Request for Proposal
Questions and Responses

---

**Request for Proposal:** Cybersecurity Risk Assessment
**Proposal Due Date:** Wednesday, March 29, 2023, by 5:00 PM EST

1. Has BPHC previously had a security standards/best practices assessment performed? No. If so, when was the last time?
2. Does BPHC have existing information security policies and procedures? Yes
3. Is there a budget or budget range for this engagement that can be shared? Yes. We don't have a range.
4. How many employees and contractors does BPHC have? Approximately 1600
5. How many employees and contractors are within BPHC's IT department? 30
6. Does BPHC have an information security department? Yes
7. What is the expected timeline for all assessments to be completed? Its in RFP
8. How will issues / deviations to the contract be addressed? Change Order
9. Is there any information of relevance left off the RFI that would be applicable to scoping of this bid? No. But we are offering vendors to ask questions.
10. Does the scope of work include review of security configurations of critical systems? No If so, can you please identify the type and quantity?
11. Who will be reviewing the RFP submission? Team from BPHC
12. How many proponents have been invited to compete? Unknown
13. Is this a one-year contract term? No. This is not a one-year contract. This is a service which will be provided by the selected security vendor. The service will be finished once the security vendor completes all the required tasks listed in the RFP.
14. Is this procurement activity considered a capital expenditure, or operational? Operational
15. Is the bid restrictive to bidders from Massachusetts? No
16. Reference paragraph C.2, will BPHC provide a list of known systems? No Known systems will be provided.
17. Reference paragraph C.4, What do credential harvesting options mean to BPHC? The main objective of this activity is to ensure that we are protected against credential harvesting attack in which a threat actor use the compromised credentials to infiltrate BPHC networks or sell them to other threat actors for the same purpose.
18. Have you developed National Institute of Standards and Technology (NIST) compliant Cybersecurity Framework (CSF) documents: System Security Plan (SSP), Cybersecurity Strategy Implementation Plan (CSIP), and System Assessment Plan (SAP), or will development of these documents be included in the scope of the contract for the selected vendor? No.

19. RFP Part IV: Statement of Rights: Indemnification and Insurance: Please provide "Schedule B" as referenced in this section which will show the description of required insurance coverage. Vendors insurance policy
20. Is BPHC open to exceptions and clarifications to the RFP? No.
21. Is it BPHC's intent to use the provided BPHC standard contract for the provision of goods or services as the contract for this agreement or is BPHC open to starting from a contract provided by the vendor for later negotiations? BPHC is open to Vendor provided contract based on BPHC negotiation.
22. If BPHC's intent is to use the provided standard contract for the provision of goods or services, does BPHC want to accept redlines to this contract after award or would any redlines need to be submitted with the proposal? Red line needs to be submitted with the proposal.
23. Does BPHC have an expectation that the vendor contributes any information to Appendix E - Privacy Policy that must be submitted with the proposal or is this Appendix included in the RFP package for vendors' information only? BPHC have an expectation that the vendor contributes any information to Appendix E - Privacy Policy that must be submitted with the proposal.
22. For reporting, would BPHC like all results rolled-up into one report, or will each business unit or geo area have its own report i.e. site specific reporting? All findings can be combined into one report.
23. Will the City consider leveraging an existing contract (i.e. master service agreements) if the selected vendor already has an agreement in place? Yes. BPHC will consider selected vendor who already has an agreement in place.
24. Are vendors permitted to request exceptions to terms and conditions of this RFP and its attachment to negotiate in line with an existing agreement? Yes, vendors are permitted to request exceptions to terms and conditions of this RFP.
25. We are unable to supply the total annual salaries for employees. Does completing the living wage agreement meet this requirement? Yes, completing the living wage agreement meet this requirement.
26. We are typically unable to provide resumes of specific staff members until an engagement is awarded. Are general role profiles and descriptions acceptable for the purposes of the RFP? Resumes of the specific staff members who will be working on this project are required to be part of the bid and there would be no exceptions.
27. If there is one functional area of the scope a vendor is unable to deliver, will an incomplete proposal be considered? No.
28. Are legal discussions available to discuss any privacy concerns with components of the RFP? No legal discussion is available to discuss any privacy concerns with components of the RFP at this point.
29. "Enumerate systems on the network": Is this referring to the internal network or externally exposed network? If internal, will this be white box or black box enumeration? Meaning, will we have visibility into the full internal network? Enumerate systems on both internal and external network. It is your responsibility to gain full visibility of BPHC network.
30. Is there a process in place to address PII or other regulated data which is exposed. Our HIPAA Privacy Policy is designed to comply with HIPAA's breach notification rule and has procedures that apply when there's been a confirmed or suspected breach.
31. Will a 3-ring binder be acceptable to use to submit our proposal? Please refer to RFP

