*PURCHASING DEPARTMENT N*ewport News Public Schools

757-591-4525/(F) 757-591-4593 12465 WARWICK BOULEVARD • NEWPORT NEWS, VA 23606-3041

December 15, 2022
Addendum #3
FOR IMMEDIATE ATTENTION

ADDENDUM NO. 3 TO ALL BIDDERS:

Reference – Request for Proposal:	Vulnerability and Penetration Testing RFP# 007-0-2023/AP
For Delivery To:	Newport News Public Schools
Proposals Due:	**Wednesday, January 11, 2023 at 2:00 PM EST**

The above-referenced RFP is hereby amended and clarified as follows:

This addendum includes the following: addition of quantities clause to general requirements, and provide responses to questions from vendors

1. **Pg.4, Statement of Needs, General Requirements (Add quantites clause below)**

   Add: #11. Quantities: Any quantities provided are for estimating purposes only and by no means obligates Newport News Public Schools.

   Responses to Offerors' Questions:

1. Are you requiring past performance in the PK-12 education space or can experience with state/local governments suffice?

   RESPONSE: Experience in the PK-12 space is preferred. Experience with state/local governments is acceptable.

2. Will a D&B report be sufficient to demonstrate financial status and capacity?

   RESPONSE: Please include Duns and Bradstreet (D&B) report to demonstrate financial status. If the D&B is not comprehensive enough, we still may ask for SOC1 or additional information, if shortlisted.

3. How do you want pricing for optional services provided since there is no space for it on the Pricing Schedule?

   RESPONSE: Please provide an hourly rate for optional services as well a separate proposal upon request.
4. Is a surety bond required (see Number 15, page 29)?

   RESPONSE: No, a surety bond is not required.

5. Are you seeking a full controls assessment (e.g.; interview based (e.g., interview-based review covering a control framework, such as NIST CSF?

   RESPONSE: We are seeking a full controls assessment based on the NIST Cybersecurity Framework with the long-term goal of 800-53.

6. Web Applications: How many web applications are in scope?

   RESPONSE: 10

7. Web Applications: What is their approximate size? e.g., number of active pages, web forms, user roles?

   RESPONSE: Varies by application. 10 to 20 pages on average per application.

8. External Penetration Testing: How many IP addresses are in scope?

   RESPONSE: 254 IP addresses. CIDR: /24

9. Internal Penetration Testing: How many IP addresses are in scope?

   RESPONSE: Internal – Up to 64,000 addresses
   (1x - /16 networks).

   Ideally, we would like to review our entire network for potential vulnerabilities. We are open to narrowing down the scope to a smaller subset of devices and or/network segments. Please provide specific details on pricing/costs for both options

10. Wireless Penetration Testing: How many locations are in scope?

    RESPONSE: 10

11. Wireless Penetration Testing: How many networks are at each location?

    RESPONSE: 6 wireless SSIDs.

12. Firewall Review: How many firewalls are in scope?

    RESPONSE: 48

13. Firewall Review: What make and model?

    RESPONSE: Checkpoint Large Enterprise Security Gateways and Fortinet FortiGate mid-range next-generation firewalls (NGFW). Specific details related to the Model / OS / Software versions are not able to be disclosed publicly.

14. Firewall Review: How many firewall rules need to be reviewed?

    RESPONSE: 300-400 rules/policies will need to be reviewed across firewall platforms. Please provide pricing on a per-rule or quantity basis.

15. Security Policies: How many policies do you currently have?

    RESPONSE: 15 total for review. We are looking to have existing policies reviewed along with identifying any gaps.

16. Security Policies: Are you open to pricing on a per-policy basis for policy development and enhancement?

    RESPONSE: Yes.

17. Cloud Assessment: What cloud applications are in scope?

    RESPONSE: 6 SaaS.

18. Cloud Assessment: How many tenants for each cloud are in scope?

    RESPONSE: 1

19. Cloud Assessment: How many subscriptions for each cloud are in scope?

    RESPONSE: 1

20. HVAC Systems and CCTV Systems: How many users are in scope for social engineering?

    RESPONSE: 1,000. Please provide pricing either per user or by quantity.

21. HVAC Systems and CCTV Systems: What social engineering methods are you open to (e.g., phishing, vishing, USB drops, etc.)?

    RESPONSE: Spear Phishing, Phishing, Vishing, **USB Drops**

22. Physical Penetration: How many sites are in scope for physical penetration?

    RESPONSE: 10

23. Physical Penetration: What is your goal for this assessment?

    RESPONSE: Identify and evaluate physical security risks to each type of school division buildings' access control systems (Security Cameras, Alarm Systems, Etc.).

24. Physical Penetration: Are you trying to meet any compliance goals?

    RESPONSE: None.

25. Physical Penetration: Is this in response to a recent physical security concern?

    RESPONSE: No.

26. Physical Penetration: Are you seeking us to review physical security policies?

    RESPONSE: No.

27. I understand that the report is due NLT 4 weeks post assessment, however, I am looking for a timeline of execution?

    RESPONSE: The major project deliverables requested in the RFP (III. Statement of Needs, B. Specific Requirements) can be broken into individual project deliverables. Each deliverable will be due NLT 4 weeks after completion unless otherwise agreed upon.

    The estimated contract award date is sometime late in February or early March 2023. We anticipate the project to start shortly thereafter and run through the remainder of the year.

28. What are the number of the firewalls in the environment?
    RESPONSE: 48

29. Are there any cloud services utilized that are in-scope?

    RESPONSE: Yes. A list of cloud providers will be provided to the awarded contractor.

30. What are the number of WiFi networks defined?

    RESPONSE: There are 6 wireless SSIDs.

31. What is the number of active devices on the network?

    RESPONSE: The network averages between 30,000-40,000 devices.

32. What are the number of network segments?

    RESPONSE: We are unable to disclose that information publicly.

33. Is the IT organization centralized or decentralized?

    RESPONSE: Our IT organization is centralized.

34. Has NNPS had this type of audit performed in the past?

    RESPONSE: Yes.

35. Has a security control framework been adopted? If yes, which one?

    RESPONSE: NIST Cybersecurity Framework (CSF)

36. How many full-time IT staff are there?

    RESPONSE: 100+

37. External Network Vulnerability Assessment and Penetration Test: Approximately how many IPs or subnets are in scope?

    RESPONSE: 254 IP addresses. CIDR: /24

38. External Network Vulnerability Assessment and Penetration Test: Is exploit testing included in the external/internal network vulnerability scans?

    RESPONSE: Yes, external applications should be tested for exploits.

39. Internal Network Vulnerability Assessment and Penetration Test: Approximately how many IPs or subnets are in scope?

    RESPONSE: Internal – Up to 64,000 addresses (1x - /16 networks).

    Ideally, we would like to review our entire network for potential vulnerabilities. We are open to narrowing down the scope to a smaller subset of devices and or/network segments. Please provide specific details on pricing/costs for both options.

    Specific details such as IP addresses, network segments and host names are not shared with the public.

40. Internal Network Vulnerability Assessment and Penetration Test: Can all network testing be done from a single location?

    RESPONSE: To perform testing on all requested network segments, the visitation of multiple sites maybe required. All the sites are located within the city of Newport News.

41. Firewall Evaluation: Excluding redundant or firewalls running in HA mode, how many firewalls are in scope?

    RESPONSE: 47

42. Web Applications: How many web applications are in scope?

    RESPONSE: 10

43. Web Applications: Are the web applications internet-facing or internal only?

    RESPONSE: There is a mix of internal and internet-facing web applications.

44. Enterprise Application Testing: How many enterprise applications are included in the scope for the risk assessment?

    RESPONSE: 10

45. Wireless Penetration Testing: Is the wireless network controller-based or access-point-based?

    RESPONSE: Access Point Based

46. Wireless Penetration Testing: How many locations are in scope for wireless network testing?

    RESPONSE: This is a division wide project, and locations may vary amongst various NNPS offices and schools.

47. Security Awareness and Social Engineering Testing: What type of social engineering activities is NNPS interested in, e.g., email phishing, vishing, smishing, tailgating?

    RESPONSE: Spear Phishing, Phishing, Vishing, **USB Drops**

48. Security Awareness and Social Engineering Testing: Please provide the number of targets for each type of testing that will be in scope.

    RESPONSE: Security Awareness – 4500, Social Engineering – 1,000

49. Cloud Security Configuration Review: What types of cloud services (IaaS, PaaS, SaaS), is the cloud security review focused on?

    RESPONSE: For this assessment, the focus will be on SaaS services that the school division utilizes.

50. Cloud Security Configuration Review: If SaaS, how many applications are in scope?

    RESPONSE: 6

51. Information Security Policies and Data Governance: Are there documented IT policies, procedures, standards, and guidelines in place? If so, how many?

    RESPONSE: 15 documents.

52. Data Centers: How many data centers are in scope for testing?

    RESPONSE: 2 datacenters.

53. Presentation of Proprietary Information: On page 13, Section V. General Terms and Conditions, Subsection C. Proprietary Information/Non-Disclosure, 3 it states that vendors should *Submit trade secrets or other proprietary information under separate cover in a sealed envelope clearly marked "PROPRIETARY."*
    Please clarify | confirm that a complete and separate proposal document that includes the proprietary information should be provided in addition to a redacted version of the same document, or does NNPS prefer that *only* proprietary information be included in the "PROPRIETARY" envelope and only non-proprietary information be provided in the original proposal?

    RESPONSE: It is at the discretion of the Offeror. Please review page 12, V. General Terms and Conditions,C. Proprietary Information/Non-Disclosure.

54. Presentation of Anti-collision, Nondiscrimination, and Drug-free Workplace Form, Contractor Questionnaire Form, and Sample Reports: Is it permissible to place the Anti-collision, Nondiscrimination, and Drug-free workplace Form, the Contractor Questionnaire Form, and the sample reports in an appendix, or does NNPS prefer that they be included in the body of the proposal document (e.g., Tab 3 Deliverables as specified in the proposal submittal requirements)

    RESPONSE: The only requirement is that the proposal submission includes these documents.

55. Pricing Schedule/Scope Item: How should the optional items be reflected in the pricing schedule as there are no line items included in the Schedule?

    RESPONSE: RESPONSE: Please provide an hourly rate for optional services as well a separate proposal upon request.

56. Pricing Schedule/Scope Item: During the pre-proposal conference, there was discussion as to what is involved in the following: *The qualified Contractor will perform an audit of the identified data systems and networks using an objective vendor-neutral framework (NIST 800-53), conduct penetration testing, and provide a report with recommended remediation options.*
    Is a comprehensive NIST 800-53 audit required, and is this audit at the enterprise level or per school division?

    RESPONSE: We would like the review done at the enterprise level. Current processes are aligned to the NIST Cybersecurity Framework. Our long-term goal is to align with the 800-53 controls.

57. Pricing Schedule/Scope Item: If a full NIST 800-53 audit is required, how should this be reflected in the pricing proposal as there is no line item included in the Pricing Schedule?

    RESPONSE: Current processes are aligned to the NIST Cybersecurity Framework. Our long-term goal is to align with the 800-53 controls. Pricing and scope of work should reflect our current environment along with a potential roadmap/recommendations to reach 800-53 compliance.

58. What is the Federal grant program funding this work? Since Federal grants often come with associated Federal government requirements that grant recipients and their vendors must adhere to, vendors must be able to incorporate those requirements into their proposals for NNPS.

    RESPONSE: NNPS will be utilizing CARES Act funding for this work.

59. What is the projected/estimated contract award date for RFP # 007-0-2023/AP?

    RESPONSE: Being that December is a short working month for NNPS, the estimated contract award date is sometime late January, early February.

60. What is the expected and/or desired period of performance for the work required under RFP#007-0-2023/AP?

    RESPONSE: The estimated contract award date is sometime late February or early March 2023. We anticipate the project to start shortly thereafter and run through the remainder of the year.

61. What is the timeline (with expected deadlines) for all deliverables under the contract to be awarded under RFP 007-0-2023/AP?

    RESPONSE: The major project deliverables requested in the RFP (III. Statement of Needs, B. Specific Requirements) can be broken into individual project deliverables. Each deliverable will be due NLT 4 weeks after completion unless otherwise agreed upon.

    The estimated contract award date is sometime late February or early March 2023. We anticipate the project to start shortly thereafter and run through the remainder of the year.

62. How and when will the requirements discussed on 08 November 22 preproposal conference be shared with vendors?

    RESPONSE: The question period closes November 14, 2022 at 12 PM EST. An addendum will be released publicly to www.eva.virginia.gov and the NNPS purchasing website http://sbo.nn.k12.va.us/purchasing/current_solicitations.html following the receipt of responses from the IT department.

63. What are the required skills that NNPS will require for the personnel who delivers the vendor proposed solution?

    RESPONSE: There are no specific skill requirements or certifications required. The contractor should describe in detail its experience in conducting cybersecurity audits in the State, Local, and Education (SLED) market. The contractor should be able to provide a detailed description of the experience and qualifications of the consultants to work on this project, including relevant industry certifications, length of time in the field, areas of specialization, and experience relevant to the deliverables in the RFP.

64. Will NNPS allow for change orders? These requirements appear very complex and we would like to understand the post-award process upon the identification of new information that changes the circumstances under which the requirements were originally set.

    RESPONSE: Any request for change affecting price, quality, quantity, delivery or cancellation will need to be communicated to the Contract Administrator in writing . The change order will be evaluated and approved by the Contract Administrator. No change order work shall commence until a Change PO is authorized and it is received by the Contractor.

65. What amount of additional funds are available to accommodate future NNPS contract change orders for these requirements?

    RESPONSE: The requested budgetary information is not shared to the public.

66. Please provide the results and report for the most recent assessment of a similar nature to the requirements of RFP # 007-0-2023/AP.

    RESPONSE: The requested results/reports from previous assessments are not shared to the public.

67. Firewall Evaluation: How many firewalls?

    RESPONSE: 48

68. Firewall Evaluation: How many rules are there per fire wall?

    RESPONSE: 300-400 rules/policies will need to be reviewed across firewall platforms. Please provide pricing on a per-rule or quantity basis.

69. Firewall Evaluation: Provide firewall HW/SW/OS version.

    RESPONSE: Checkpoint Large Enterprise Security Gateways and Fortinet FortiGate mid-range next-generation firewalls (NGFW). Specific details related to the Model / OS / Software versions are not able to be disclosed publicly.

70. Information Security Policies and Data Governance General Requirements: About how many policies are there and about how long is each document on average?

    RESPONSE: 15 Policies / Documents for review. Polices range from between 3-10 pages on average.

71. Information Security Policies and Data Governance General Requirements: Which state, local, and federal laws has the program been built against?

    RESPONSE: Children's Internet Protection APP ("CIPA"), Children's Online Privacy Protection Rule ("COPPA"), Virginia Freedom of Information Act (FOIA), Virginia Consumer Data Protection Act ("VCDPA"), Health Insurance Portability and Accountability Act ("HIPAA"),
    Family Educational Rights and Privacy Act ("FERPA").

72. Security Policies: About how many policies are there and about how long is each document on average?

    RESPONSE: 15 Policies / Documents for review. Policies range from between 3-10 pages on average.

73. External Penetration Scope: Please list in scope network ranges, IP addresses, and/or host names to be tested.

    RESPONSE: A total of 254 IP addresses. CIDR: /24

74. External Penetration Test Scope: Please list any hosts and/or networks that should be excluded from the test.

    RESPONSE: The requested network/host information is not shared with the public. A list of excluded hosts/networks will be provided to the awarded Contractor.

75. External Penetration Test Scope: Please list external domains to target.

    RESPONSE: nn.k12.va.us, nnschools.org

76. External Penetration Test Scope: Please list external domains to target.

    RESPONSE: nn.k12.va.us, nnschools.org

77. External Penetration Test Scope: Please list any SAAS (software as a service), or similar in use.

    RESPONSE: Microsoft, Google

78. External Penetration Test Scope: Are there any (intrusion Detection/Intrusion Prevention) or WAFs (Web Application Firewalls) that could affect testing?

    RESPONSE: IPS/IDS technologies are in use. Exceptions can be made if needed for the assessment.

79. External Penetration Test Scope: Has this environment received testing in the past? If so, when was the most recent test?

    RESPONSE: Yes. Additional details are not shared with the public.

80. Internal Penetration Test Scope: Please list in scope network ranges, IP addresses, and/or hostnames to be tested

    RESPONSE: Internal – Up to 64,000 addresses (1x - /16 networks).

    Ideally, we would like to review our entire network for potential vulnerabilities. We are open to narrowing down the scope to a smaller subset of devices and or/network segments. Please provide specific details on pricing/costs for both options

81. Internal Penetration Test Scope: Please list any hosts and/or networks that should be excluded from the test.
    RESPONSE: The requested network/host information is not shared with the public. A list of excluded hosts/networks will be provided to the awarded Contractor.

82. Internal Penetration Test Scope: Man-in-the Middle (MiTM) Testing.

    RESPONSE: MiTM is within scope of this assessment. Please provide specific details for pricing/cost.

83. Internal Penetration Test Scope: Please list source locations for the testing.

    RESPONSE: Specific details such as IP addresses, network segments and host names are not shared with the public. Please provide specific details on pricing/costs, either by host, IP address or network segment.

84. Internal Penetration Test Scope: Has the environment received testing in the past? If so, when was the most recent test?

    RESPONSE: Yes. Additional details are not shared with the public.

85. Internal Penetration Test Scope: What is the account lockout policy?

    RESPONSE: The requested policy information is not shared with the public.

86. Internal Penetration Test Scope: Should Tevora attempt to dump Active Directory hashes if sufficient access to do so is acquired?

    RESPONSE: Yes.

87. Wireless Network Test Scope: Please list in scope target SSIDs.

    RESPONSE: There are 6 SSIDs in total that need to be tested.

88. Vulnerability Assessment Scope: Please list in scope network ranges, IP addresses, and/or host names to be tested.

    RESPONSE: External - 254 IP addresses (1x /24 network). Internal – Up to 64,000 addresses (1x - /16 networks).

    Specific details such as IP addresses and host names are not shared with the public. Please provide specific details on pricing/costs for scanning.

89. Vulnerability Assessment Scope: Please list any hosts and/or networks that should be excluded from the test.

    RESPONSE: The requested excluded network/host information is not shared with the public. A list of excluded hosts/networks will be provided to the awarded Contractor.

90. Vulnerability Assessment Scope: Please list source locations.

    RESPONSE: The requested source location information is not shared with the public.

91. Cloud Infrastructure Scope: Please list any hostnames or IPs of publicly facing compute instances, load balancers, or other public endpoints.

    RESPONSE: None

92. Cloud Infrastructure Scope: Please list any storage buckets, such as Amazon S3 or Google Cloud Storage, in use.

    RESPONSE: None

93. Cloud Infrastructure Scope: Please list any cloud native services in use, such as AWS Lambda, AWS RDS, Google Kubernetes Engine, etc.

    RESPONSE: Microsoft. Specific cloud-native services will be provided to the awarded contractor.

94. Cloud Infrastructure Scope: Wil Tevora be provided read only accounts to the scoped cloud environment(s)?

    RESPONSE: Read-only access to the cloud environment can be provided if required for the assessment.

95. Cloud Infrastructure Scope: What environment will be used for testing? For example, prod, dev, stage, internal, etc.)

    RESPONSE: Variable on the application being tested.

96. Cloud Infrastructure Scope: Please list public domains. If no domains are given Tevora will attempt to discover domains during testing.

    RESPONSE: nn.k12.va.us, nnschools.org

97. Cloud Infrastructure Scope: Has this environment received testing in the past? If so, when was the most recent test?

    RESPONSE: No.

98. Web Application Scope: Please list the base URLs of the Web applications and/or services to be tested. Include hostnames and nonstandard ports.

    RESPONSE: Specific web application details are not disclosed to the public.

99. Web Application Scope: What environment will be used for testing? For example, prod, dev, stage, internal, etc.)

    RESPONSE: The testing environment is variable per application.

100. Web Application Scope: Approximately how many unique dynamic endpoints/pages does the application have?

    RESPONSE: Varies by application. 10-20 pages on average per application.

101. Web Application Scope: Please specify test account details for in scope applications.

RESPONSE: Test account details will not be disclosed to the public. The account information will be provided to the awarded contractor.

102. Web Application Scope: Are there any (Web Application Firewalls) or rate limiting policies that could affect testing?

RESPONSE: Yes. Exceptions can be made if needed for testing.

103. Web Application Scope: List any forms or URLs that could be sensitive to fuzzing e.g. a form which sends an email or triggers a manual process.

RESPONSE: Specific web form details are not disclosed to the public.

104. Web Application Scope: How many user roles will be in scope for testing?

RESPONSE: 4 roles-per application.

105. Web Application Scope: Is the application multi-tenant?

RESPONSE: No.

106. Web Application Scope: Has this application received testing in the past? If so, when was the most recent test?

RESPONSE: No.

107. API Scope: Please list the base URLs of the APIs to be tested. Include host names and nonstandard ports.

RESPONSE: Test account details will are not disclosed to the public. The account information will be provided to the awarded contractor.

108. API Scope: Please describe the intended/expected use cases for the API.

RESPONSE: NNPS only utilizes third-party API's to connect applications. We do not have our own API.

109. API Scope: What environment will be used for testing? For example, prod, dev, stage, internal, etc.).

RESPONSE: None, as we do not have any in-hose API's.

110. API Scope: Please specify the credentials for the API applications.

RESPONSE: Account details are not disclosed to the public. The account information will be provided to the awarded contractor.

111. API Scope: What API documentation and/or code examples will be made available for testing?

RESPONSE: Information will be provided for any third-Party API integration between applications used by the school division.

112. API Scope: Please list applications that interact with the API and describe their intended use.

RESPONSE: Specific application details related are not disclosed to the public. The account information will be provided to the awarded contractor.

113. API Scope: Are there any (Web Application Firewalls) or rate limiting policies that could affect testing?

RESPONSE: None.

114. API Scope: List any forms or URLs that could be sensitive to fuzzing e.g. a form which sends an email or triggers a manual process.

RESPONSE: Specific URL and Forum details are not disclosed to the public. This information will be provided to the awarded Contractor.

115. API Scope: How many user roles will be used in scope for testing?

RESPONSE: Not applicable for this assessment.

116. API Scope: Is the API multi-tenant?

RESPONSE: Not applicable for this assessment.

117. API Scope: Has this application received testing in the past? If so, when was the most recent test?

RESPONSE: Not applicable for this assessment.

118. Physical Security: What is the number of authorized testing locations?

RESPONSE: 10 locations within the City of Newport News.

119. Physical Security: Do you own the building(s) being targeted?

RESPONSE: Yes, the school division owns all buildings that are within the scope for this assessment.

120. Physical Security: Please indicate preferred attacker objectives.

RESPONSE: Identify and evaluate physical security risks to each type of school division buildings' access control systems (Security Cameras, Alarm Systems, Etc.).

121. Physical Security: Are there any areas or activities to be excluded from the scope?

RESPONSE: Physical Security testing should not interrupt student instruction or the daily business activities of the school division.

122. Can you please share a few more details as well as the budget?

RESPONSE: All the information has been made public. Please review the RFP and addendum. As for the budget, that information will not be made public.

123. Page 4, #7. Will it be necessary to visit multiple sites or is it possible to reach all data from one location?

RESPONSE: To perform testing on all requested network segments, the visitation of multiple sites will be required.

124. If multiple sites must be visited to accomplish the goals, how many sites?

RESPONSE: 10 Sites.

125. Page 5, B. Specific Requirements, #1.b. How much of the environment to be tested in the cloud?

RESPONSE: We would to test our primary cloud infrastructure/SaaS apps hosted within Microsoft.

126. Page 6, B. Specific Requirements, #2.a. Will a network map be available?

RESPONSE: A network map will be provided to the awarded Contractor.

127. Page 6, B. Specific Requirements, #2.e. How many business systems are in-scope?

RESPONSE: 10

128. Page 6, B. Specific Requirements, #3.a. Are the third party systems to be included as part of this task?

RESPONSE: No. External testing should only be performed on our network range.

129. Page 6, B. Specific Requirements, #3.c. How large are the four wireless systems?

RESPONSE: 6 SSID's that span across all NNPS buildings

130. Are any systems Azure or Amazon Web Services?

RESPONSE: Cloud technologies from Microsoft are utilized. Specific platforms will not be made public.

131. Page 6, B. Specific Requirements, #3.a. How many systems are in-scope including

a. Number of servers in-scope (Windows, others – please list)?
b. Number of users?
c. Number of firewalls?
d. Number of websites?
e. Number of applications?
f. Number of Internet sites?

Up to 64,000 addresses (1x - /16 networks).
48 Firewalls
200-400 Servers
10 Web Applications

Ideally, we would like to review our entire network for potential vulnerabilities.

We are open to narrowing down the scope to a smaller subset of devices and or/network segments. Please provide specific details on pricing/costs for both option

132. Page 6, B. Specific Requirements, #4.a. How many different sets of fire configuration rules are in-scope?

RESPONSE: 300-400 firewall rules/policies will need to be reviewed across firewall platforms. Rules across platforms are standardized. Please provide pricing on a per-rule or quantity basis.

133. Do employees have remote access?

RESPONSE: Yes.

134. What remote accesses protocols are in-scope?

RESPONSE: VPN. Specific technologies and methodologies that are in use are not disclosed to the public.

135. What database technologies are in-scope?

RESPONSE: Microsoft. Specific database technologies are not disclosed to the public.

136. Do your processes currently adhere to NIST 800-53 controls?

RESPONSE: Current processes are aligned to the NIST Cybersecurity Framework. Our long-term goal is to align to the 800-53 controls.

137. Page 6, B. Specific Requirements, #6.a. How many cybersecurity policies exist to be reviewed?

RESPONSE: 15 Policies / Documents for review. Polices range from between 3-10 pages on average.

138. Page 7, B. Specific Requirements, #6.d. How many new policies are needed?

RESPONSE: We are leveraging this audit to determine what gaps are in our current policy rule base. Please provide pricing based by policy or level of effort required.

139. Page 7, B. Reporting and Presentation. Do you require a separate report for each separate task even if they are undertaken consecutively?

RESPONSE: The major project deliverables requested in the RFP (III. Statement of Needs, B. Specific Requirements) can be broken into individual project deliverables. Separate reports for each deliverable are preferred.

140. Page 24. May progress payments be included?

RESPONSE: No. NNPS will make milestone payments to the awarded Contractor since each deliverable will be broken into individual project deliverables, and due NLT 4 weeks after completion. Following the acceptance and review of the deliverable(s) by the Contract Administrator, the awarded Contractor will be instructed to submit their invoice for payment.

141. External Penetration/Vulnerability Assessment: How many systems are in scope (i.e. how many live IPs are exposed to the internet)?

RESPONSE: 254 Ips (/24).

142. Internal Penetration/Vulnerability Assessment: While the RFP states that there are 40k devices on the network, what's the scope of this test (i.e., is the intent to test a sample, or all systems? If the intent is a sampling, what is the intended sample size)?

RESPONSE: Up to 64,000 addresses (1x - /16 networks).

Ideally, we would like to review our entire network for potential vulnerabilities. We are open to narrowing down the scope to a smaller subset of devices and or/network segments. Please provide specific details on pricing/costs for both options.

143. Web Application Assessment: How many web applications are in scope?

RESPONSE: 10

144. Firewall Evaluation: How many (unique) Firewalls and FW configurations are in scope?

RESPONSE: 47 firewalls. Configurations are standardized across the majority of devices.

145. Firewall Evaluation: What is the average number of rules per device and in aggregate?

RESPONSE: 300-400 rules/policies will need to be reviewed across firewall platforms. Please provide pricing on a per-rule or quantity basis.

146. Firewall Evaluation: How many IDS/IPS systems are in scope?

RESPONSE: 1

147. Policy and Process Assessments: What regulatory standards are the documents to be evaluated against?

RESPONSE: Childrens Internet Protection APP ("CIPA"), Children's Online Privacy Protection Rule ("COPPA"), Virginia Freedom of Information Act (FOIA), Virginia Consumer Data Protection Act ("VCDPA"), Health Insurance Portability and Accountability Act ("HIPAA"),
Family Educational Rights and Privacy Act ("FERPA").

148. Policy and Process Assessments: What is the rough count of existing policies and processes?

RESPONSE: 15

149. Policy and Process Assessments: Are procedures also in scope for evaluation, or just the policies?

RESPONSE: We are looking to have existing policies reviewed. Identification of any gaps in current policies. Assistance with creation and remediation of policy gaps.

150. Submission Instructions: Would you consider accepting electronic (email) submissions of vendor's proposals?

RESPONSE: Proposals received by telephone, telegraph, facsimile, or any other means of electronic transfer shall not be accepted.

151. Reference RFP Paragraph III., A.6., Page 4: Will Newport News Public Schools (NNPS) supply the list of network infrastructure, networks, and types of end user devices for use in preparing are proposal?

RESPONSE: A generalized overview of the school divisions network is specified in the RFP. We are unable to provide specific technologies, network diagrams, and methodologies that are in use to the public.

152. Reference RFP Paragraph III., B.2.a., Page 5: Does NNPS require purely an assessment using technical tools to determine vulnerabilities; or does NNPS require examinations and tests of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 security controls to evaluate the level and success of implementation so that there are no vulnerabilities or risks associated with their implementation?

RESPONSE: Current processes are aligned to the NIST Cybersecurity Framework. This assessment should be based on that framework. Our long-term goal is to align to the 800-53 controls.

153. Reference RFP Paragraph III., B.6.a.-d, Pages 6 and 7: We believe subparagraphs "a" through "d" are somewhat redundant in scope. Does NNPS require assessment of existing policies against a framework such as NIST SP 800-53 to identify gaps and recommend updates; or, does NNPS require drafting of new policies to fill those gaps similar in scope to what is being required in RFP Paragraph III.B.7.?

RESPONSE: Identify gaps and recommend updates to existing policies. Templates for recommended policies would be ideal.

154. Does NNPS have an incumbent Contractor providing these services?

RESPONSE: No.

155. Page 5, Section 1: Can NNPS provide the number of IP Addresses (Internal and External) and web applications that are considered in scope?

RESPONSE:
External - 254 IP addresses. CIDR: /24
Internal - Up to 64,000 addresses
(1x - /16 networks).

Ideally, we would like to review our entire network for potential vulnerabilities. We are open to narrowing down the scope to a smaller subset of devices and or/network segments. Please provide specific details on pricing/costs for both options

156. Page 5, Section 1: Does NNPS have any time restrictions in which testing can occur?

RESPONSE: Testing should be non-intrusive. It is preferred that all testing occurs during off-hours to minimize any potential user impact.

157. Page 6, Section 3: Can NNPS provide the number of Wireless SSID's, access points, and physical locations that are considered to be in scope for the wireless penetration testing?

RESPONSE: Six wireless SSIDs. 10 locations located within the City of Newport News, Virginia.

158. Page 6, Section 4: Can NNPS provide the number of firewalls that are considered in scope for the firewall review?

RESPONSE: 48

159. Page 9, Section G: Where in our proposal response does NNPS want the cover page and anti-collusion/nondiscrimination form included?

RESPONSE: NNPS requires that the submission of the proposals shall include those documents. The location of the above mentioned documents is up to the Offeror.

160. Where in our proposal response does NNPS want the response to Attachment B included?

RESPONSE: Please see the above response, Q&A #159.

161. When is the intended award date for the project?

RESPONSE: Being that December is a short working month for NNPS, the estimated contract award date is sometime late February or early March.

162. Is there an incumbent for the project? If so, who is the incumbent?

RESPONSE: No.

163. What is the anticipated budget?

RESPONSE: That information will not be made public.

164. Does NNPS have an anticipated start time for this project?

RESPONSE: Being that December is a short working month for NNPS, the estimated contract award date is sometime late February or early March.

165. Section IV. Special Instructions To the Offeror, Tab 4-Financial Proposal states, " include a copy of the three (3) most recent annual reports to date". For clarification: Is NNPS looking for a report for each quarter for the last 3 years, or is NNPS looking for a report of each of the last 3 quarters?

RESPONSE: The language reads to include three most recent annual reports. In addition, provide financial statements for each quarter since the last annual report to date.

166. Section IV. Special Instructions to the Offeror, Tab 5-Experience states, "include a minimum of four (4) references for which the Offeror has completed services comparable to those described herein. Two (2) of the references must be active accounts and two (2) must be recently (within the past 5 years) terminated accounts". Will NNPS accept 4 current multi-year references?

RESPONSE: Yes, that is acceptable.

167. On page 28 of the RFP, Attachment B-Question 12 asks vendors to "Give two (2) banking institution references. Are these two references for Banking Institutions we have provided cybersecurity services for ? Or are you looking for banking institutions to provide testament to our financial stability ? Please clarify what NNPS is looking for from this question.

RESPONSE: Please provide banking institution references for financial stability purposes.

168. On page 28 of the RFP, Attachment B, Question 13, asks vendors to "list three (3) material suppliers and amount of credit available" and on page 29 of the RFP, Attachment B, Question 15 states, " bonding reference: list surety company and highest coverage." Please provide clarification as to what information these two sections are looking for. Are these areas applicable to this particular solicitation and scope of work?

RESPONSE: No. Those areas are not applicable to this solicitation and scope.

All other provisions of the IFB shall remain unchanged.

Sincerely,
Antonio Palmer, MBA, CPPB, VCO, VCA
Senior Procurement Specialist
757-591-7493 x10755

_____
Name of Firm

_____
Signature/Title

_____
Date