ROANOKE COUNTY

Purchasing Division
5204 Bernard Drive, Suite 300-F, P.O. Box 29800
Roanoke, Virginia 24018-0798
TEL: (540) 772-2061 FAX: (540) 772-2074

May 12, 2022
ADDENDUM NO. 1 TO ALL BIDDERS/OFFERRORS:

Reference – RFP #2022-095

Description: Answers to Vendor Submitted Questions

RFP Issue Date: April 28, 2022 Proposal Due: May 26, 2022

The above Project is hereby changed as addressed below:

1. Will all potential vendors receive a copy of all submitted questions and answers, or just those they submit directly?
   Answer: This addendum covers all questions submitted by vendors regarding this project.

2. Would you consider an extension to this RFP in order to allow adequate time to respond?
   *Answer: We have extended the due date for this project to **May 26, 2022** at 2:00 PM EST.*

3. We understand that the submission method for this response is via hardcopy mail. Would you consider accepting email submission instead?
   As stated within the RFP, electronic submissions are not acceptable.

4. We also understand that as part of our response, we need to illustrate our financial condition. If we are unable to submit our entire response electronically, will you accept that our financial statements be emailed rather than mailed? It is our company's policy to submit financial information electronically and password protect financial statements to limit disclosure.
   *Answer: The Offeror shall submit as **Attachment 2**, a current annual financial report and the previous year's report and a statement regarding any recent or foreseeable mergers or acquisitions. Financial statements may be marked as "confidential" in accordance with the requirements set out in Section 3(G) of this RFP. Electronic submissions are not acceptable.*

5. Can the references be a mix and match from both prime and subcontractor?
   Answer: Yes.

6. Section 3.c.12: This section asks vendors to "Prospective Offerors should submit, at a minimum, a description of the marketing approach and promotions they intend to pursue to maximize revenues generated from the services or items requested in this RFP. Provide examples of any promotions or promotional materials. (See Attachment B)". This language seems to imply that the vendor will be required to engage in targeted marketing efforts of some kind, which would make sense if there were a right-to-hunt

type of RFP where the winning vendor they was able to position services to individual departments or agencies within the county. However, this RFP reads as though it is for a single project award. Can you please clarify the County's intent? I.e. is this RFP intended as a single project or are the requested services a catalogue of services that would be consumed across several different contracts/projects by various purchasing entities?
Answer: This section does not apply. The project will not be under a revenue-sharing model.

7. Is there a budget set for this project?
Answer: Roanoke County does not disclose budgetary items for projects.

8. Spend on this contract in the last financial year?
Answer: We are not prepared to disclose spending this project.

9. On PDF pg. 32, the RFP states that the offeror shall submit conditions and exceptions on Attachment 5. The attachment is not included in the RFP. Can you please provide?
Answer: Attachment 5 is an attachment created by the Offeror should they have conditions or exceptions to our sample contract (Attachment A).

10. Would County please provide some clarity around its references in Attachment B to "Attachments 1–7?" Are these intended to be separate documents, or are they just intended to be section titles within our proposal (Attachment B)?
Answer: These are to be separate documents developed by the Offeror containing the information as outlined.

11. Each such Offeror shall include in its proposal response the Identification Number issued to it by the Virginia State Corporation Commission (SCC) and should list its business entity name as it is listed with the SCC - Please clarify if subcontractors/ team members need to have an Identification Number issued to it by the Virginia State Corporation Commission (SCC)?
Answer: The primary contractor should provide their Virginia SCC number, if applicable.

12. Will minority and women owned small businesses be subject to additional points part of the evaluation criteria?
Answer: No, there are no set-asides for this project.

13. Is the non-mandatory pre-proposal conference recorded? If so, can parties receive a copy?
Answer: The pre-proposal conference was not recorded. Much of the information discussed has been outline in this addendum.

14. Is there a page limit for the proposal package?
Answer: No

15. Regarding Section 3 Instructions to Offerors, item J – we do not see a Fee Proposal Form in the RFP or on bid page for this solicitation. Can you please provide this form or guidance on how our pricing should be presented?
Answer: Vendors may submit their pricing in any format they feel applicable.

16. Is there currently an incumbent company or previous incumbent, who completed a similar contract performing these services? If so - are they eligible to bid on this project and can you please provide the incumbent contract number, dollar value, and period of performance?
Answer: We do not disclose this information.

17. When is the project intended to be awarded and what is the potential start date?
Answer: We anticipate making an award in August

18. By when would the project need to be completed?
Answer: November 1, 2022

19. Are the 128 IPs reference the range of IPs in the subnet, and if so, what is the estimated quantity of live hosts in each edge network?
Answer: We have 2 internet edges and each are assigned a /128 subnet. One subnet is using 80 IPS for host and the other is using 10 IPs. Each edge has 2 PAT addresses.

20. Are the number of users and the number of endpoint devices roughly the same? If not, what is the quantity of endpoints?
Answer: Approx. 1300 users and 1550 workstations.

21. Please verify endpoint configurations are not in scope for 'configuration reviews.'
Answer: Endpoint configuration review is not in scope.

22. What is the approximate quantity of MS servers (are these physical, virtual, or both)?
Answer: Both, 15 Physical and 215 virtual

23. What is the approximate quantity of virtual servers?
Answer: Approximately 234

24. Does the county manage its VMWare environment or is it hosted in a cloud provider or other service provider?
Answer: We manage our own VMWare environment.

25. What is the approximate quantity of network devices?
Answer: Approximately 150 switches, router and firewalls

26. Are there multiple networks?
Answer: Yes, we have multiple networks.

27. Internal and External Vulnerability assessments are included, as well as external penetration testing, please verify internal penetration testing is out of scope for this engagement.
Answer: Internal penetration testing is out of scope.

28. Does 'analyze controls that are in place' include a gap analysis against a specific regulatory or compliance standard?
Answer: No, we are looking for best practices.

29. Please confirm a wireless (WiFi) assessment is out of scope.
Answer: Wireless is out of scope.

30. If Wireless is in scope, how many physical locations and SSIDs are in scope?
Answer: Wireless is out of scope.

31. For configuration reviews, is an assessment against a known standard (i.e., CIS benchmark) acceptable?
Answer: Yes and, if possible, provide the CIS Benchmark assessments with NIST CSF mapping.

32. For server configuration reviews, would an assessment against the CIS configuration benchmarks be acceptable?
Answer: Yes and, if possible, provide the CIS Benchmark assessments with NIST CSF mapping.

33. Please confirm endpoint configuration reviews are out of scope.
Answer: We are only looking for router and firewall configuration reviews.

34. Any particular pain-points from the last contract if this is an existing contract?
Answer: None

35. Total number of live/active Internet facing IP addresses?
Answer: We have 2 internet edges and each are assigned a /128 subnet. One subnet is using 80 IPS for host and the other is using 10 IPs. Each edge has 2 PAT addresses.

36. Types of publicly accessible services (e.g. FTP, SFTP, SMTP)?
Answer: HTTP, HTTPS, FTP, SFTP, and SMTP

37. Which operating systems are in use?
Answer: Mostly Windows, a few Linux

38. Is the network segmented or flat?
Answer: Segmented

39. Can all networks/VLANs in scope be accessed from one network point?
Answer: Yes

40. Number of networks/VLANs in scope?
Answer: 350

41. Is there any Wireless capability?
Answer: Wireless is out of scope

42. Is the solution centrally configured?
Answer: Wireless is out of scope

43. Number of Access Points?
Answer: Wireless is out of scope

44. Number of SSIDs broadcasted?
Answer: Wireless is out of scope

45. Are 2.4Ghz, 5Ghz, or both frequencies broadcasted?
Answer: Wireless is out of scope

46. What types of authentication are in use, if any?
Answer: Wireless is out of scope

47. Where is geographical location of the internal environment?
Answer: Roanoke, Virginia

48. If there are multiple sites, where are the locations for each?
Answer: Roanoke, Virginia

49. Can all locations be accessed from one main site?
Answer: Yes

50. What are the number of common server builds that require a build review.
Answer: Windows 2012 R2, 2016, and 2019

51. Firewall Review/Rulebase Review?
Answer: Yes

52. Number of Firewalls including brands?
Answer: 2 Firewalls that need to reviewed and they are Cisco

53. Is the requirement for a full firewall configuration review and/or a rulebase review?
Answer: Full Fire Config review and Rules

54. Number of rules per rulebase/firewall?
Answer: Since this document is open to the public we do not feel comfortable answering.

55. Number of routers including brands?
Answer: 31, Cisco

56. Number of security/firewall rules in place (if any)?
Answer: Since this document is open to the public we do not feel comfortable answering.

57. How many external IP addresses are in scope for the pen test?
Answer: We have 2 internet edges and each are assigned a /128 subnet. One subnet is using 80 IPS for host and the other is using 10 IPs. Each edge has 2 PAT addresses.

58. Do you desire to do credentialed and non-credentialed vulnerability assessments?
Answer: Which ever gives us the best assessment.

59. Are you interested in having an assessment against NIST CSF completed as a part of analyzing controls in place? The framework is a great match for doing that along with planning a desired future state.
Answer: Yes

60. Can this engagement be done fully remote?
Answer: Yes

61. Section 6, please define the details regarding the request for “analyze controls that are in place”.
Answer: Analyze Logging, alerting or automation that helps maintain the cyber security of our infrastructure.

62. Is the customer able to provide softcopies of the DMZ and Network Architecture for design reviews, or do they require on site access?
Answer: We can supply a soft copy.

63. Is the customer able to provide softcopies or remote access for a Virtual Infrastructure Security Assessment or do they require on site access?
Answer: We can give remote access.

64. Is the server configurations available as a softcopy or remote access or do they require on site access?
Answer: We can give remote access.

