GRAND VALLEY STATE UNIVERSITY
www.gvsu.edu

To: **Prospective Bidder**

Date: **April 5, 2024**

Subject: **RFP # 224-41: PCI Penetration Testing**

RE: **Addendum # 1: Questions and Answers**

Question # 1: Do we know how many live assets are within these Class C subnets?

- 10.20.0.0/24
- 10.20.1.0/24
- 10.20.2.0/24
- 10.20.3.0/24
- 10.20.4.0/24
- 10.20.5.0/24
- 10.20.6.0/24
- 10.20.7.0/24
- 10.20.8.0/24
- 10.20.9.0/24
- 10.20.10.0/24

Answer # 1: **200 or so devices – see question # 3 below.**

Question # 2: How many Externally phasing IPv4 addresses are within scope for this penetration test engagement from the list below?

External from PCI
148.61.0.0 3 TO PCI NETS
35.0.0.0 TO PCI NETS
10.[8-9].0.0 TO PCI NETS

Answer # 2: **20 estimated.**

Question # 3: Are we performing segmentation testing on the assets below?

PCI Inventory estimates
Network Devices 75 Cisco IOS; Cisco OEAP
Servers 40 Windows; RHEL;VMWARE
Workstations 50 Various Models/Makes; Windows 10;
Windows 2016 Server; WinPOS

Answer # 3: **Yes.**

Question # 4: We can provide an OVA or NUC (device). Any preference on which one we can use for the engagement? We can provide access to the NUC where the data can be deleted with that account which will reside in the /opt/pentest/GVSU/ folder.
Answer # 4: We'd prefer an OVA – we can accommodate a physical device however we have had vendors send us bad hardware which took up our time to correct.

Question # 5: Any web applications and APIs and third-party frameworks in scope? If so, will different roles be provided for the web applications and APIs for testing?
Answer # 5: If you find any web applications or APIs yes, they would be in scope. No additional roles would be provided.

Question # 6: What is the project budget for this effort?
Answer # 6: Budget will be based on the quotes we receive for the RFP.

Question # 7: Is this the first time doing this type of effort?
Answer # 7: No.

Question # 8: What was the award amount if this has been performed in the past?
Answer # 8: Various quotes have been awarded in the past.

Question # 9: The RFP states "Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.4 of the DSS standards." and then says "Application-level penetration testing is not required because GVSU only uses third-party software that is purchased and certified to be PCI compliant." Can we assume for costing purposes Application testing is not in scope?
Answer # 9: We do not expect any source code evaluation. However, if an application is found we would expect it to be scanned for vulnerabilities.

Question # 10: The RFP requires "Includes review and consideration of threats and vulnerabilities experienced in the last 12 months." Can you please elaborate on the type and quantity of findings experienced in the past and is a dedicated report required for this task?
Answer # 10: The intent here is that you are up to date on the current threat environment and current on IOCs.

Question # 11: The RFP lists out 10 Class C internal addresses. How many live IPs are considered in the test scope?
Answer # 11: There are around 200 devices.

Question # 12: The RFP lists out 10 Class C internal addresses. Is discovery of live IPs required or will more information be provided on the locations of live addresses?
Answer # 12: For external no, for internal yes.

Question # 13: The RFP lists out three extremely large subnets for external testing. How many live IPs are considered in the test scope?
Answer # 13: External around 20 IPs.

Question # 14: The RFP lists out three extremely large subnets for external testing. Is discovery of live IPs required or will more information be provided on the locations of live addresses?
Answer # 14: No.

Question # 15: The RFP lists out 165 systems in the PCI inventory. Is this the number of live systems requiring testing within the 10 Class C addresses or in addition?
Answer # 15: That is part of the estimated 200 internal systems.

Question # 16: The RFP lists out a lot of insurance requirements that may or may not be required. Is the 10Million Technology Errors and Omissions required in this situation? This is above industry standard and would disqualify many cyber vendors.
Answer: **Any insurance requirements would be discussed during post bid award to the winning firm.**

Question # 17: Is the 10Million Privacy & Networks Security Liability required in this situation? This is above industry standard and would disqualify many cyber vendors.
Answer # 17: **Any insurance requirements would be discussed during post bid award to the winning firm.**

Question # 18: The RFP states "Grand Valley State University policy to remain compliant at all times with all U.S. export control regulations, including but not limited to the International Traffic in Arms Regulations and Export Administration Regulations. Before". Do you require certifications such as CJIS in order perform testing if we may access ITAR / EAR data? Please elaborate on any other requirements if ITAR / EAR data will be included in the scope.
Answer # 18: **Any export control requirements (if applicable) would be discussed during post bid award to the winning firm.**

Question # 19: The RFP project name in the contract form is "Penetration test and red/purple team cross training". What red/purple team cross training is required as we did not find a references to details associated with this portion of the task in the RFP.
Answer # 19: **It would be nice if you would let us observe your methods, but it is not required.**

Question # 20: The RFP states: "The undersigned certifies that company is at least 51% owned, controlled, and actively managed by…" Is there a requirement to be one of these disadvantaged organizations in order to bid and or is favor being afforded to these groups?
Answer # 20: **No, that is never a deciding factor or criteria in which supplier is awarded the contract. The decision we make is strictly based on the bid submission from the suppliers and how they compare with our evaluation criteria as outlined in the RFP. The reason we ask that question when conducting RFPs is just to have a way to capture which vendors that we do work are MBE businesses. This allows us to, as best we can, track our Tier 1 and Tier 2 spend and then we can post those numbers every FY.**

Question # 21: Does GVSU have any other location (including date centers) other than Allendale, Grand Rapids, Holland, Muskegon, and Traverse City?
Answer # 21: **None that are relevant to this RFP.**

Question # 22: Approximately how many full-time employees does GVSU have?
Answer # 22: **This is not relevant to this RFP.**

Question # 23: Is GVSU's network hosted in-house, at a data center, or both?
Answer # 23: **This is not relevant to this RFP.**

Question # 24: Are there any time limitations as to when security testing can take place or can testing occur during standard business hours? (8:00 a.m.-5:00 p.m. CT, M-F)? If there are limitations, please list the days and times available for testing.
Answer # 24: **No time limitations.**

Answer # 25: Has GVSU gone through a formal penetration test or had quarterly vulnerability scans performed on their network in the past? If so, when?
Answer # 25: **This is not relevant to this RFP.**

Question # 26: External Network Testing - How many external IP addresses (public IPs) does GVSU own?
Answer # 26: **This is not relevant to this RFP.**

Question # 27: How many of these IPs are routed or active and in scope for testing?
Answer # 27: **20 Estimated.**

Question # 28: Are there any virtual hosts on these IPs (those that would only respond to a hostname, such as multiple websites on a single IP address)? If so, how many?
Answer # 28: **This is not relevant to this RFP.**

Question # 29: Confirming that GVSU does NOT require Web Application Testing. Is this correct?
Answer # 29: **If an application is discovered we would expect it to be in scope.**

Question # 30: Internal Network Testing - Of the 40 servers listed in GVSU's PCI Inventory Estimates, how many are physical servers and how many are virtual servers? How many total user accounts does GVSU have? How many levels of user accounts does GVSU have?
Answer # 30: **These not relevant to this RFP.**

Question # 31: Does GVSU require Wireless Testing?
Answer # 31: **For segmentation testing it would be ideal to test from a wireless connection, but it is not an absolute requirement.**

Question # 32: Does GVSU require Wireless Testing? If so, does GVSU prefer testing of the internal network FROM a wireless connection OR testing of the wireless network itself? How many locations are included in wireless testing? Where are these locations in relation to each other? How many SSIDs at each location? How many wireless access points at each location?
Answer # 32: **If wireless testing is done it would be from one subnet. The number of SSIDs and access points are irrelevant.**

Question # 33: External network penetration test: Estimated number of public IPs/Services per assessment?
Answer # 33: **20 estimated.**

Question # 34: Internal network penetration test: Estimated number of Internal IPs/Services per assessment?
Answer # 34: **200 estimated.**

Question # 35: Do you have any web applications to be covered as part of this Pen Test? If yes, then an Estimated number of websites/applications to be tested?
Answer # 35: **If web applications are discovered yes, they would be in scope. There are likely under 50.**

Question # 36: Is the application-level penetration testing in scope for this project or not?
Page 5. "Expected Test Types- 5) Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.4 of the DSS standards."
Page 7. "Assumptions- Application-level penetration testing is not required because GVSU only uses third-party software that is purchased and certified to be PCI compliant. GVSU expects that all third-party software vendors conduct annual application-level code reviews and penetration tests. It is expected that fixes will be released in a timely fashion if issues are found during testing."
It seems that there are no vulnerabilities listed in the 6.4 DSS Standards (6.4 is about application layer), and the RFP states that there is no application testing to occur as those vendors certify testing of them.

Answer: #36: **If apps are discovered we would expect you them to be scanned for standard vulnerabilities. I believe the intent for page 7 was that we would not expect any examination of source code for vulnerabilities. However, we would expect general application testing (fuzzing, brute force etc., if apps are discovered).**

Question # 37: Is there a certain compliance mandate driving the assessment?
Answer # 37: **PCI Compliance.**

Question # 38: What is the end goal of the assessment?
Answer # 38: **Compliance with PCI.**

Question # 39: Has the organization conducted a vulnerability assessment or penetration test before?
Answer # 39: **This is not applicable to this RFP.**

Question # 40: Are there any time restrictions for performing the assessment (All work is performed during normal work hours of 8am to 5pm local time unless specified)?
Answer # 40: **No time restrictions.**

Question # 41: Is there a certain compliance mandate driving the assessment?
Answer # 41: **PCI Compliance.**

Question # 42: Delivery Model:
Answer # 42: **Hybrid (Remote and/or Onsite).**

Question # 43: Is External Penetration Testing in Scope? (Penetration test against external (WAN) environment.)
Answer # 43: **Yes, 1-10 Ips.**

Question # 44: Is Internal Penetration Testing in scope? (Penetration testing against the private (LAN) environment.)
Answer # 44: **Yes. 1 - 100 Ips.**

Question # 45: Does the Internal Penetration Test include PCI DSS testing?
Answer # 45: **Yes – network segments are specified in the RFP.**

Question # 46: Is Wireless Testing in scope? (Penetration testing against the wireless environment.)
Answer # 46: **Ideally, wireless test for segmentation from PCI would be tested. One SID and vlan.**

Question # 47: Is Ransomware Testing in scope?
Answer # 47: **No.**

Question # 48: Is Social Engineering (Email) Testing in scope? (Security awareness testing through simulated social engineering campaigns.)
Answer # 48: **No.**

Question # 49: Is Social Engineering (Vishing/SMShing) Testing in scope? (Security awareness testing through simulated social engineering campaigns.)
Answer # 49: **No.**

Question # 50: Is Social Engineering (Physical) Testing in scope? (Evaluation of the organizations physical security controls using non-intrusive techniques.)
Answer # 50: **No.**

Question # 51: Is Mobile Application Testing in scope?
Answer # 51: **No.**

Question # 52: Is Remediation Validation Testing in scope? (Follow up testing to validate the remediation of previously identified vulnerabilities.)
Answer # 52: No.

Question # 53: Is Remediation Service in scope? (A time-boxed effort in which Converge will work to remediate a mutually agreed upon list of issues drawn from those uncovered during testing.)
Answer # 53: No.

Question # 54: Penetration Test Methodology? (The approach in which the penetration test will be conducted.)
Answer # 54: Gray Box (Some information regarding the environment is provided).

Question # 55: How large is the PCI environment? Number of users?
Answer # 55: We have around 200 nodes – users would be less than that number.

Question # 56: Number of firewalls?
Answer # 56: This is not needed for this RFP.

Question # 57: What level merchant is the University?
Answer # 57: If you are referring to SAQ levels, we have several. I don't believe specifics are necessary for this RFP.

Question # 58: How many applications are in the PCI environment (we understand that the applications themselves will not be tested)?
Answer # 58: If web applications are found in the environment, we would expect a standard vulnerability scan to be done. We do not expect any source code analysis.

Question # 59: Item 3.19 Insurance, Items i and j. We are requesting that the University consider accepting $2.5 million in coverage. Over the last 5 years our carriers have decreased our coverage from an initial $10 million to $5 million and this year to $2.5 million dollars while our premiums have remained the same as if the coverage was still at a $10 million dollar level thus making it difficult for small businesses to afford higher coverage.
Answer # 59: Any insurance requirements would be discussed during post bid award to the winning firm.

Question # 60: Item 3.3.7 Proprietary/Confidential Information. Will you accept a redacted proposal to be used in the event a Freedom of Information Act request is made?
Answer # 60: If applicable this would be discussed during post bid award to the winning firm.