organizations (WNPO), Minority Women Non-Profit Organizations (MWNPO), and local businesses.

1.3 Submission Options

Vendors are welcome to submit proposals for one or more of the five projects described herein, according to their areas of expertise. Proposals must clearly identify which project(s) the vendor is responding to.

In addition to the lump sum pricing vendors must submit an itemized list of all proposed charges including (equipment, parts, materials, software, shipping, labor, installation, integration, implementation, maintenance, etc.) Cost must be itemized and broken down separately for each project effort.

All prices are inclusive of travel. No additional charges including travel lodging, and other expenses will be allowed.

1.4 RFP Questions

All questions regarding this RFP must reference the specific Project Number and if applicable the section in question. Questions must be submitted in writing by the deadline specified in Section 2, RFP Timeline.

2. RFP TIMELINE AND KEY DATES

The following schedule governs the solicitation process. BPHC reserves the right to modify these dates as necessary with written notice to prospective vendors.

Milestone	Date
RFP Issued and Posted on the Boston Globe	May 8, 2026, 11:00 AM EST
Deadline for Written Questions	May 14, 2026, 5:00 PM EST
Responses to Questions Published	May 29, 2026, 5:00 PM EST
Proposal Submission Deadline	June 8, 2026, 5:00 PM EST
Proposal Evaluation Period	June 9, 2026 – June 12, 2026
Vendor Presentations/Interviews (if applicable)	June 15, 2026 – June 19, 2026
Anticipated Contract Start Date	July 1, 2026

3. SCOPE OF WORK

This RFP encompasses five (5) distinct project areas. Vendors may propose on individual projects or any combination thereof. Each project must be priced independently with itemized cost breakdowns.

3.1 Project 1: Patch and Software Update Process Remediation

3.1.1 Objective

Identify and resolve existing deficiencies in BPHC's patch management and software update procedures. The selected vendor shall document, automate, and test the complete process lifecycle to ensure consistent, reliable, and timely application of patches and updates across the enterprise environment.

3.1.2 Scope of Services

The vendor shall provide the following services:

a) Conduct a comprehensive assessment of the current patch and software update procedures, identifying gaps, inefficiencies, and risks.

b) Repair issues with SCCM and Patch My PC deployments to all devices and servers to cover all existing needed patches.

c) Design and document a standardized, repeatable patch management lifecycle, including scheduling, testing, deployment, verification, and rollback procedures.

d) Develop and implement automation tools and scripts to streamline the patch deployment process.

e) Perform end-to-end testing of the documented process to validate reliability and effectiveness.

f) Provide knowledge transfer, and training to BPHC ITS staff on the updated processes and automation tools.

3.1.3 Environment

Patching and software updates include, but are not limited to:

- Configuration of services across servers and hosts
- Certificate management to comply with current cryptographic standards
- Cisco network equipment firmware and software upgrades
- [X] servers and [X] hosts (exact counts to be confirmed during vendor onboarding)

3.1.4 Deliverables

- Current-state assessment report with gap analysis
- Fully Operational Patching system that covers all PC's, Servers and applications.
- Documented patch management lifecycle procedures

- Automation scripts and deployment tools
- Test plans and results documentation
- Knowledge transfer sessions, documentation and training materials

3.2 Project 2: Web Application Security Hardening

3.2.1 Objective

Harden approximately seven (7) BPHC web applications by systematically remediating previously identified vulnerabilities to reduce the organization's overall security posture.

3.2.2 Scope of Services

a) Review existing vulnerability assessment and penetration testing reports for each application.

b) Develop a prioritized remediation plan based on risk severity (critical, high, medium, low).

c) Manage project meetings with stakeholders and application vendors as needed

d) Execute remediation activities for identified vulnerabilities, including but not limited to patches, input validation, authentication and session management, access controls, encryption validated for compliance with NIST Federal Information Processing Standards, secure configuration, and patching of application components.

e) Remediation may include implementation or enhancement of cryptographic controls.

f) Perform post-remediation verification testing to confirm that vulnerabilities have been effectively addressed.

g) Provide a final operational and security posture report for each application detailing remediation actions taken and residual risk.

3.2.3 Deliverables

- Prioritized remediation plan per application
- Remediation of identified vulnerabilities across approximately seven (7) web applications
- Post-remediation verification test results
- Final operational and security posture report per application

3.3 Project 3: IT Governance Policy and Plan Development

3.3.1 Objective

Develop comprehensive Information Technology plans and policy documents aligned with the NIST Cybersecurity Framework, industry best practices, and BPHC's specific business needs. These documents shall provide the governance foundation for daily operations performed by BPHC IT staff.

3.3.2 Scope of Services

a) Facilitate stakeholder meetings to assess current IT governance maturity and identify organizational requirements.

b) Develop the following plans and policy documents:

   a) Manage the project through to completion, including facilitating meetings, documenting and communicating tasks and project updates, and performing applicable test exercises with BPHC stakeholders.

   b) Ensure all documents are mapped to relevant NIST Framework controls and categories.

   c) Conduct tabletop exercises or test procedures as applicable to validate plans.

3.3.3 Deliverables

BPHC may substitute any requested plan or policy for an alternative of equivalent scope and complexity based on project requirements

- Contingency and Disaster Recovery Plan
- Data Center Controls Policy Document
- Data and System Backups Policy Document
- Patch Management Policy Document
- NIST Framework mapping and alignment documentation
- Meeting minutes, project status reports, and communication logs
- Tabletop exercise results and after-action reports

3.4 Project 4: Data Classification Program and ePHI Data Flow Mapping

3.4.1 Objective

Implement a formal Data Classification program for BPHC and lead the development of an electronic Protected Health Information (ePHI) data flow network map. This project will establish the foundational framework for BPHC to identify, categorize, and protect sensitive data assets across the organization.

3.4.2 Scope of Services

a) Develop and implement a Data Classification policy and framework, including classification tiers (e.g., Public, Internal, Confidential, Restricted), handling procedures, and labeling standards.

b) Lead the discovery and mapping of ePHI data flows across the network, identifying systems, applications, databases, and transmission paths that store, process, or transmit ePHI.

c) Facilitate and manage project meetings with stakeholders, including coordination with Data Loss Prevention (DLP) vendors.

d) Manage task allocation, provide regular project updates, and produce comprehensive documentation.

e) Provide recommendations for DLP processing, tools and technologies to support the data classification program.

3.4.3 Deliverables

- Data Classification Policy and Framework Document
- ePHI Data Flow Network Map
- Data asset inventory and classification catalog
- DLP vendor evaluation and recommendations report
- Meeting minutes, project updates, and stakeholder communications

3.5 Project 5: VLAN Implementation and Network Segmentation

3.5.1 Objective

Design, apply, and implement Virtual Local Area Networks (VLANs) and associated network controls to logically separate systems within BPHC's network infrastructure. This project will enhance network security by isolating critical systems and reducing the blast radius of potential security incidents.

3.5.2 Scope of Services

a) Assess the current network topology and identify systems and services requiring logical segmentation.

b) Assessment and design must comply with NIST guidelines and where applicable Criminal Justice Information Services (CJIS) security policy requirements,

c) Design a VLAN architecture that addresses security, performance, and operational requirements.

d) Develop a detailed implementation plan, including phased rollout, testing, and rollback procedures.

e) Implement VLANs and associated access control lists (ACLs), firewall rules, and inter-VLAN routing configurations.

f) Coordinate with other vendors as necessary to establish dependencies and align project timelines.

g) Manage the project from preparation through implementation, including documentation and stakeholder communications.

3.5.3 Deliverables

- Current-state network assessment report
- VLAN design and architecture documentation
- Implementation plan with phased rollout schedule
- Implemented VLANs with validated network segmentation
- Updated network diagrams reflecting new VLAN topology
- Post-implementation test results and validation report

4. PROPOSAL REQUIREMENTS

Each proposal must include the following components, organized in the order listed below. Vendors responding to multiple projects should provide information for each project separately where applicable.

4.1 Cover Letter

A cover letter on vendor letterhead, signed by an authorized representative, indicating the project(s) for which the proposal is being submitted and confirming the vendor's ability to meet the requirements described in this RFP.

4.2 Company Profile and Qualifications

- U.S. based Company name, address, and primary point of contact
- Year established, number of employees, and organizational structure
- Description of relevant experience providing similar services to government, healthcare, or public sector organizations
- Relevant certifications (e.g., CISSP, CISM, CEH, PMP, ITIL)
- At least three (3) client references for comparable engagements within the last five (5) years

4.3 Technical Approach

For each project proposed, provide a detailed description of the vendor's technical approach, including methodology, tools, frameworks, and standards to be employed. The approach should demonstrate an understanding of the public health environment and BPHC's operational context.

4.4 Project Plan and Timeline

For each project proposed, include a detailed project plan with defined milestones, dependencies, resource assignments, and estimated timeline from kickoff to completion.

4.5 Staffing Plan

Identify the proposed project team, including key personnel, roles, and responsibilities. Provide resumes or qualifications summaries for all key staff assigned to the engagement.

4.6 Cost Proposal

Cost must be itemized and broken down separately for each project. The cost proposal must include:

- Labor rates by role (hourly and/or fixed fee)
- Estimated hours by project phase and task

- Travel and other direct expenses (if applicable)
- Total fixed-price or not-to-exceed amount per project
- Any assumptions that affect pricing

4.7 Exceptions and Assumptions

Identify any exceptions to the terms of this RFP and any assumptions made in preparing the proposal.

5. EVALUATION CRITERIA

Proposals will be evaluated based on the following criteria. BPHC reserves the right to request clarification, conduct interviews, or request presentations as part of the evaluation process.

Evaluation Criteria
Technical Approach and Methodology
Relevant Experience and Qualifications
Project Plan and Staffing
Cost Proposal
References and Past Performance

6. GENERAL TERMS AND CONDITIONS

6.1 Right to Reject

BPHC reserves the right to reject any or all proposals, to waive any informalities or irregularities in proposals, and to accept or negotiate modifications to any proposal if it is in the best interest of the Commission.

6.2 Confidentiality

All information provided by BPHC in connection with this RFP is confidential. Vendors should not disclose any BPHC data, systems information, or project details to third parties without prior written consent.

6.3 Insurance Requirements

The selected vendor(s) must maintain, at a minimum, the following insurance coverage throughout the term of the contract: commercial general liability, professional liability (errors and omissions), workers' compensation, and cyber liability insurance. Specific minimum coverage amounts will be stipulated in the contract.

6.4 Compliance

The selected vendor(s) shall comply with all applicable federal, state, and local laws and regulations, including but not limited to HIPAA, HITECH, and Massachusetts data privacy laws (M.G.L. c. 93H). Vendors must demonstrate familiarity with the NIST Cybersecurity Framework.

6.5 Background Checks

All vendor personnel assigned to work at BPHC or with access to BPHC systems and data may be subject to background checks as a condition of engagement.

6.6 Contract Term

The anticipated contract period is June 18, 2026 through November 30, 2026, with the option to extend by mutual agreement and if/when additional funds are made available. Individual project timelines may vary within the overall contract period. 6/18/26-11/30/26

This contract is partially fund by a CDC Public Health Infrastructure Grant, Assistance Listing Number 93.967."

7. SUBMISSION INSTRUCTIONS

7.1 Submission Deadline

Proposals must be received no later than May 28, 2026 at 5:00 PM Eastern Standard Time. Late submissions will not be considered.

7.2 Submission Method

Proposals must be submitted electronically in PDF format to:

Email: RFR@bphc.org

Subject Line: RFP# BPHC-ITS-2026-03 – IT Security Infrastructure and Governance – Project Number - Section (if applicable), [Vendor Name]

7.3 Questions

All questions regarding this RFP must be submitted in writing by the deadline specified in Section 2. Questions must reference the specific Project Number and if applicable the section in question. Questions should be directed to RFR@bphc.org

7.4 Proposal Format

Proposals should not exceed fifty (50) pages per project (excluding resumes and appendices). Proposals must be clearly organized and follow the structure outlined in Section 4, Proposal Requirements.

APPENDIX A: PROJECT SUMMARY MATRIX

Project #	Title	Description
Project 1	**Patch and Software Update Process Remediation**	Identify and fix issues in patch/update procedures; document, automate, and test the lifecycle
Project 2	**Web Application Security Hardening**	Harden approximately 7 web applications by remediating identified vulnerabilities
Project 3	**IT Governance Policy and Plan Development**	Develop IT plans and policies aligned with NIST Framework, including DR, backup, and patch management
Project 4	**Data Classification and ePHI Data Flow Mapping**	Implement Data Classification program; develop ePHI data flow network map
Project 5	**VLAN Implementation and Network Segmentation and network Mapping**	Apply, implement, and map VLANs and controls for logical system separation