GRAND VALLEY STATE UNIVERSITY
www.gvsu.edu

To: **Prospective Bidder**
Date: **March 17, 2023**
Subject: **Request for Proposal - Bid# 223-30 Penetration Testing**
RE: **Q&A Responses: - Addendum # 1**

Questions and Answers:

1. Can you clarify what is needed for point 7 of the Expected Test Types? Do you want a review of security incidents that happened at GVSU in the past 12 months?
    a. To be clear I believe you are asking about: "7) Includes review and consideration of threats and vulnerabilities experienced in the last 12 months" The intent here is that you are testing for up-to-date threats in the current threat landscape.

2. Is there an Active Directory environment used for authentication on devices in the PCI network?
    a. Our PCI network is a distinct separate environment.

3. Can you confirm that tests can be done 100% remotely as mentioned here?
    a. Yes, the work can be done 100% remotely.

4. Is there a PCI QSA requirement for award of this contract?
    a. A PCI QSA is strongly preferred but we will consider each proposal on its merits.

5. Are you looking for an ASV?
    a. No. However, it would be a bonus.

6. Please confirm whether application penetration testing is out of scope? The RFP's "Expected Test Types" point 5 seems to conflict with the "Assumption" statement.
    a. Application testing meaning a code review of any software is out of scope. If you find a web applications presence, we will assume you would scan it for vulnerabilities.

7. Can you please provide the evaluation criteria that will be used to select the winning responder?
    a. A matrix of scores will be evaluate including the following:
    Engagement quote Credentials of Analysts (1-5) QSA Compliant (1 or 5)
    Appropriate Scoping (1-5) 3 References (1-5) Overall Presentation (1-5)

8. Has an assessment of this kind been performed before? If so, what was the contract value?
    a. Yes. The contract value was within industry standards.

9. 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?
    a. Previous incumbent: Yes.
    Are they eligible: Yes.
    Contract details: Not appropriate to share.

10. Specify the VLAN details how many are included in the Scope?
    a. 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.

11. Can you please provide the current number of infrastructure details (Physical Server, Virtual Server, Network Devices, etc.)?
    a. In PCI there are 50-75 nodes.

12. How much (%) of the infrastructure is in the cloud?
    a. A few vendor sites are cloud based but overall, very little.

13. In the IT department/environment, how many employees work?
    a. Not relevant to this project.

14. Do you manage your own data Center, or do you utilize any 3rd-party/colocation facilities?
    a. We have our own data centers.

15. Is there a funding/financial/budget range estimated that can help us to provide a quotation for this project?
    a. Yes, there is funding. We anticipate costs to be along industry standards.

16. The RFP requests VLANS to be "scanned", and alternatively requests "penetration testing". Following vulnerability scanning, is an attempted exploitation of discovered vulnerabilities desired?
    a. Yes.

17. Does GVSU have an intended budget for this assessment?
    a. Yes, GVSU has a budget for this project. GVSU will not share the dollar amount of that budget with an external organization. Our request is that each vendor provide their best possible price on the original response.

18. RFP Scope item 9 lists several sub bullets, the first two of which end in a "?". The second bullet ends in "including?". Is there additional description for these points, or is this a typo?
    a. This is a typo. Item 9 should read:

        1) Since network segmentation is used to isolate the CDE from other networks:
            a. 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.
            b. Penetration testing must verify that segmentation controls meet PCI requirements.
            c. Covers all segmentation controls/methods in use.
            d. Verifies that segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.

19. Does GVSU have an intended budget for this assessment? Please clarify whether application-layer penetration tests are required. Bullet 5) of the "Expected Test Types" section implies that they are. However, the "Assumptions" section states that "Application-level penetration testing is not required because GVSU only uses third-party software that is purchased and certified to be PCI compliant."
    a. Discovered applications should be scanned for vulnerabilities. Code level review of applications is not in scope.

20. Approximately how many live/active IP addresses are in scope for the external test?
    a. There are 7.

21. Approximately how many live/active IP addresses are in scope for the internal test?
    a. There are 50-75 nodes.

22. Will the selected vendor have an opportunity to negotiate mutually agreeable terms and conditions to support delivery of the engagement during the selection process?
    a. We will evaluate all the proposals we receive at the close of the RFP. If we have any questions or clarifications, we will communicate via the RFP process.

23. Does the University require a specific format for the proposal and topics to be included (i.e., scope, project management methodology, timeline, references, cost)? If so, is the University able to provide the required format of the submitted proposal?
    a. No specific format but the clearer, more professional, and well done the better!

24. How many different PCI segmented VLANs are required to be tested (if not accessible from one location)?
    a. 7 PCI segments.

25. For the External Penetration Assessment, what are the total number of hosts that are externally accessible (out of the three PCI ranges provided in the RFP)?
    a. 7 access points.

26. Additionally, out of the total number of externally accessible hosts, how many total services are available from the Internet (FTP, HTTP, HTTPS, etc.)?
    a. We assume you would be able to determine that information as part of the testing.

27. GVSU open to T&M pricing or does GVSU want to see fixed pricing?
    a. We need a fixed quote to evaluate the proposals.

28. Does GVSU desire a separate pricing document or can pricing be included in the technical proposal?
    a. Pricing can be included in the technical proposal.

29. Is there a budget for this project? Are you able to provide the budget estimate?
    a. Yes, we have budget, but we are not able to provide an estimate.

30. What are the evaluation criteria for how the winning proposal will be determined?
    a. Proposal evalutations will include: Company Engagement quote Credentials of Analysts (1-5) QSA Compliant (1 or 5) Appropriate Scoping (1-5) 3 References (1-5) Overall Presentation (1-5)

31. Is onsite or remote work preferred?
    a. Either is acceptable.

32. Does the GVSU currently conduct penetration testing? If so, what is the typical frequency and type (internal, external, web, etc)?
    a. Yes, we conduct internal scanning. Frequency and type are in line with industry standards.

33. Is there an incumbent who is currently providing these services? If so, is there a reason for considering replacement of the incumbent?
    a. Yes, there is an incumbent. We request RFPs for major projects and fairly evaluate each proposal.

34. Who will the awardee coordinate with to perform the work?
    a. GVSU IT Security staff will coordinate the project.

35. Has GVSU experienced any breaches within the last 3 years? If so, can GVSU provide information on the nature of the breach and remediation steps taken?
    a. GVSU has not experienced any breaches that have impacted the PCI environment.

36. We did not see the due date for the answers. When will the answers be provided? We assume that we will see all questions and answers that are submitted.
    a. We hope to have questions answered and published in a timely manner.

37. Depending on the number of questions and timing of the answers, will GVSU consider delaying the due date of the proposal?
    a. No, we will not delay the date of the proposal.

38. The RFP states that we should acknowledge receipt of all addenda. We only have the RFP document. Are there other documents? Or will the addenda include the Q&A responses?
    a. The IT Security department has no additional addenda, the RFP process may require additional documentation, and I defer to that unit for clarification.