65. Is the firewall and router configurations available as a softcopy or remote access or do they require on site access?
Answer: We can give remote access.

66. Does the work need to be performed onsite or can it be performed remotely from onshore locations?
Answer: US Only

67. Can work be performed and supported from locations outside the United States as well?
Answer: US only

68. What are the requirements for reporting as far as output for all informational, low, medium, and high findings?
Answer: No requirement

69. What are the plans for remediation after all the Internal/External and all Environments have been tested and scanned?
Answer: No Plans at this time

70. Is there a specific format that is required or a general report shall suffice for completion of VAPT and Executive Reporting?
Answer: No requirement

71. How many resources can be allocated for this VAPT RFP (i.e., One Penetration Subject Matter Expert, One Project Manager, etc....)?
Answer: No limit.

72. What’s your headcount of users (employees + contractors + interns)? What number/percentage of your workforce resides within organizational facilities? What number/percentage works remotely?
Answer: 1300 end-users, 200 remote users

73. How much (%) of the infrastructure is in the cloud?
Answer: 10%

74. How many physical locations?
Answer: Around 30

75. What is the aggregate Internet Capacity per location (<300mbps, <1gbps, <4gbps, up to 10gbps)?
Answer: Currently 300 Mbps and 200 Mbps

76. Do you manage your own data Center, or do you utilize any 3rd-party/colocation facilities?
Answer: We Manage

77. Do current network maps exist?
Answer: Yes

78. Do the network maps contain segmentation information?
Answer: No

79. Do any cloud environments fall under this review?
Answer: No

80. How many virtual hosts exist?
Answer: 13

81. How many physical locations exist for the virtual hosts?
Answer: Two

82. Are servers deployed from a gold image to ensure consistency?
Answer: Since this document is open to the public we do not feel comfortable answering.

83. Do network changes follow a formalize change control process?
Answer: Since this document is open to the public we do not feel comfortable answering.

84. Are changes to configuration logged in a centralized logging tool (SIEM, etc.)?
Answer: Since this document is open to the public we do not feel comfortable answering.

85. Will the internal vulnerability scan include penetration testing, similar to the External Penetration Assessment requested?
Answer: No Internal Pen Test

86. How many external services are web only (HTTP and HTTPS)?
Answer: Most of the services are Web Only.

87. Will the External Penetration testing include social engineering testing (i.e., phishing, vishing)? If so, how many employees will be considered as part of the social engineering test?
Answer: No, Social Engineering test needed.

88. How many DMZ or network design reviews will be included in-scope?
Answer: Approximately 20 DMZ

89. How many different server operating system will be assessed? (i.e., Windows, Linux, AIX, etc.)
Answer: Mostly Windows with some Linux

90. Section 6: How many site-2-site VPN's are in place?
Answer: 20

91. Section 6: Regarding configuration reviews, are you comfortable with using a sampling approach of the servers or do you want all instances reviewed? If a sample approach is acceptable, what percentage would you like to see?
Answer: Yes we are open to that. 20% sampled

92. What framework do you want to use for the control's evaluation (NIST 800-53?)
Answer: The formal framework preferred would be NIST CSF with mapping/references to NIST 800-53 as applicable.

93. Are the controls to be evaluated from an organizational level or from a systems level or both?
Answer: System Level

94. Is the external pentest a Blackbox test with no credentials?
Answer: No

95. Does it include any externally facing web applications, APIs, or mobile applications?
Answer: 44 Public facing web site. No mobile apps and no APIs

96. Are there any externally facing industrial control systems such as traffic management systems, Water systems, etc?
Answer: No

97. Which cloud services are being used (Azure, AWS, Google)?
Answer: Out of scope

98. How many SaaS services are being used?
Answer: Out of scope

99. What departments are in scope? Administration? Public services?
Answer: Both

100. When was the last project of this nature performed and who performed it?
Answer: Since this document is open to the public we do not feel comfortable answering.

101. Do you have a documented incident and breach response process?
Answer: Since this document is open to the public we do not feel comfortable answering.

102. Is County's IT organization centralized or decentralized?
Answer: Centralized

103. Is this penetration testing due to any regulatory requirements?
Answer: No

104. Do you have a vulnerability management technology you use? If so, what technology?
Answer: No

105. Would you want us to run our own vulnerability management technology?
Answer: No

106. Do you have an asset inventory on what devices are in scope to run vulnerability scans against?
Answer: Yes

107. Any devices out of scope (printers, phones, conference booking room systems, etc)?
Answer: No

108. Do you have a network topology?
Answer: Yes

Note: A signed acknowledgment of this addendum must be received at the location indicated on the original solicitation either prior to the proposal due date or attached to your proposal. Signature on this addendum does not substitute for your signature on the original proposal/bid document. The original proposal/bid document must be signed.

Thank you,

Neil Huss
Phone: (540) 283-8151
nhuss@roanokecountyva.gov

Sign Name:	Print Name:
Name of Firm:	Date: