Questions and Answers for Cybersecurity Risk Assessment and Plan

1. Is this fed grant work?

   Answer: No

2. Would you be able to provide us a timeline on when work is expected to start and end?

   Answer: Start two weeks after the contract is all setup.

3. Is there currently an incumbent company or previous incumbent, who completed similar contract performing these services?

   Answer: No

4. Is there any External Interface need to Pentest?

   Answer: No

5. Are any vendor products installed for Governance, Risk, and Compliance (GRC) tracking?

   Answer: No

6. Are any vendor products installed for Security Incident & Event Management (SIEM)?

   Answer: No

7. How many Active Directory Environment domain is included in Penetration testing?

   Answer: None.

8. Do you want this as a red team exercise to test the SOC/NOC's response where they will get to see the results and update their Knowledge Base (KB) afterward or Blue team where we work with the SOC/NOC and share our attacks so they can update their KB during the testing?

   Answer: No.

9. How many physical locations are included in Pen testing?

   Answer: None.

10. Is “web application” security testing in scope?

    Answer: The Assessment will consist of meetings with our internal staff to determine the security risks.

11. Do you manage your own data Center, or do you utilize any 3rd-party/colocation facilities?

    Answer: No

16. For the found vulnerabilities, Penetration testing need to be conducted?

    Answer: No

17. Do the vendor need to design CIS controls against the risk?

    Answer: Discover via Risk Assessment

18. Does the company host inhouse development team?

    Answer: No

19. Does BPHC require vulnerability scans to be done?

    Answer: No.

20. Does BPHC require penetration testing to be conducted?

    Answer: No.

21. Does BPHC require any social engineering campaigns to be conducted?

    Answer: No.

22. Besides the CCTV system review, does BPHC require physical access controls to be reviewed to sensitive areas?

    Answer: No.

23. Are there IT vendors that will need to be interviewed for any areas in scope?

    Answer: No.

24. Is the organization centralized (single entity) or does the organization have multiple (more than one) semi-autonomous business units, regions, etc.?

    Answer: Single Entity with 6 Bureaus, 23 Programs and 10 Service Centers

25. How is security coordinated across the organization?

    Answer: Discover via Risk Assessment

26. Have you implemented a formal information security program?

    Answer: No

27. What is the Network manufacturer?

    Answer: Cisco

28. Is there a DR site?

    Answer: No

29. Any 802.11based Wireless VoIP CPE?

    Answer: Yes

30. Is network segregated for data and voice?

    Answer: Yes

31. Is proper power (PoE) present?

    Answer: Unknown

32. How is E-911 configured and does it meet industry requirements?

    Answer: Unknown

33. How many media Gateways are present?

    Answer: None

34. Are there POTS lines at each location or are all calls forwarded out a central gateway?

    Answer: No

35. Who deployed the VoIP infrastructure?

    Answer: Unknown

36. Who owns the VoIP deployment (Data Team, Telephony Team, or a combination)?

    Answer: Network Team

37. Are you using Exchange, Office 365, or a hybrid?

    Answer: O365

38. What type of VoIP system is in use?

    Answer: Cisco

39. Can all internal networks be accessed from one internal network drop?

    Answer: Yes

40. Is wireless testing to include exploitation of client-side vulnerabilities?

    Answer: No.

41. Do you want social engineering to occur as part of this engagement?

    Answer: No.

42. How often do you update your security policies?

    Answer: When needed.

43. Have you implemented an information asset classification and management program?

    Answer: No.

44. Does it include data/information?

    Answer: No

45. Is your IT infrastructure/information assets centrally managed?

    Answer: Yes

46. Do you outsource any of your business functions that handle sensitive information?

    Answer: Unknown. Should be part of the Assessment.

47. Antivirus solution(s) deployed?

    Answer: Yes

48. Do you have documented organizational roles, responsibilities?

    Answer: Yes

49. Do you have documented security policies and procedures?

    Answer: Yes/No

50. How many security policies exist?

    Answer: 2

51. Do you have a documented inventory of assets, technologies, databases?

    Answer: Yes

52. Do you have a documented change management process?

    Answer: Yes

53. Do you anticipate that we will need to evaluate 3rd party applications and connectivity?

    Answer: Yes

54. Do you have a documented incident and breach response process?

    Answer: Yes

55. Do you have any timing issues or deadlines that will affect the project schedule?

    Answer: No

56. Are all devices able to be reached from a centralized location?

    Answer: No

57. Page 6, Item 1 Qualifications & Experience. Please confirm that we are not expected to include resumes in our response (it will be difficult to do so with the page limitations).

    Answer: All vendors are required to provide summary of experience and certifications each consultant.

58. Has the Boston Health Commission been assessed previously?

    Answer: No.

59. Is testing to include exploitation of vulnerabilities?

    Answer: No (i.e. penetration testing)

60. Do you have a mobility security strategy in place?

    Answer: No.

61. Do you develop your own mobile applications?

    Answer: No.

62. Is your internal network infrastructure segmented (e.g., firewalls or other access controls devices manage access to different part of the network)?

    Answer: Yes

63. What security technologies are in scope?

    Answer: All

64. Is a current network diagram maintained that identifies all system components and access points in scope?

    Answer: Yes

65. Have you conducted an information security assessment or audit of your environment within the past twelve months?

    Answer: No

66. Is the Cybersecurity Assessment performed evaluating NIST Cybersecurity standards to verify compliance with HIPAA regulations?

    Answer: Yes

67. Do you allow personally owned devices on your network?

    Answer: No.

68. Are any additional technologies in scope (ex. AS/400, mainframe, HSM, SAN, Citrix, ESXi, etc.)?

    Answer: No.

69. In the event you are considered a finalist in the process, will Boston Public Health negotiate contractual term in good faith for both parties?

    Answer: Yes, typically General Counsel will review the Contractual terms and negotiate in good faith for both parties.

70. Can attachments be included for terms and conditions to maintain the response to the 12-page limit or does the limit include terms and conditions?

    Answer: 12-page limit is only meant for the response. Therefore, you can include terms and condition which would not be counted towards the 12-page limit.

71. How many policies and procedures are in scope? Are these based on the NIST framework?

    Answer: 2 Policies. Unknown procedures

72. Has the Boston Public Health Commission evaluated what tier they currently fall into for framework implementation?

    Answer: No.

73. Has the Boston Public Health Commission identified a target tier?
    Answer: No.

74. Does the one-inch margin requirement include top and bottom as well as left and right?

    Answer: One-inch margin only includes top and bottom.

75. The RFP requests detailed descriptions for vendors' qualifications and approach (for example, "ensuring complete and detailed descriptions of the Firm's/Team's abilities to meet the requirement of this RFP" in section D). Would BPHC consider expanding the page limit to ensure detailed responses from vendors?

    Answer: The detailed responses page limit is 12. However, you can add Terms and condition, what our responsibilities are" and "what the clients responsibilities are" for each type of "investigation/activity" that will be occurring separately.

76. What is the approximate size of the facilities in scope (e.g. sq. feet, number of floors, etc.)?

    Answer: Unknown

77. The Final Evaluation Phase (Page 7 of 9) states that the preference for the interview is on-site. Given the ongoing pandemic, is the Boston Health Commission likely to favor video conference interviews?

    Answer: Yes, due to pandemic we will be conducting the interview via virtual video conference.

78. Will firm(s) who are selected have an opportunity to negotiate the terms and conditions, as listed in Attachment B, for the final contract?
    If so, should firms provide their own terms and conditions or provide feedback (redlines) of the attached terms and conditions within the submitted proposal.

    Answer: Yes, the vendor can provide their own terms and condition. However, the General Counsel will have the final say or will negotiate the terms and conditions.

79. If exploitation of vulnerabilities is to occur, do you have a “non-production” environment that can be utilized for exploitation testing?

    Answer: No.

80. Are security configuration reviews conducted on a regular basis (at least annually) for critical systems, infrastructure and devices?

    Answer: No.

81. Has BPHC completed a similar assessment in the past?

    Answer: No.

82. Is the Information Technology Services Department (ITSD) a department that is outside of BPHC?

    Answer: No.

83. Would the selected vendor be taking direction from ITSD or BPHC?

    Answer: ITS Department will help manage project with vendor.

84. Does BPHC require any of the work to be completed on-site?

    Answer: It all depends on the vendor proposal and how the vendor would complete the assessment and plan.

85. Is BPHC requiring a new SSP to be created or does BPHC intend for the selected vendor to update the existing SSP?

    Answer: Yes. This project should have new SSP created.

86. Does BPHC intend for the selected vendor to perform vulnerability scanning and penetration testing?

    Answer: No

87. The type (i.e. IIS, apache, etc.) and number of web server configurations to be reviewed.

    Answer: 3. Apache tomcat 7, IIS, Apache 2.4

88. How many applications that store, process, or transmit critical/sensitive/regulated are in your environment?

    Answer: ALL applications – estimate 30-35 are in our environment

89. Do you allow sensitive or regulated data to be transmitted, stored, accessed, or modified from mobile devices?

    Answer: Estimate – 6-10 (all cloud based allow access)

Infrastructure	**Count**
Server Hosts	30
Virtual Servers	160
Server and Storage Locations	7
Firewall/IDS Cluster	2
Firewall Rules	110
Firewall only	1
Switches	100
Layer 2 Switches	70
Routers	30
VPN Devices	1
Email Servers	0
SQL Databases	45
File Servers	4
Cameras	120
Wireless AP’s	61
Wireless Locations	5
Desktops/Laptops	1200
Ipads	27
Applications	45
Cloud Based Applications	10
Users	1400
Hosts	1100
Printers Canon MFD’s	67
Voip Phones	1200
Cell Phones	400
Non- Windows Servers (Unix OS)	1
Custom Developed Applications	0
Active Directory Domains	1
Wireless SSID’s (1 Private and 1 Public)	2
Physical Locations	25
IT Staff	22
Security Staff	1
External IP Addresses	10
Internal IP Addresses	2000
Call Manager	3
Unity	2
Emergency Responder	2
Presence and Contact Servers	0
VLANS	150