**Date:** January 18, 2021

**Title:** RFB/RFP #2022978304 Security Risk Assessment Services

**Subject:** Question and Answers

1. How many unique network locations are in scope for vulnerability analysis and penetration testing? All facilities owned and managed by Tarrant County Hospital District dba JPS Health Network are within scope for vulnerability analysis and penetration testing.
2. Please provide high level details of each network location. RFP calls out up to 12,000 IPs, can you break that down into:
   1. Network Location <x>
      1. Internal network: <xxxx> hosts
      2. External network: <xxxx> hosts

We will discuss with the selected Respondent after a contract is awarded.

1. For the “Penetration Test” after the assessment is completed, would you like us to attempt exploitation of identified vulnerabilities, or does the activity stop at the vulnerability identification, analysis, and risk rating stage (known exploit w/ CVSS)? Refer to Page 11, Section 2, Desired Elements, second bullet, first sub-bullet: *Perform simulated exploitations to confirm actual vulnerabilities and eliminate “false positives”*.
2. Do you have a Medical Device Security tool solution (e.g., Medigate, Asimily, Ordr) on your network already? We will discuss with the selected Respondent after a contract is awarded.
3. Can you confirm how many EHRs per year you would like assessed as part of the Promoting Interoperability Security Controls (formerly Meaningful Use) assessment? Epic is the electronic medical record system used by JPS.
4. Is the intent to have a PCI DSS Assessment performed and, if so, at what frequency? The risk assessment scope does not include a dedicated PCI DSS Assessment.
5. Page 10, Item 1.  Do you have an estimate of the number of policies that may need to be developed? Findings identified in the SRA final report will help determine any required changes to affected policies and procedures.
6. Page 12, Item 3.  Do you already have some type of Medical Device Security Program, or will this need to be developed from the beginning? We will discuss with the selected Respondent after a contract is awarded.
7. Page 14, Item 4.  For the CIRP Table-Top Exercise – is this a one-day (or part of one day) exercise?  How often does it occur – more than once a year? Refer to Page 14, Section 4, Scheduling.
8. Page 14, Item 5.  For the Business Impact Analysis – how many core divisions are to be included? Core divisions includes information technology, clinical/ambulatory care, ancillary services, compliance, human resources, law enforcement, and facility maintenance.
9. Page 14, Item 5.  For the Business Impact Analysis – how many types of systems (technology/applications) are in-scope? The scope includes systems and applications deemed critical to patient care and operations. A complete list of critical systems will be addressed after vendor selection and contract award.
10. Page 14, Item 5.  For the Business Impact Analysis (BIA) – Have you previously identified those systems deemed critical? A complete list of critical systems will be addressed after vendor selection and contract award.
11. Page 14, Item 5.  For the Business Impact Analysis – how many systems and applications have been identified as critical? A complete list of critical systems will be addressed after vendor selection and contract award.
12. Page 14, Item 5.  Will the BIA include more than critical systems? The scope includes systems and applications deemed critical to patient care and operations.
13. Page 14, Item 5.  Do you currently have a listing of all suppliers who would need to be included in the BIA? Supplier information will be addressed after vendor selection and contract award.
14. Page 14, Item 5.  For the Business Impact Analysis – how many personnel will need to be interviewed? An exact number of interview candidates is not available at this time, but the candidate mix should represent information technology, clinical/ambulatory care, ancillary services, compliance, human resources, law enforcement, and facility maintenance.
15. Page 11, Item 2.  Will a different environment be included in the semi-annual penetration tests or is it the same environment each time? We do not anticipate significant changes to our IP address blocks for the duration of this engagement.
16. Page 11, Item 2.  How many systems, servers, endpoints, firewalls, routers/switches, etc. are to be included during each semi-annual penetration test? The selected Respondent is responsible for hardware identification during the discovery phase of each scheduled penetration test.
17. Page 11, Item 2.  Is the semi-annual penetration test to include more than scans (which is what your wording is)? Refer to Page 11, Section 2, Desired Elements.
18. Page 11, Item 2.  Are you looking for a threat hunting component during the penetration test item you call “analyze network traffic” or is this for purposes of penetration testing analysis?  Refer to Page 11, Section 2, Purpose.
19. Page 13, Item 3.  How many medical devices are in-scope? An exact number of medical devices that transmit, store, process, access, or use protected health information will be discussed with the selected Respondent after a contract is awarded.
20. Page 14, Item 5.  BIA – How many departments are in-scope? Departments representing information technology, clinical/ambulatory care, ancillary services, compliance, human resources, law enforcement, and facility maintenance.
21. Can you provide access to the District Information Security Governance Framework or tell us what framework the District currently uses?  We will discuss with the selected Respondent after a contract is awarded.
22. Section II.C references PCI-DSS. Can you please clarify the scope of PCI services to be included in the assessments?  The risk assessment scope does not include a dedicated PCI DSS Assessment.
23. Section II. D.1: How many physical sites are included in the assessments and the general location of sites? All District facilities are within scope of the proposed Risk Assessment. Location of current District facilities is available at wwww.jpshealthnet.org.
24. Section II. D.2: Penetration Testing. Can you please verify if hosts subject to penetration testing are available from a central network location? The selected Respondent is responsible for hardware identification during the discovery phase of each scheduled penetration test.
25. Section B.3.b. – gives the due date as January 3, 2022. The Schedule on page 8 shows it is January 24, 2022. Please confirm the due date.  The response deadline – as stated on the RFP cover sheet and our public Internet website at https://www.jpshealthnet.org/rfp/security-risk-assessment-services-0 - is Monday January 24th, 2022, 2:00 p.m. CST. Consult the designated Contracts Administrator for further guidance.
26. Can the District clarify the information required in Tab 2. Company Background and how it differs from the information required in the Business Profile in Tab 3.  Consult the designated Contracts Administrator regarding Company Background requirements.
27. Is it possible for a vendor to bid on one or two of the services in the RFP or is it required that we bid on all five services listed in the RFP? Proposals must address all elements outlined in Section D. Scope of Services and Minimum Requirements.
28. To confirm, are you looking for this assessment to be all inclusive and ensure full compliance with HIPAA and PCI compliance requirements?  HIPAA compliance is the primary consideration, and notification of significant PCI compliance concerns is desirable. A PCI compliance risk assessment is not within scope of the services for this engagement.
29. If so, what level of PCI compliance is required currently? Refer to response in Question #30.
30. What has been the historical remediation time requirement?  i.e. 1-2 days or longer?  Note: this is heavily driven by the number of findings/gaps we identify.  This is difficult to estimate at this time without some reference point. Remediation by the selected Respondent is not within the scope of this engagement. We expect the selected Respondent to identify, document, and prioritize known issues as outlined within Section D. Scope of Services and Minimum Requirements. The District is responsible for remediation activities.
31. How many employees work for the entire institution (subs / affiliates included)? Our current workforce exceeds 10,000 persons including medical/clinical/operations staff, contractors, and volunteers. We are a teaching hospital and sponsor multiple resident, medical student, nursing, and allied health training programs.
32. Total Number of Full Time Equivalent (FTE) IT employees. The exact number of FTE’s will be discussed with the selected Respondent after a contract is awarded.
33. Have there been any changes to key IT management or any other key personnel in the past 12 months? Mr. Robert Earley retired as Chief Executive Officer in November 2021; he was succeeded by Dr. Karen Duncan effective January 1, 2022.
34. Is an MSP used for IT / Network Support?  If so, for what functions? We will discuss with the selected Respondent after a contract is awarded.
35. Have penetration tests and/or vulnerability scans been performed in the last 12 months?  We will discuss with the selected Respondent after a contract is awarded.
36. Has the institution completed a Cybersecurity Risk/Gap Assessment (or similar framework) in the past 12 months? If so, have you reached the required Maturity level? We will discuss with the selected Respondent after a contract is awarded.Has the Institution experienced IT related fraud or major events (outage, system change) in the last 12 months that we should be aware of? We will discuss with the selected Respondent after a contract is awarded.
37. How many key / in-scope applications are maintained on internally managed servers?  Please be specific for in-house vs hosted.  We will discuss with the selected Respondent after a contract is awarded.
38. Has the Institution implemented any sort of cloud-based services? (Office 365, Azure, AWS, etc.)? We will discuss with the selected Respondent after a contract is awarded.
39. Does the Institution use any SIEM monitoring applications or tools for the internal network?   We will discuss with the selected Respondent after a contract is awarded.
40. Have there been any changes in key vendors in the last year?  Are any such changes planned? We will discuss with the selected Respondent after a contract is awarded.
41. Have there been significant changes to network configuration, technology, or services in the last 12 months?  Are any such changes planned? We will discuss with the selected Respondent after a contract is awarded.
42. Does the institution perform any in-house application or code development?  If so, please explain. We will discuss with the selected Respondent after a contract is awarded.
43. Please indicate the number of the following items that are considered in-scope: # of Physical Servers # of Virtual Servers. We will discuss with the selected Respondent after a contract is awarded.
44. Please indicate the number of the following items that are considered in-scope: # of Total End Points # of Active AD Accounts. We will discuss with the selected Respondent after a contract is awarded.
45. How many total sub-net ranges will be included in the scans and related penetration test? We will discuss with the selected Respondent after a contract is awarded.
46. Will there be any time constraints on scanning or testing the internal network? If so, please indicate. We will discuss with the selected Respondent after a contract is awarded.
47. Has the organization removed local administrator rights for all domain users on local workstations and servers? We will discuss with the selected Respondent after a contract is awarded.
48. Has the institution implemented multi-factor authentication for privileged users? i.e. domain admins, key vendors, etc. We will discuss with the selected Respondent after a contract is awarded.
49. Will the organization allow testing to be performed with a secure BKD remote device (small form factor PC) accessible through a secure “TeamViewer” (or similar) secure connection? If no, please indicate preferred testing method. We will discuss with the selected Respondent after a contract is awarded.
50. Please indicate the total “number” of public IP address (including ranges) you would like to have tested.  We will discuss with the selected Respondent after a contract is awarded.
51. Please indicate the total “number” of internet domains registered to the organization. This information is publicly available through open discovery.
52. What is the brand of the institutions' Firewall(s)? We will discuss with the selected Respondent after a contract is awarded.
53. Does the Institution use external monitoring for the Firewall / IDS / IPS?    We will discuss with the selected Respondent after a contract is awarded.
54. How many medical devices are under management? We will discuss with the selected Respondent after a contract is awarded.
55. Who owns the medical device management process? We will discuss with the selected Respondent after a contract is awarded.
56. Do you outsource any part of the medical device management process (e.g., initial install, tracking, preventative maintenance, repair, upgrading, patching, FDA recalls, disposing, selling)? We will discuss with the selected Respondent after a contract is awarded.
57. What system or means do you track medical devices information (e.g., make, model, serial number, setup date, last touch date, preventative maintenance schedule, safety recalls, patching, depreciation life, end of life, end of service)? We will discuss with the selected Respondent after a contract is awarded.
58. Do you perform an IT security assessment prior to purchasing devices? We will discuss with the selected Respondent after a contract is awarded.
59. Do you have technical capabilities to segment and/or isolate devices on the network? We will discuss with the selected Respondent after a contract is awarded.
60. How many scenarios will be covered in each exercise?  We will discuss with the selected Respondent after a contract is awarded.
61. How long have the past sessions lasted, hours wise? We will discuss with the selected Respondent after a contract is awarded.
62. Do you have a formal list of scenarios to be covered each year?  If so, please confirm. We will discuss with the selected Respondent after a contract is awarded.
63. Is this considered an update to what has already been created or a start from scratch BIA project? We will discuss with the selected Respondent after a contract is awarded.
64. Has a tier ranking of critical systems already been performed? We will discuss with the selected Respondent after a contract is awarded.

All corrections, changes, additions, revisions, and/or clarifications in this Addendum #1 to the RFP are hereby made a part of the RFB/RFP for #2022978304 Security Risk Assessment Services.

All Respondents to the RFB/RFP shall acknowledge receipt and acceptance of this Addendum #1 by signing in the space provided and submitting the signed Addendum #1 with the RFB/RFP.

Proposals submitted without an executed copy of this Addendum #1 attached may be considered informal and may be rejected.

Received, acknowledged, and conditions agreed to on this \_\_\_\_\_\_\_\_\_ day of \_\_\_\_\_\_\_\_\_, 2022, by:

Respondent: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Company Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

If there are questions pertaining to this addendum please contact \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ at [Bid\_submissions@jpshealth.org](mailto:Bid_submissions@jpshealth.org)