32. Will you accept an electronic signature on the Application Cover Page and the Proposer Certification forms? Yes
33. Please confirm that the technical proposal and cost proposal can be sent in one email. Please refer to RFP
34. Regarding **Responsible Bidder Attestation** (item #4 on pp. 11-12): The RFP states that the bidder will attest that they comply "with all laws prerequisite to doing business in the Commonwealth of Massachusetts." Should bidders use Article X of the BPHC Standard Contract as a reference for these laws? That is correct. All vendors need to comply with all laws prerequisite to doing business in the Commonwealth of Massachusetts.
35. Regarding **References** (item #7 on pg. 4): The RFP requests "A list of at least three (3) references from a Public Agencies organization…" Will references from federal government agencies be considered acceptable? Yes, federal government agencies are acceptable
36. Regarding **List of Prime Contractors and Subcontractors** (item # 8 on pg. 4): Can BPHC please clarify the nature of this question? Is the goal to learn about subcontractors or outside vendors that might be brought on to this project? We have no plans to bring any subcontractors onto this project; we are unclear on what is being asked about prime contractors, since we would be the only prime. Is BPHC asking about our teaming partners outside of this project? It is BPHC goal to learn about subcontractors or outside vendors that might be brought on to this project. If the contractor does not have a sub-contractor. Just write "NA"
37. Are resumes required for both key and non-key personnel? Please refer to RFP
38. Would BPHC allow the assessment to be conducted remotely? Yes, the risk assessment can be conducted remotely as long as the incumbent can fulfill all the requirements stated in the RFP. If yes, will BPHC allow installation of scanning and wireless sensors on BPHC's internal network? No
39. Is a security clearance or background check required? No.
40. Does the assessing team need to be based in the U.S.? Yes
41. Does the final presentation have to be made in-person? No.
42. Has this type of assessment been conducted in prior years? Yes. If so, is there a current incumbent? No
43. You requested that the proposals not be stapled, would you like them bound in another way or loose sheets of paper in a folder? Please refer to RFP
44. Can you clarify what you are requesting for the following requirement: A list of all prime contractors and subcontractors that their agency does business with related to the service in this RFP? It is BPHC goal to learn about subcontractors or outside vendors that might be brought on to this project. If the contractor does not have a sub-contractor. Just write "NA".
45. None of the forms included in Appendix 0 are listed on the Appendix A checklist. Appendix 0 does not exist in the RFP. Which, if any, forms are to be included with the proposal?
46. Section A.6 (page 12 of RFP) references Veteran-Owned Businesses, but Appendix C-E (page 21) only lists M/WBE certification. Is veteran certification status eligible for those 10 points? Yes, veteran certification status will be eligible for the 10 points.

47. Is this testing engagement required to fulfil any specific regulatory/compliance needs and if so, which frameworks? The security risk 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,…, etc.
48. Would you like us to perform follow up testing after you have remediated the findings to validate your remediations? This RFP does not cover the remediation process
49. Is it required to sign the Disclosure of Employees or Officers of Boston Public Health Center letter? If so, can be a digital signature? Yes, digital signature is accepted.
50. Could the agency please clarify if Section List of Prime Contractors and Subcontractors are you referring to the prime/subcontractor that will perform the scope of work? It is BPHC goal to learn about subcontractors or outside vendors that might be brought on to this project. If the prime contractor does not have a sub-contractor. Just write "NA".
51. Section EVALUATION states the following: Proposer's financial ability to provide the services. Could the agency please clarify what kind of financial ability will be evaluated? It means that BPHC want to make sure that the vendor is in good standing with it finances.
52. Is it required to provide any kind of financial information to be in compliance with the evaluation? If so, please provide what information is required. All BPHC wants a statement that the vendor is in a good financial standing.
53. Is it required to provide the COI alongside the proposal response? No.
54. Could you the agency please grant an extension on the due date? No.
55. Does the agency accept remote resources to work on the project? Yes
56. Does the agency prefer on-site resources to execute the project? Yes
57. Does the agency require wet ink signatures? It is not required wet ink signatures at this time.
58. Is it allowed to use digital signatures to sign the forms? Yes
59. If the resources we provide at the time of proposal submission are not available at the time of a potential contract award could we replace them with equally qualified resources? No. BPHC require same resources which were proposed at the time of the bid.
60. Do the references need to be from higher education level? No
61. If we are using a subcontractor, can the subcontractor meet the minimum requirements? Everyone must meet the requirements.
62. Does the agency have a percentage established for MBE/DBE/WBE? All MBE/DBE/WBE have to be Commonwealth of Massachusetts registered CUBE vendor to receive extra points. https://www.mass.gov/orgs/supplier-diversity-office-sdo
63. If we are using a subcontractor, can the subcontractor meet MBE/DBE/WBE participation? MBE/DBE/WBE participation is not a requirement. However, If the prime vendor proposes an MBE/DBE/WBE sub-contractor. Please make sure that the sub-contractor is a Commonwealth of Massachusetts registered CUBE vendor. https://www.mass.gov/orgs/supplier-diversity-office-sdo
64. Will access be granted to internal network physically or remotely? Yes. Both. Please advise as we will need to determine if our team will have to travel to the location.
65. Is there a written set of cybersecurity policies and procedures already in place? Yes.

66. Is there currently annual cybersecurity awareness training for all staff? In Process
67. Has there been a cybersecurity assessment performed in the past and if so when? Yes 2013
68. Is it acceptable to use an assessment approach that is based on NIST 800-53 and also CFS, and HIPAA? Yes
69. How many physical buildings are involved. 26 Locations. Could you please separate out major facilities versus tiny outposts. 6 Large locations and 20 small locations.
70. How many facilities are HIPAA regulated? None.

Wireless Questions

1. How many physical locations will be tested? This is on the RFP
2. How many SSIDs will be tested? (Please list for each location) 2
3. What type of networks exist? (Corporate, Guest, BYOB) Corporate and Guest
4. Is BYOD in scope for this assessment? No.
5. Will the expectation be to assess the infrastructure of the wireless environment and access points or just identify rogue devices? Full assessment of wireless infrastructure.
6. Will we have a clearly identified list of wireless networks and devices that are expected? Yes.
7. Will Vendor have access to wireless controllers to perform assessments of environment? Yes.
8. Will this assessment need to be done onsite? We feel that most of wireless assessment would need to be done onsite.
9. How far apart are the ten locations? All locations are located in City of Boston.
10. What is your approximate number of Access Points in the scope? 145

Network Questions

1. Is there any authenticated testing to be included in the scope? Please refer to RFP
2. Is access to all sites possible from a single location? Yes

External Questions;

1. What technology is expected in an external scan of BPHC? We have no expectations. Vendor with best solution will be chosen.
2. Has BPHC experienced any issues from their external infrastructure impacting security and if yes what were they? No
3. Will a list of known services and domains be provided? No.
4. Is OSINT gathering of external IPs outside the BPHC scope expected and required? No.
5. Does BPHC uses any WAF or IDS that would our scans. If so, will BPHC agree to whitelist the attacking IP? Yes. Will discuss whitelisting.
6. Are externally facing servers hosted in-house or on cloud? Both

7. I wanted to clarify the meaning of external perimeter testing. Are you seeking supply chain cyber risk assessments in order to get a full view of that external perimeter? Yes.
8. Do you want any cloud environments tested such as Azure or Amazon Web Services? Yes. Azure
9. Are there any remote access services in use (on-demand VPN, GoTo my PC, LogMeIn, etc.)? VPN
10. How many employees have remote access? 500
11. Are there any in-bound modems (or remote access) in use? No
12. Do the "external scans" have to originate from within the U.S.? Yes
13. Regarding External Testing, how many DNS domains are included? BPHC.org and BostonEms.org (Ex: vpn.acme.com and rdp.acme.com are the same domain)

Internal Penetration Test:

1. Are BYOD in scope of this assessment? No
2. Has BPHC experienced any issues from their external infrastructure impacting security and if yes what were they? No
3. Do you have a mainframe or databases? yes. we have databases.
4. If exploitable vulnerabilities are discover by testers are exploits authorized beyond what is in the RFI? Yes. As long as it doesn't cause any issues with the system or application.
5. Will brute force and password spraying attacks be authorized? Yes.
6. Will DCC provided equipment accessed remotely be allowed for testing internally? Yes.
7. Will accounts be provided for internal testing? Yes.
8. Will this assessment need to be performed onsite? This is up to vendor.
9. For internal testing and database testing, can the organization provide remote access to the supplier to complete this work (e.g. a VPN, VDI, or other remote technology), or will this work be required to be performed onsite? Can be remote or local.
10. Reference paragraph C.1, what is the number of workstations and servers in the external and internal environments? Please refer to the RFP
11. Please confirm the Internal IP count - we see a total of 1,491 - is that correct? We estimate roughly 2000
12. Are we to ingest the customers' vulnerability assessment data or will they want to use our scan-on-behalf Qualys option for internal & external vulnerability scanning? The security vendors are supposed to used their own tools.
13. "Capture User Credentials": There are 4 vectors listed to obtain credentials. Are all 4 vectors required or just listed as examples? The vendor can use any methods to obtain credentials. Thus, we do not expect the vendor to use all the 4 vectors to obtain credentials. Keystroke logging is approached with extreme caution due to the potential to capture PII or PHI and if required, would need to be approached uniquely.
14. Are all of these devices a requirement for vulnerability testing? Or is this a list of potential scope? Due to the sensitive nature of some of these devices deployed in a production environment they should be approached with caution. If testing is required, a more focused testing approach would be required. The vendor is required to conduct security risk assessment based on the requirements listed in the RFP.
15. How many Internet facing hosts comprise the internal and external environment (servers, routers, firewalls, IDS/IPS)?

- How many servers are virtual and how many physical? 95 Virtual 35 Physical
- How many web servers? 20
- IDS/IPS – do you utilize one and if so, is it locally managed? Yes. Yes
- What other connected devices are in-scope? All

16. Can all work be reachable from one location? Yes.
    Please list all internal network segments in scope (management, production, development, DMZ, etc.). PC, Phone, Camera, Wireless, DMZ, Management, Servers.
17. Type of servers? Windows servers and one Linux. Windows 2008 to Windows 2022
18. How many users? 1600
19. Will BPHC provide hardware/laptops, etc., to perform the tasks outlined on pg. 7, paragraph 4 (e.g., Windows password hashes in-memory, keystroke logging)? No BPHC equipment will be provided to the vendor.
20. How many IP addresses are in scope for the internal penetration test? 2000
21. Are there any systems that would be tested which could be characterized as fragile (systems with tendency to crash)? No
22. How many hosts (endpoints) are in the network? Refer to RFP
23. How many sites/locations need to be tested? 26 Locations
24. If you have multiple locations, can their LANs all be reached via private connections (ex vpns, mpls, etc.)? Yes
25. Is the target environment primarily windows based, and if no, what technologies are used? This information can be provided to selected bidder
26. What is the approximate number of Internal host (desktops, laptops, etc..) to be tested? 1400
27. What is the approximate number of Internal Servers to be tested? 130

User Privilege Escalation:

1. Will accounts be provided for user privilege testing? No
2. What services are provided internally? Discussed during the project.
3. How will access be allowed (via BPHC provided equipment?) Both Vendor and BPHC Equipment

Segmentation Testing:

1. How many segmented networks are in place? 95 Vlans
2. Will architecture diagrams be provided? Yes
3. What is the escalation expectation if testers are able to escape segmented environment? Document Findings
4. What is segmented environment used for and what if any compliance is required (PCI, HIPPA, etc). Its not built out for security purposes.
5. What security controls are in place in segmented environment that testers should be aware of? Firewall for DMZ segment.
6. Will this assessment need to be performed onsite? Vendor's decision
7. For segmentation testing, how many networks are considered segmented/completely isolated? There are 95 Vlans None are completely isolated. Please define sample set of networks to be tested (e.g., routers, switches, firewalls).

8. The BHPC devices table states there are 95 VLANs. The description of this requirement states a sample of completely isolated/segmented networks. Can you please confirm that this requirement is for a subset of networks and not a segmentation test of all isolated networks. Subset of networks 10%

Application Testing Questions:

1. What are each of the 5 applications architecture and software stack? 4 of these are externally hosted. Serv-U runs on Windows.
2. Is static / dynamic code (SAST/DAST) testing required or just web application penetration testing (WAPT)? Web Application penetration testing
3. Are the 5 applications externally facing or internally? externally
4. How many web pages are each of the applications? This varies from 2-3 for Serv-U to 50 or more for Sharepoint.
5. Do each have a development environment? No.
6. What data type is processed through the applications? PHI data on clients.
7. Has a WAPT been performed on any of the 5 applications? No
8. Will it be a credentialed test or uncredentialed? uncredentialed
9. Are there APIs in place and are they in scope? No
10. Are these applications internally managed / owned or outsourced? If outsourced will the vendor be assisting or participating in the assessment? All are externally managed except Serv-U which we host.
11. Are these web applications and is BPHC expecting to perform authenticated scans? No.
12. Is the scope limited to running automated vulnerability scans against these web applications or is BPHC also expecting to perform a comprehensive Penetration test on each of these 5 critical applications? Perform comprehensive testing on these 5 applications.
13. Are the five in-scope applications internet accessible, or are they internal applications? Mix of Internal and External Applications
14. Will application and database testing be performed on production or non-production systems? Production environment
15. Are the applications in-scope standard web applications? Or are any of them thick-client style applications, or using non-browser based interfaces / APIs? All are standard web browser-based applications.
16. What is the number of applications does BPHC want in scope - mobile based or server based? 5 external applications
17. Do you want only scans on the 5 applications or a vulnerability assessment? Penetration testing must be conducted on the 5 external applications.
18. Would you like them tested with admin credentials? No.
19. Will BPHC provide scanning tools for applications and databases? BPHC will not provide any scanning tools.
20. Can you provide more detail on the five critical applications?
    a. What is their functionality? Patient information, Financial, and staffing work hours.
    b. How many live web pages are in scope for testing on each application? Approximately 100

21. How many web forms (pages) that require user interaction? from 2-3 for Serv-U to 50 or more for Sharepoint.
    a. What is the number and type of user roles? All applications have user roles based on department/job function as well as administrator roles.
22. How many web applications need to be tested? 5 applications
23. For each web application that needs to be tested please answer the following questions:
    a. What is this app used for? Patient information, Financial, and staffing work hours.
    b. Will the tests be authenticated and if so, how many roles will be tested? (Ex: if employees and customers use the app, there are likely at least 2 roles to be tested): unauthenticated.
24. Any mobile application within scope? No.
25. What is the purpose of the application and what are it's key functions? We don't feel this is needed to respond
26. What development environment has been utilized for the application (e.g. ASP.NET, PHP, J2EE etc.)? PHP
27. During testing will the application be a development/staging or live environment? Live
28. Approximately how many static web pages are there within the application? Unknown
29. Approximately how many unique dynamic pages are within the application? None
30. Approximately how many unique input fields are there? Unknown
31. What browser(s) has the site been designed for? Chrome and Edge
32. Does the site use Active X? No
33. Where is the application currently accessible from? (Internet, Intranet etc.) Internet and Internal
34. If the application is accessible from the Internet, please supply the URL (including HTTP/S prefix) We don't feel this is needed to respond
35. If not, will it be available from the Internet at the time of testing? Yes
36. Please qualify the timeframe(s) within which we are permitted access to the application. After 5pm.
37. Is the application hosted by a third party? Some
38. Other than from an unauthenticated perspective, does the application require test user credentials for the testing?? No.
39. Will dummy/Test user accounts be supplied? No
40. Will a hardware token be required to access the application? No
41. Approximately what percentage of the pages have forms? Unknown
42. Does the application allow users to upload files? Yes. Some have form and some allow uploads
43. Does the application pull content from any third party applications? No

Database Assessment:

1. What is the software of the databases? SQL and MySql
2. Is there a dev/test environment that testing will be performed in/on? No.
3. Will credentials be provided for testing? No.

4. What are the size and data types in each database? Size between 0.002 GB and 110.6 GB. Data types: Finance, EMS, ITS,…, etc
5. What security systems are in place currently (IBM Security Guardium, Imperva Data Security, etc) None.
6. Is there a dedicated team to support applications/data bases? Yes
7. Has there been any concerns of database breaches in the past? No.
8. Has an assessment been performed in the past and if yes will those reports be provided? No reports will be provided
9. Are the databases commercial "off the shelf solutions" (e.g. MS-SQL, Oracle, etc.)? Yes.
10. Is the Database and Network testing to be performed using authenticated or unauthenticated scanning? Unauthenticated scanning
11. Is the database assessment limited to testing or database reviews as well? Refer to the Database Assessment section in the RFP.
12. What kind of servers are the 16 database servers that need to be assessed in the database assessment? Microsoft Windows
13. For database assessments, would you like for us to scope from your environment or externally? It is up to the vendor.

Brute Force Attack:

1. Will the AD environment be accessible for this assessment? Yes.
2. Will this test be performed in a test environment or production? Production
3. Will password policies be provided for test? Yes.
4. Will this be done in coordination with the external and internal penetration test? Vendor decision
5. Will OSINT gathering of compromised passwords be expected for this assessment? Gathering of compromised passwords is expected for this assessment. The method used to perform this task is the vendor's decision.
6. Is there an expectation of this requirement being done in a live environment? Yes. Or can this be performed offline in an environment where the passwords are decoupled from usernames?
7. Do you want our pen tester to crack passwords, Yes if so how many, or can we use a tool to assess the strength of all passwords in a domain? Crack 10 passwords at most.

Social Engineering:

1. Does BPHC have an existing training and awareness program in place for their internal employees and external customers? Yes. But not deployed yet.
2. Are there any employees / customers out of scope for this assessment? No.
3. What are the objectives of this assessment? What are indicators of success? Understanding of Users awareness.
4. Can these attacks be done in coordination or as individual tests (Phishing, Employee Impersonation, Pretesting, etc) Either or Both
5. For Phishing, how many scenarios are in scope and how many staff are to be targeted? The phishing testing should include: Opening an attachment, clinking on a link, wire transfer scam, updating a password,…, etc. There are approximately 1400 BPHC employees

6. Employee impersonation and pretexting involves calling BPHC employees and both require an invented scenario and research. Can we club both these aspects to perform a common phone call or vishing campaign or is BPHC expecting employee impersonation be performed separately from Pretexting? BPHC expect the security vendor to perform Impersonation and Pretexting seperately.
7. For phone calls, what should be the employee sample size to whom we would make calls to? There are approximately 1400 BPHC employees
8. Will BPHC provide a list of recommended social engineering targets? No
9. What is the number of users in scope for Phishing assessment - how many email targets? 200 BPHC users
10. Do you want a single social engineering test or combined methodologies, resulting in multiple tests? Combined methodologies
11. How many employees are in scope for email social engineering? 200 BPHC users
12. How many employees are in scope for phone social engineering? 200 BPHC users
13. How many user mailboxes should be targeted? 200 BPHC users
14. How many users for vishing should be targeted? 200 BPHC users
15. How many total employees do you have and how many of them do you want Phished and Vished? There are approximately 1400 BPHC employees. We want to target 200 BPHC users for social engineering.

NIST Security Framework:

1. Is the specific NIST security framework 800-53v4 or the CSF? Either security framework would work.
2. Will each finding have an associated NIST security control and assessors evaluation of overall maturity? Please refer to RFP

Tactical vs. Strategic Recommendations:

1. Is the roadmap expected to include recommended courses of action if there is variability in decision making? AKA: Good, Better, Best? Yes.