Maine's Public Universities
UNIVERSITY OF MAINE SYSTEM

REQUEST FOR PROPOSALS #2020-017
Payment Card Industry (PCI) Data Security Penetration Testing
RESPONSE ADDENDUM #01
December 10, 2019

QUESTIONS

1. The Cost Template excel does not list Presque Isle (though the RFP does) or the Bangor location for the University of Maine at Augusta for testing on tab 1; however, they are included on tab 3 for travel costs. Is this an oversight, and will the University be releasing an updated excel? Should vendors add lines for the two missing locations?
   Answer: Yes it was an oversight, cost template is updated.

2. Page 6, Item 1.13, top of page. "All campuses…must be afforded the use of this solution…" Does this mean that some campuses will not participate in the testing?
   Answer: No this is standard language in our RFP template.

3. What is the budget for this project?

   Answer: University does not share this information during RFP process.

4. Page 9, Item 1.2.3 Confidentiality. May we submit a redacted proposal for use with any FOAA requests?
   Answer: You may, however what may be redacted needs to be compliant with Maine Freedom of Access Act (FOAA), 1 MRSA §401 et seq.

5. Are Campus visits cost included or billed hourly?
   Answer: If your solution requires travel, you should specify any travel rates by campus, see cost template Table 3

6. Is the 10 IP count a total figure for both University of Maine at Augusta locations, i.e., Augusta and Bangor? If not, please provide individual IP counts for testing.
   Answer: Yes it's a total, with 8 at the Augusta location and 2 at the Bangor location.

7. Will the University require only one deliverable per year per location as part of this project?
   Answer: The requirements for PCI penetration testing are annual. If a change is made to the environment an additional penetration test may be requested. We expect this would be costed separately.

8. Page 6, Item 1.1.4. Is it possible to conduct testing remotely since these are penetration tests?
   Answer: External and internal penetration testing is required, but bidders may propose both these types be done remotely.

9. Page 6, Item 1.1.4., 2nd paragraph. Do you already have PCI devices inventoried or must discovery occur?
   Answer: PCI devices are inventoried and information will be provided to the penetration testers.

10. Page 112, Item 1.3.7. Are potential presentations able to be conducted via teleconference?
    Answer: Yes all will be done via Zoom.

11. Page 23, Instructions, 5th paragraph, Hourly Rate. Are these tests one time during the year or will there be multiple tests at various campuses?
    Answer: These Level I PCI tests are one time during the year. If a change is made to the environment an additional penetration test may be requested. We expect this would be costed separately.

12. Can logical elements all be reached from one location or is each campus completely separate?
    Answer: In the past, vendors have provided a device that would be place at internal vantage point, mostly likely afforded by physical connection to the internal segment being tested .

13. How many data bases does each campus have?

    Answer: No databases are in scope for Level I testing.

14. What data bases are they?

    Answer: N/A

15. How many firewalls/routers/switches are within scope at each campus?

    Answer: One per campus.

16. How many servers are in-scope at each campus?
    Answer: We store no credit card data on University servers. The full breakdown of device count between clients and supporting servers will be provided to the winning bidder.

17. How many devices are in-scope at each campus?

    Answer: see updated device counts below

#	Institution Name	Location	IP
1	University of Maine	Orono, Maine	75
2	University of Maine at Farmington	Farmington. Maine	10
3	University of Southern Maine	Portland, Maine	10
4	University of Maine at Augusta	Augusta. Maine	8
5	University of Maine Augusta – Bangor Campus	Bangor, Maine	2
6	University of Maine at Fort Kent	Fort Kent, Maine	3
7	University of Maine at Machias	Machias, Maine	3
8	University of Maine at Presque Isle	Presque Isle, Maine	2

18. How many web applications?
    Answer: As testing needs arise, the University will develop testing requirements in conjunction with the winning bidder at rates contained in their proposal. We have no specific web applications to test at this time.

19. How many mobile applications?
    Answer: As testing needs arise, the University will develop testing requirements in conjunction with the winning bidder at rates contained in their proposal. We have no specific mobile applications to test at this time.

20. What is the anticipated budget for this project?
    Answer: During the past years, the University has paid approximately $13,000 for penetration testing of the PCI sites. Our goals have been to meet the requirements of PCI-DSS. We are prepared to pay more if the most suitable solution is higher.

21. Fill out our PCI Pen Testing Discovery Doc. Please complete 1 copy for each site in scope(7 docs total).
    Answer: We will present Pen Testing discovery details to the winning bidder.

22. Can the internal network penetration tests for each of the UMaine sites be performed from a single location or will we have to travel to each site separately to access the networks?
    Answer: No single location will provide a vantage point for all internal penetration tests. No, travel is not a requirement for this solution.

23. Will the payment devices/assets be remotely accessible via a VPN Tunnel
    Answer: We do not offer VPN access to internal payment environments.

24. Can testing be done remotely?
    Answer: External and internal penetration testing is required, but bidders may propose both these types be done remotely.

25. Maine is a large state so can campus visits be remote via video, and or phone?
    Answer: External and internal penetration testing is required, but bidders may propose both these types be done remotely. Communications with Information Security Analysts can be done remotely via phone or desktop video.

26. How many card transactions do you handle per year?
    Answer: Transactions counts may be provided to the winning bidder as needed.

27. Approximately how many individual transactions per year, regardless of value?
    Answer: Transactions counts may be provided to the winning bidder as needed.

28. For example has a particular SAQ been mandated as a result of a breach, a deadline been set, or reduction in requirements been agreed
Answer: Merchants self-assess with no externally mandated SAQ.

29. Did you complete a self-assessment or were you assessed by a QSA?
Answer: The University merchants all complete self-assessments and are not assessed by a QSA.

30. Are you a merchant/service provider?
Answer: No. The University is not a service provider at this point. No contracted merchants have been allowed to operate on the University's networks

31. Are you compliant with any other information security standards?
Answer: Parts of the University are subject to a number of compliance programs including GLBA, Export Control (ITAR/EAR), and HIPAA. However, penetration testing under this RFP is only required for PCI.

32. Can you tell us more about the network segregation?
Answer: Each campus has one or more firewalled segments to protect payment devices. Full details will be provided to the winning bidder.

33. Number of workstations at each site?
Answer: Each merchant consists primarily of workstation/client devices. A final break-down of client & server device count will be provided to the winning bidder.

34. Number of servers at each site?
Answer: Each merchant consists primarily of workstation/client devices. A final break-down of client & server device count will be provided to the winning bidder.

35. Which operating systems are in use?
Answer: Details of Operating systems types will be provided to the winning bidder.

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

37. Can all networks/VLANs in scope be accessed from one network point?
Answer: No, and we seek affordable approaches to providing the required Internal and External pentests, to include the use of remote access devices.

38. