SECTION 1: UNIQUE QUESTIONS BY PROJECT

Project 1 — Patch and Software Update Process Remediation

Q1. Does "repair issues with SCCM and Patch My PC deployments" require ongoing operational management, or is this a one-time configuration and remediation engagement with knowledge transfer to BPHC staff?

Response: This is a one-time configuration and remediation engagement. The vendor is expected to resolve existing deployment issues and complete knowledge transfer to BPHC staff. Ongoing operational management is not within scope.

Q2. Is the selected vendor expected to maintain or provide ongoing support for the patch management system beyond the November 30, 2026 contract end date?

Response: No. BPHC does not expect the vendor to provide ongoing support beyond the November 30, 2026 contract end date.

Q3. Will BPHC define the list of patches to apply, or is BPHC requesting the vendor to provide an analysis of existing data to prioritize patching efforts?

Response: BPHC will provide the list of required patches. The vendor is expected to ensure all identified patches are applied and to configure the environment so that newly applicable patches install automatically going forward.

Q4. Are there defined objectives/KPIs for the number of patches to apply or vulnerabilities to remediate?

Response: Yes. BPHC maintains a complete patch and vulnerability report (Arctic Wolf) that defines the target remediation set against which progress is measured.

Q5. Are there any considerations to patching that should be accounted for, such as secure enclaves, zero-trust architecture, etc.?

Response: No. BPHC's objective is for all in-scope applications to be configured and operating correctly within its SCCM/Intune environment. No secure-enclave or zero-trust considerations apply to this engagement.

Q6. Which vulnerability discovery tool will BPHC use, and which data source will be authoritative for measuring remediation progress?

Response: Arctic Wolf is the authoritative source. The Arctic Wolf patch listing will be used to measure remediation progress.

Q7. What percentage of devices are currently enrolled, reachable, and reporting accurately through SCCM/MECM or other management tools?

Response: BPHC estimates that approximately 90% of devices with SCCM installed are reporting correctly. Exact figures are not currently confirmed; validating and improving coverage is part of this engagement.

Q8. Are servers patched through the same process as endpoints, or through a separate server patching process?

Response: Most servers are patched manually: SCCM is used to download patches, which are then installed manually. A limited number of servers are configured for automatic installation.

Q9. Are non-Cisco network devices, firewalls, wireless controllers, VPN appliances, or security appliances in scope?

Response: No. Scope is limited to desktops and servers. Network and security appliances are out of scope.

Q10. How many applications are included in the statement that the patching system must cover "all PCs, servers, and applications"?

Response: Up to 50 applications.

Q11. What reporting, dashboards, or evidence will BPHC require to accept the final deliverables?

Response: An Arctic Wolf report confirming the patch list is fully up to date will serve as acceptance evidence.

Q12. Will the vendor receive administrative access to SCCM/MECM, Patch My PC, servers, endpoints, network equipment, certificate authorities, and reporting tools?

Response: Yes. The vendor will be granted the administrative access required to complete the engagement.

Q13. What version of SCCM (or MECM/Intune) is currently deployed, and is the environment co-managed or standalone?

Response: SCCM version 2503; console version 5.2503.1083.1500; site version 5.0.9135.1000. The environment is co-managed (Intune/SCCM).

Q14. Who from ITS will be the target audience (roles/teams) for training and knowledge transfer?

Response: The Server Infrastructure Team.

Q15. What does "fully operational" mean to BPHC (coverage expectations and verification evidence)?

Response: "Fully operational" means all devices can be patched successfully and no systems are flagged as missed on the Arctic Wolf report.

Q16. Are there any internal standards or restrictions on scripting/automation approaches for this environment?

Response: BPHC prefers the use of existing tools with little to no additional scripting. Where scripting is necessary, the vendor must explain why the result cannot be achieved with existing products and must train BPHC staff on any scripts used.

Project 2 — Web Application Security Hardening

Q1. Are exploit testing activities included in verification testing after remediation, or is validation limited to non-exploit confirmation?

Response: Penetration testing is out of scope. Validation is limited to non-exploit confirmation.

Q2. Are mitigating controls acceptable for complex vulnerabilities that cannot be simply fixed in source code, or for vulnerable legacy dependencies requiring large-scale refactoring?

Response: Yes. Compensating controls may be considered where a direct source-code fix is not feasible.

