GRAND VALLEY
STATE UNIVERSITY
www.gvsu.edu

To: **Prospective Bidder**
Date: **April 4, 2022**
Subject: **Request for Proposal** - **Bid# 222-31 Penetration Testing**
RE: **Correction to RFP #222-31 Language and Q&A Responses: - Addendum** # **1**

Correction to RFP:

Please disregard point #5 under the “Bid Information and Instructions” section. The language stating “use the enclosed proposal and contract sheet to record pricing information” was a typo and should have been removed before the RFP was posted. Therefore, please disregard point # 5 and include any and all pricing with your bid submission.

Questions and Answers:

1. Is application penetration testing required? Under the expected test types it appears that it is but under “Assumptions” it appears no application penetration testing is required. If required, see question 2.
    a. Web scanning and surface testing is expected. Code review, dynamic, and static code analysis are outside of the scope.
2. Per “Expected Test Types” item 5, you indicate that application-layer penetration testing must be included. Are there specific web (or other) applications that must be tested? If so, can you please specify the types of applications, approximate number of functional pages, and number of application roles to be tested?
    a. Web scanning, input injection, sql injection, etc.
3. Approximately how many live hosts are accessible from the Internet.
    a. Zero.
4. Regarding “External from PCI”, must scanning occur FROM the networks listed?
    a. Scanning must occur from each of the subnets listed as well as one net referred to as an office net or NET201/210.
5. Is there currently an incumbent company or previous incumbent, who completed similar contract performing these services? If so - are they eligible to bid on this project and can you please provide incumbent contract number, dollar value and period of performance?
    a. I am new to this position, I am not sure who did our last PCI Pent test.

6. Approximately how many computer endpoints do you have (desktop PCs, laptops, servers)?
    a. In PCI there are 50-75 nodes.
7. Can you tell the total number of endpoints you want protected?
    a. Not sure what you mean by “protected” This is for a penetration test.
8. What’s your headcount of users (employees + contractors+interns)? What number/percentage of your workforce resides within organizational facilities? What number/percentage works remotely?
    a. I am not sure how this is relevant.
9. How much (%) of the infrastructure is in cloud?
    a. For PCI I don’t believe there are any cloud elements.
10. What is the size of the IT environment?
    a. See #6 for PCI.
11. How many physical locations?
    a. Not relevant to this RFP.
12. What is the aggregate Internet Capacity per location (<300mbps, <1gbps, <4gbps, up to 10gbps)?
    a. In general, we have 10gbps but for pci specifically it may be more limited.
13. Do you manage your own data Center, or do you utilize any 3rd-party/colocation facilities?
    a. Manage our own data centers.
14. What is the approximate budget?
    a. I do not have budget numbers.
15. Where can we find the enclosed proposal and contract sheet to record pricing information in the RFP document?
    a. Please disregard point #5 under the “Bid Information and Instructions” section. The language stating “use the enclosed proposal and contract sheet to record pricing information” was a typo and should have been removed before the RFP was posted. Therefore, please disregard point # 5 and include any and all pricing with your bid submission.
16. Will the awarded vendor have access to the previous Pen Test reports?
    a. No we would not provide access to that information.
17. Does the vendor have to be a QSA?
    a. We would need the vendor to be QSA to be awarded this contract.
18. Is the GVSU wireless internal network in scope?
    a. No, there is no in scope wireless.
19. Is a PCI DSS physical security assessment in scope?
    a. According to PCI DSS v3.2, there is a requirement to test whether there is restricted physical access to cardholder data. For this contract there is no requirement for physical access requirements.

20. Are you willing to accept modifications to the Insurance requirements?
    a. At this time, we are not able to change the T&Cs as stated in the RFP. However, after the close date and bids are submitted/reviewed by our internal team if there is a desire to move forward with a vendor that has concerns with our T&Cs we can address those concerns at that time. We would work with our Legal Office to determine if any changes would be allowed or accepted.
21. What is the total contract term and the start date?
    a. GVSU hopes to schedule this for mid-April. We envision a one-to-two-week test period and then would expect to receive the pen test report within two weeks of completion.
22. We understand that Penetration tests to be conducted on annual basis, please confirm.
    a. PCI Pen tests must be annual, this particular engagement is NOT annual we would expect to do an RFP next year.
23. Please confirm the testing time, Non- working hours, Weekend, Any day?
    a. Any is fine as long as the work is done – we would not limit that on our end.
24. Is Vendor expected to scan any URL's. If Yes, please list:
    a. In short yes. Based on industry-accepted penetration testing approaches (for example, NIST SP800-115).
    b. Includes coverage for the entire Card Holder Data Environment (CDE) perimeter and critical systems.
    c. Includes testing from both inside and outside the network.
    d. Includes testing to validate any segmentation and scope- reduction controls.
    e. Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5 of the DSS standards.
    f. Defines network-layer penetration tests to include components that support network functions as well as operating systems.
    g. Includes review and consideration of threats and vulnerabilities experienced in the last 12 months.
    h. Specifies retention of penetration testing results and remediation activities results.
    i. Since network segmentation is used to isolate the CDE from other networks:
    j. Tests to ensure penetration-testing procedures defined to test all segmentation methods, to confirm they are operational and effective, and isolate all out-of-scope systems from systems in the CDE?
    k. Penetration testing must verify that segmentation controls meet the following?
    l. Performed at least annually and after any changes to segmentation controls/methods.
    m. Covers all segmentation controls/methods in use.
    n. Verifies that segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.

25. Post Penetration test, if any critical vulnerabilities are identified, post fixing the vulnerability should we conduct follow-up Penetration test with limited scope.
    a. That would be a nice option but is not expected.
26. Clause 2.0: Termination: Could the Firm (DXC) include wind-down fees in its proposal in the event of early termination?
    a. At this time, we are not able to change the T&Cs as stated in the RFP. However, after the close date and bids are submitted/reviewed by our internal team if there is a desire to move forward with a vendor that has concerns with our T&Cs we can address those concerns at that time. We would work with our Legal Office to determine if any changes would be allowed or accepted.
27. Can you confirm that this test can be delivered out of Offshore location?
    a. It is unlikely that we would pick a vendor using an offshore location for this engagement.
28. Clause 3.0: General Terms and Conditions: Is answering the RFP imply without changes imply an acceptance of the General Terms and Conditions?
    a. Yes.
29. Clause 3.0: General Terms and Conditions: Is it possible to negotiate some of the terms included in Section 3? If so, all the terms or only some of the terms? What would be the calendar and the process?
    a. At this time, we are not able to change the T&Cs as stated in the RFP. However, after the close date and bids are submitted/reviewed by our internal team if there is a desire to move forward with a vendor that has concerns with our T&Cs we can address those concerns at that time. We would work with our Legal Office to determine if any changes would be allowed or accepted.
30. Clause 3.1.8 Indemnifications: Specifically, is it possible to limit the scope of this clause? Is it possible to limit the indemnification to 3rd party claims? If so, what is the calendar and process to negotiate the terms?
    a. At this time, we are not able to change the T&Cs as stated in the RFP. However, after the close date and bids are submitted/reviewed by our internal team if there is a desire to move forward with a vendor that has concerns with our T&Cs we can address those concerns at that time. We would work with our Legal Office to determine if any changes would be allowed or accepted.
31. Clause 3.1.8: Indemnifications: Is it possible to add a limitation of liability? If so, what is the calendar and process to negotiate the terms?
    a. At this time, we are not able to change the T&Cs as stated in the RFP. However, after the close date and bids are submitted/reviewed by our internal team if there is a desire to move forward with a vendor that has concerns with our T&Cs we can address those concerns at that time. We would work with our Legal Office to determine if any changes would be allowed or accepted.
32. What are the payment terms? Is Net 30 acceptable?
    a. If there is a desire to move forward with a vendor that has concerns with our T&Cs we can address those concerns at that time including payment terms.

33. Please clarify scope of penetration testing. The Scope section states that "Fulfill all requirements as defined by PCI DSS v3.2 for external penetration test... (section 11.3.1)" but "Expected Test Types section" covers sections 11.3.2 - 11.3.4. Are all sections of 11.3 (11.3.1 - 11.3.4) included in scope of this RFP or is it only external penetration testing (11.3.1)?
    a. Sorry for the confusion yes, we are expecting 11.3.1 as well as 11.3.2 - 11.3.4 In short we would expect testing that segmentation methods are operational and effective.
34. Expected Test Types paragraph 5 states "Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5 of the DSS standards". However, assumptions paragraph states that application-level penetration testing is not required because GVSU only uses third-party software which has been certified to be PCI compliant. Since DSS Requirement 6.5 involves identifying common coding vulnerabilities in software development processes, will any application-level penetration testing be required? If custom code or applications are developed and then hosted on critical systems, how many applications are running which should be considered in-scope for a penetration assessment?
    a. We are not seeking a code review per se, however if you find an application with known vulnerabilities or suspected we would hope you would explore those options.
35. Is segmentation testing required from each internal (CDE in-scope) VLAN? From each non-CDE VLAN to each internal PCI VLAN?
    a. Yes, we are seeking segmentation testing. It is likely not practical to do a per VLAN analysis. We would hope you would evaluate if you can get out of the PCI VLAN.
36. Expected Test Types mentions that testing should cover all segmentation methods in use. Are multiple segmentation solutions implemented on the Internal VLAN? Or are there different segmentation solutions from External to GVSU and External from PCI to PCI?
    a. A variety of segmentations are used.
37. Will a wireless network component be in-scope of this penetration test?
    a. No.
38. Can wireless scanning/exploitation be performed on identified networks?
    a. It is not required for this engagement.
39. Will on-site physical intrusion testing be required?
    a. No.
40. Will Social Engineering testing be required?
    a. For this engagement no, we are more interested in the technical pen test end.
41. Will we be able to do both remote and on-site penetration testing at the same time?
    a. I would not expect this to be an issue if you choose to be on site.

42. Kindly confirm whether it is a mandatory requirement that the service provider should be a QSA or ASV for (PCI) Data Security Standard, v3.2:
    a. Yes, we expect QSA.
43. With reference (Section “Expected Testing Types” point 5 in the RFP Document) to Requirement 6.5 of the (PCI) Data Security Standard, v3.2. Please confirm if the scope includes process/policy evaluation or only testing?
    a. Only testing.
44. As per the PCI standard, SAST & DAST need to be evaluated at the application layer. But, referring to (Section “Assumptions” in the RFP Document) it's defined in the RFP that application testing is out of scope. Please confirm.
    a. Application testing is out of scope.
45. Kindly confirm if Grand Valley State University (GVSU) expects to complete the entire penetration testing procedure (excluding reporting) in 2 weeks? (Referring to section “Schedule” in the RFP document.)
    a. That is our hope yes.
46. Kindly confirm if all the subcomponents of sections 11.3, 11.3.1 and 6.5 related to (PCI) Data Security Standard, v3.2 are part of the scope.
    a. Yes, they are part of the scope.
47. Kindly specify the mandatory details to be specified as for the references/ case studies.
    a. We are not sure what you are asking with this question so we cannot formulate a response.
48. As per the (Section “Bid Specifications and Information” point 5), we must use the contract sheet to record pricing information. However, we could not find the attachment in the portal. Kindly provide us with all the relevant documents for this RFP.
    a. Please disregard point #5 under the “Bid Information and Instructions” section. The language stating “use the enclosed proposal and contract sheet to record pricing information” was a typo and should have been removed before the RFP was posted. Therefore, please disregard point # 5 and include any and all pricing with your bid submission.
49. Will you please let me know if you would like this to be a white, grey or black box approach? Since this is a 1-2-week test period, I’m assuming it’ll be grey or white but wanted to verify.
    a. Grey.