Q3. Does BPHC have preferred SAST, DAST, or IAST tooling for remediation and verification, or is tool selection at the vendor's discretion?

Response: BPHC does not mandate specific SAST/DAST/IAST tooling. Tool selection is at the vendor's discretion, subject to BPHC review and approval prior to use.

Q4. Is the FIPS compliance requirement applicable across all seven applications, or only those handling ePHI or subject to CDC grant requirements?

Response: FIPS compliance is required for applications handling sensitive information and wherever feasible. Any exceptions must be documented and approved by BPHC.

Q5. For code changes, what are BPHC's expectations? Will vendor developers be onboarded, and are specific security or code-quality artifacts required?

Response: The selected vendor is expected to provide application-vendor coordination and advisory support to BPHC application owners and the database administrator. Required code changes will be implemented by the BPHC team or the application vendor.

Q6. What authentication mechanisms are currently in use (custom auth, SSO, IAM integration)?

Response: Microsoft Entra single sign-on (SSO).

Q7. Is there a preferred risk-scoring framework (CVSS version, OWASP risk rating) for prioritization?

Response: CVSS is the preferred risk-scoring framework.

Q8. Which tools were used to generate the vulnerability findings (DAST, SAST, manual PT, etc.)?

Response: BPHC's managed services provider conducts the scans; the specific tooling is not known to BPHC.

Q9. What is the age of the most recent vulnerability assessment and penetration test reports for each application?

Response: December 2025.

Q10. Will vendors be granted direct access to application source code, configuration repositories, and deployment pipelines?

Response: No. The vendor provides advisory support. Any required code changes will be made by the BPHC team or the application vendor.

Q11. Please clarify whether remediation includes source-code changes, configuration changes, server/database hardening, application-vendor coordination, infrastructure remediation, or advisory support.

Response: Remediation is limited to application-vendor coordination and advisory support to application owners and the database administrator.

Q12. Will BPHC provide any follow-up support after verification (within the contract window)?

Response: Advisory support is expected to remain available through post-remediation verification within the contract window. No support is expected beyond the contract term.

Q13. Does BPHC currently have any WAF appliances or services applied to its web applications?

Response: BPHC does not operate a dedicated Web Application Firewall (WAF) for the in-scope applications. Perimeter protection is provided by a Palo Alto next-generation firewall with URL filtering and spam filtering subscriptions, along with associated threat-prevention capabilities. WAF deployment is not within the scope of this project; vendors may note where a WAF would serve as a recommended compensating control for vulnerabilities that cannot be readily remediated in source code.

Project 3 — IT Governance Policy and Plan Development

Q1. To what level of specificity is NIST CSF mapping required: function and category, or down to subcategory and informative references?

Response: Mapping is required primarily at the function and category level, with subcategory and informative-reference mapping where needed.

Q2. Which CJIS controls are in scope, and which BPHC systems or data types are subject to CJIS requirements?

Response: CJIS requirements apply to the specific services/systems identified as subject to CJIS policy. Additional detail will be provided to the selected vendor.

Q3. Are there specific Massachusetts (M.G.L. c. 93H) WISP or notification language requirements that must be embedded in the policy deliverables?

Response: Applicable regulations may be referenced subject to BPHC approval.

Q4. Is independent third-party validation or attestation expected at the end of the project, or is internal documentation sufficient?

Response: BPHC will validate and approve the IT governance policies and plans developed under this engagement. Independent third-party attestation is not required.

Q5. How many BPHC IT staff members and dedicated cybersecurity staff support the environment?

Response: To be discussed with the selected vendor.

Q6. Approximately how many formal, documented IT security policies are currently in place, and when were they last reviewed?

Response: Up to 15 policies are currently in place and have been reviewed recently.

Q7. Is a formal process currently in place for periodic cybersecurity risk assessment and mitigation, or is one expected to be developed?

Response: Yes. BPHC is implementing an annual cybersecurity risk assessment and mitigation process, beginning this year.

Q8. Are cybersecurity roles formally assigned within ITS, and should the deliverables include a RACI matrix?

Response: Cybersecurity roles are defined. A RACI matrix reference will be provided if needed.

Q9. Is a formal security awareness training program currently operational, and how frequently is training delivered?

Response: Yes. Training is delivered frequently.

Q10. To what degree is cybersecurity integrated into BPHC's overall business strategy or public health mission, and should the governance plan address business alignment explicitly?

Response: This may be explored in greater detail during the vendor interview, if applicable.

Q11. Should vendors treat the Section 3.3.3 Deliverables list as the authoritative document set?

Response: Yes. Section 3.3.3 (Deliverables) is the authoritative document set. The sub-items under Section 3.3.2(b) describe project-management and validation activities rather than naming the documents to be produced; vendors should rely on the Section 3.3.3 list.

Q12. Are there governance committee or board approval workflows that must be factored into the policy-ratification timeline?

Response: The BPHC project lead will manage all approvals.

Q13. What are the "specific business needs" of BPHC that governance deliverables must align to?

Response: This may be discussed in greater detail during the vendor interview, if applicable.

Q14. Has BPHC completed a formal Business Impact Analysis or similar documentation (critical system inventories, continuity assessments, recovery prioritization, downtime impact analyses)?

Response: No. BPHC has not created or completed a formal Business Impact Analysis or similar documentation.

Q15. Are there prior audits (internal/external) or compliance assessments available for vendor review?

Response: Available as needed.

Q16. Can vendors use AI-based note-taking or transcription to document meeting minutes?

Response: BPHC-approved AI tools may be used for note-taking of non-sensitive information only.

Q17. What is the scope of the Disaster Recovery plan (technology domain, business service, recovery scenario, location, or all of the above)?

Response: BPHC does not currently have a Disaster Recovery plan; developing one is a requirement of this engagement (see the Contingency and Disaster Recovery Plan deliverable in Section 3.3.3). The vendor is expected to define the appropriate scope — across technology domains, business services, recovery scenarios, and locations — in coordination with BPHC.

Q18. Does BPHC anticipate substituting any of the listed deliverables, and if so, which ones?

Response: As provided in Section 3.3.3, BPHC may substitute any requested plan or policy for an alternative of equivalent scope and complexity. BPHC has no current plans to do so but wishes to keep the option open.

Project 4 — Data Classification and ePHI Data Flow Mapping

Q1. Does BPHC have a preferred data classification tier structure, or is the vendor expected to propose one?

Response: Section 3.4.2(a) provides example tiers (Public, Internal, Confidential, Restricted). The vendor is expected to propose and implement a final classification framework based on these examples, aligned to HIPAA and applicable Massachusetts requirements and subject to BPHC approval.

Q2. Does BPHC own data discovery and scanning tooling (e.g., Varonis, BigID, Microsoft Purview), or is the vendor expected to provide tooling for ePHI discovery?

Response: BPHC uses Skyhigh DLP.

Q3. Is the ePHI data flow mapping expected to be a network/infrastructure-layer diagram, an application/business-process diagram, or both?

Response: Both. BPHC expects network/infrastructure-layer and application/business-process views.

Q4. Are there business areas outside BPHC's approximately 1,300 employees (contractors, partner clinics, vendors) whose data flows must be included?

Response: Where applicable, mapping should account for ePHI flows to and from external parties.

Q5. Will scope include end-to-end data security posture management, including ties to incident response/breach processes, monitoring and alerting, and exfiltration indicators of compromise?

Response: Primary scope is data classification and ePHI data-flow mapping; integration with incident response and monitoring may be addressed at an advisory level.

Q6. What is the estimated volumetric scale of BPHC's data?

Response: Approximately up to 10 TB.

Q7. Does the ePHI mapping need to include data at rest, data in transit, and data in use, or primarily transit/transmission paths?

Response: Mapping should address data at rest, in transit, and in use.

Q8. Beyond HIPAA, are there specific data types (HIV/AIDS status, substance-use treatment, mental health, reproductive health) where BPHC applies additional state-law protections?

Response: Details will be provided to the selected vendor.

Q9. Please confirm the expected level of detail and output format for the ePHI data flow network map and the data asset inventory/classification catalog.

Response: Expected deliverables are an ePHI data-flow network map and a data asset inventory/classification catalog, provided in an editable, BPHC-approved format.

Project 5 — VLAN Implementation and Network Segmentation

Q1. How are BPHC sites interconnected (leased lines, MPLS, SD-WAN, cloud links)?

Response: A mix of Comcast Ethernet Network Services (ENS) and the local BoNet WAN.

Q2. How many wireless networks are there, and what are their use cases?

Response: Approximately 20. Most locations have wireless, used for company laptops and phones as well as public access.

Q3. Are any network devices nearing end-of-life or out-of-support status?

Response: Yes — some access points and core switches.

Q4. Does new hardware need to be procured?

Response: BPHC is not aware of any required procurement. Vendors are invited to advise if hardware is needed.

Q5. Does the environment include OT, IoT, or ICS networks?

Response: Yes.

Q6. Is there a desired VLAN architecture already designed to be tested/implemented, or must one be created as part of the engagement?

Response: Each location contains separate networks, and larger locations have multiple VLANs by floor. Traffic is currently configured with separate Data, Voice, and Camera VLANs.

Q7. Does the implementation include endpoint reconfiguration (NAC, 802.1X, device re-IPing), or is it limited to network infrastructure changes?

Response: Whatever is required to achieve the desired results is in scope.

Q8. Does BPHC have a preferred or required Network Access Control platform (e.g., Cisco ISE, Aruba ClearPass)?

Response: Cisco ISE.

Q9. Is internal traffic currently being filtered or shaped by any tools/devices?

Response: No filtering or shaping is currently in place; SolarWinds tools are used to capture traffic.

Q10. Will dynamic VLAN assignment to supplicants be required?

Response: BPHC wants industry best practices implemented; if dynamic VLAN assignment is part of best practice, then yes.

Q11. What is the driving force for this project — a zero-trust initiative or a compliance issue?

Response: Network segmentation was identified as a weak point in a security audit.

Q12. Is IPv6 in use or a requirement for future use?

Response: IPv6 is not currently in use. If recommended, BPHC would require it for future use.

Q13. Is there a guest network that needs to be logically segmented but co-existing on the network infrastructure?

Response: BPHC does not currently have one but would welcome it.

Q14. Is there a test environment available, and how closely does it resemble production?

Response: No.

Q15. Who is currently in charge of KTLO (keep-the-lights-on) network management duties?

Response: Currently unassigned.

Q16. Who are the key stakeholders that will need to be involved with this project?

Response: CSO, DTS, DEA, the EA Team, and the SI Team.

Q17. What service provider platforms are in scope (AWS, Azure, Google Cloud)?

Response: Microsoft Azure.

Q18. Are any components on-premises or colocated in a physical data center (self-hosted)?

Response: Yes. BPHC operates two data centers.

Q19. Is this a hybrid environment where services may need routes across service providers, self-hosted, SaaS, or PaaS solutions?

Response: Yes. BPHC has a City WAN partnership and Comcast connectivity.

Q20. Which NIST guidelines are in scope, and is a specific framework (e.g., NIST SP 800-171) required?

Response: The NIST Risk Management Framework, including SP 800-53B.

Q21. Is the goal to achieve a specific compliance certification (e.g., CMMC Level 2)?

Response: The objective is to enhance network security by isolating critical systems and reducing the blast radius of potential security incidents; a specific certification is not the goal.

Q22. Will evaluating and recommending fit-for-purpose network solutions be in scope?

Response: Yes. Evaluating and recommending fit-for-purpose solutions is within scope, subject to BPHC approval.

Q23. Are there any licensing considerations in scope (existing contracts, consolidation for cost optimization)?

Response: Opportunities for consolidation and cost optimization may be proposed.

Q24. Please confirm who will approve firewall/ACL changes.

Response: The Lead Network Manager (Change Control Team).

Q25. Please confirm warranty/support expectations for segmentation configuration changes after implementation during the contract term.

Response: No post-implementation warranty or support expectations apply.

Cross-Project / General Questions

Q1. Is on-site presence required at BPHC facilities, and if so, for which projects and at what minimum percentage of effort?

Response: On-site presence is not required; however, the vendor must be available to come on-site if needed.

Q2. What is BPHC's expected reporting cadence (weekly status, biweekly steering committee, monthly executive update)?

Response: Weekly status reporting, or as otherwise determined by stakeholders.

Q3. Who will be the BPHC primary point of contact for each project, and what is their anticipated weekly time commitment?

Response: BPHC will provide a contact list prior to project start.

Q4. Will BPHC provide a technical sponsor (network engineer, application owner, GRC lead) for each project to validate findings and approve changes?

Response: Yes.

Q5. Does BPHC have an existing project management tool (Jira, Asana, ServiceNow, Smartsheet) the vendor must use, or is the vendor's tooling acceptable?

Response: BPHC does not mandate a specific project management tool. The vendor's tooling is acceptable, subject to BPHC review.

Q6. If a vendor proposes on all five projects, should the Company Profile, Cover Letter, and Staffing Plan be repeated in each project section, or submitted once with project-specific addenda?

Response: Corporate qualification materials (Company Profile, Cover Letter, Staffing Plan) should be submitted once, with project-specific addenda provided for each project proposed.

Q7. Are evaluation criteria weighted? If so, can BPHC provide the percentage weighting for each criterion?

Response: The evaluation criteria are listed in Section 5: Technical Approach and Methodology; Relevant Experience and Qualifications; Project Plan and Staffing; Cost Proposal; and References and Past Performance. BPHC has not published numerical weightings; proposals are evaluated against these criteria on a best-value basis.

Q8. What are the minimum coverage amounts required for commercial general liability, professional liability (E&O), and cyber liability insurance?

Response: Per Section 6.3, the selected vendor must maintain commercial general liability, professional liability (errors and omissions), workers' compensation, and cyber liability insurance. Specific minimum coverage amounts are not stated in the RFP and will be stipulated in the contract.

Q9. Do any of the eight workplace organizations operate in clinical or patient-facing environments requiring after-hours or weekend-only change windows?

Response: The workplace organizations do not operate in clinical or patient-facing environments; they operate in client-facing environments.

Q10. What level of background investigation is required (CORI, federal, fingerprint-based)?

Response: CORI.

Q11. Are teaming arrangements or subcontracting relationships permitted, and what are the disclosure requirements?

Response: Teaming and subcontracting arrangements are permitted. All subcontractors must be disclosed in the proposal, including the scope of work each will perform.

Q12. Can vendors be awarded multiple projects, and can the same personnel be proposed across multiple projects?

Response: Yes. Vendors may be awarded multiple projects, and the same personnel may be proposed across projects, provided capacity to deliver is demonstrated.

Q13. What is the anticipated contract type — Firm Fixed Price, Time and Materials, or Labor Hour?

Response: Per Sections 1.3 and 4.6, BPHC requires lump-sum pricing with a total fixed-price or not-to-exceed amount per project, supported by itemized cost breakdowns (labor rates by role and estimated hours by phase and task).

Q14. Are there specific federal flow-down requirements, reporting obligations, or compliance restrictions stemming from the CDC Public Health Infrastructure Grant (Assistance Listing No. 93.967)?

Response: Yes. BPHC reports to the CDC under the Public Health Infrastructure Grant (Assistance Listing No. 93.967). Applicable federal flow-down and reporting obligations apply.

Q15. Will BPHC provide remote VPN access for vendors performing assessment and implementation work?

Response: Yes. BPHC will provide the selected vendor with the required VPN access.

Q16. Is there a preference for local vendors?

Response: Per Section 1.2, BPHC encourages submissions from local businesses and supports the local economy; qualified local vendors are given consideration.

Q17. What is the annual budget allocated for this RFP?

Response: BPHC's budget is subject to annual approval. A specific RFP budget figure is not published.

Q18. Can vendors provide entire services from an offshore location (outside U.S. geography)?

Response: No. Per Section 1.1, only qualified, U.S.-based vendors will be considered, and services must be delivered from within the United States.

Q19. Who are the previous incumbents on this project?

Response: None. This is the first time BPHC is engaging a vendor for this scope.

Q20. Does BPHC require City of Boston supplier/vendor registration before proposal submission, or only after award?

Response: Only after award.

Q21. For vendors submitting on multiple projects, will BPHC give evaluation consideration to integrated delivery efficiencies, or is each project scored strictly independently?

Response: BPHC will consider integrated delivery efficiencies for vendors proposing on multiple projects; however, each project will be evaluated on its own merits.

Q22. For advisory/professional-services-only projects with no equipment or materials, is a labor-only itemization (by role, phase, and task) sufficient for Section 1.3 itemized pricing?

Response: Yes. For advisory/professional-services-only projects with no equipment or materials, a labor-only itemization by role, phase, and task satisfies the Section 1.3 itemized pricing requirement.

Q23. Please confirm whether BPHC expects separate workstreams per project or an integrated program management approach when a vendor is awarded multiple projects.

Response: When a vendor is awarded multiple projects, BPHC expects an integrated program management approach with clearly defined per-project workstreams.

Q24. Please define BPHC's expected acceptance process for deliverables, including review cycles, approval authorities, documentation formats, and whether formal sign-off is required.

Response: Each deliverable is subject to BPHC review, with the BPHC project lead holding approval authority and formal written sign-off required for each deliverable.

Q25. Are there mandatory BPHC project management, change management, documentation, security review, or governance templates vendors must use?

Response: BPHC does not require any mandatory templates. Vendor templates are acceptable, subject to BPHC review and approval.

Q26. Will BPHC provide access to current-state documentation, architecture diagrams, asset inventories, prior assessments, and system configurations during onboarding?

Response: Yes. BPHC will provide relevant current-state documentation, diagrams, inventories, and prior assessments during onboarding, as applicable to each project.

Q27. Please identify whether BPHC has target completion dates or priority sequencing across the five projects.

Response: The overall contract period runs through November 30, 2026 (Section 6.6); individual project timelines may vary within that window.

Q28. Please confirm BPHC stakeholder availability for discovery workshops, technical interviews, application-owner meetings, security reviews, CAB reviews, tabletop exercises, and deliverable reviews.

Response: BPHC stakeholders will be made available for discovery workshops, interviews, reviews, and related sessions, scheduled in coordination with the BPHC project lead.

Q29. Please clarify whether BPHC has planned blackout periods, maintenance freezes, holiday restrictions, fiscal-year constraints, or operational windows affecting implementation schedules.

Response: BPHC has no planned blackout periods, maintenance freezes, holiday restrictions, or fiscal-year constraints. However, the vendor must provide advance notification to BPHC ITS staff before any potentially disruptive activity, so that ITS can notify the entire BPHC staff or affected departments. Server patching must be performed after hours (see related response below).

Q30. Please identify any dependencies on incumbent vendors, MSPs, application vendors, security vendors, network service providers, or cloud providers that may affect schedule, access, or implementation authority.

Response: Dependencies include BPHC's managed security services provider, application vendors, and network service providers (Comcast and the City WAN partnership). Coordination with these parties will be facilitated by BPHC.

Q31. Please confirm whether references must be specific to the project being proposed or may represent comparable engagements generally.

Response: References may represent comparable engagements; they need not be specific to the exact project proposed.

Q32. Does BPHC have a preference for references from public health agencies, healthcare entities, municipal/state government, or other public-sector organizations?

Response: BPHC values references from public health agencies, healthcare entities, and municipal/state government, but will consider all relevant public- and private-sector references.

Q33. Are subcontractor references acceptable when subcontractors will perform a defined portion of the work?

Response: Yes, where the subcontractor will perform a defined portion of the work.

Q34. Are resumes required only for key personnel or for all personnel proposed?

Response: Resumes are required for all key personnel. Resumes for additional proposed personnel are encouraged but not mandatory.

Q35. Are there mandatory certifications for project personnel beyond the RFP examples (e.g., CISSP, CISM, CEH, PMP, GIAC)?

Response: Beyond the examples cited in the RFP, no additional certifications are mandatory; relevant certifications will be viewed favorably during evaluation.

Q36. Please confirm whether CUBE, MBE, WBE, VBE, DOBE, LGBTBE, MNPO, WNPO, or local business status will be evaluated or scored as part of award preference.

Response: Per Section 1.2, BPHC encourages submissions from Commonwealth of Massachusetts Certified Underrepresented Business Enterprises (CUBE) — including MBE, WBE, VBE, DOBE, LGBTBE, MNPO, WNPO, and MWNPO — and local businesses. Vendors may reference their certification status under the Commonwealth's Supplier Diversity Program (https://www.mass.gov/supplier-diversity-program-sdp).

Q37. Will BPHC conduct oral presentations or interviews for all shortlisted vendors, only selected vendors, or only if clarification is required?

Response: Shortlisted vendors should expect an interview.

Q38. Will BPHC consider proposed innovations, accelerators, automation, reusable templates, or process improvements as part of the Technical Approach score?

Response: Yes. Proposed innovations, accelerators, automation, and reusable templates may be considered as part of the Technical Approach evaluation.

Q39. Please confirm whether the 50-page limit applies separately to each project response for multi-project vendors, and whether shared corporate qualifications, resumes, and pricing appendices are excluded from the per-project page count.

Response: Per Section 7.4, the 50-page limit applies per project, excluding resumes and appendices. Shared corporate qualifications, resumes, and pricing appendices are excluded from the per-project page count.

Q40. Please confirm whether BPHC prefers milestone-based, monthly progress-based, or deliverable-based invoicing.

Response: BPHC prefers deliverable-based invoicing; milestone-based or monthly progress-based invoicing will also be considered.

Q41. Please confirm how BPHC will handle material scope changes after award (unexpected asset counts, third-party delays, expanded requirements).

Response: Material scope changes will be handled through BPHC's change-control process via a written change order approved by the BPHC project lead prior to execution.

Q42. Will BPHC provide vendor personnel with BPHC-issued laptops and credentials, or are vendors expected to use their own devices with VPN access?

Response: Vendors are expected to use their own devices with BPHC-provided VPN access.

Q43. Beyond HIPAA, HITECH, M.G.L. c. 93H, and NIST CSF, are there other frameworks BPHC is aligning to (HITRUST, CIS Controls, CDC PHIG-specific control requirements)?

Response: Per Section 6.4, BPHC aligns to HIPAA, HITECH, Massachusetts data privacy law (M.G.L. c. 93H), and the NIST Cybersecurity Framework, with CJIS where applicable (Project 5). No additional frameworks (e.g., HITRUST, CIS Controls) are specified in the RFP.

Q44. Please confirm whether cost will be evaluated on a lowest-price technically acceptable basis, best-value basis, or another method.

Response: Cost is one of five evaluation criteria listed in Section 5; evaluation is multi-factor (best-value) rather than lowest-price technically acceptable.

Q45. Are all 1,300 users in scope for Projects 1–5, or are specific groups excluded?

Response: Specific BPHC stakeholders will have defined roles in the projects; not all 1,300 users are directly in scope.

Q46. Are there any workforce groups with special compliance handling requirements (ePHI/CJIS) affecting access controls, segmentation design, or documentation scope?

Response: Yes. Refer to Appendix A (project summary matrix) and the RFP details for ePHI/CJIS handling requirements.

Q47. What Microsoft licensing tiers are currently in place (G3, G5, G5 Security)?

Response: Currently on Microsoft G3. However, we are looking to upgrade to G5.

Q48. Are there any plans to upgrade or change Microsoft licensing tiers that could impact security capabilities, patching posture, data classification, or DLP approach?

Response: BPHC may upgrade its Microsoft licensing tiers based on discussion and vendor recommendations during the engagement.

Q49. Please confirm whether BPHC is primarily procuring professional services and that any software/equipment costs must be itemized per project.

Response: Yes. BPHC is primarily procuring professional services. Any software or equipment costs must be itemized separately per project.

Q50. Please confirm whether any project activities require after-hours execution (e.g., patching deployment windows, VLAN cutovers).

Response: Server patching must be performed after hours. Desktop patching may occur during business hours, with users warned by the system prior to action. VLAN cutovers should be scheduled with the BPHC change-control team.

Q51. Please clarify what BPHC expects under "maintenance" for each project, if anything.

Response: BPHC does not anticipate ongoing maintenance obligations beyond the contract term for these engagements.

Q52. Will BPHC provide development resources needed to deploy remediations into production, and resources for QA and regression testing?

Response: For Project 2, code changes and production deployment, QA, and regression testing will be performed by the BPHC team or the application vendor. BPHC will make appropriate resources available for coordination.

Q53. Please confirm whether verification testing must be performed by the same vendor or may be coordinated with application vendors.

Response: Verification testing may be coordinated with application vendors; it is not required to be performed solely by the selected vendor.

Q54. Please confirm whether the vendor is expected to provide any follow-up support after post-remediation verification (within the contract window).

Response: The vendor is expected to provide advisory support through post-remediation verification within the contract window; no support is expected beyond the contract term.

Q55. Approximately how long does BPHC's onboarding and access provisioning process typically take (background checks, system access, badges)?

Response: Refer to the most recent communication for the timeline and any extensions.
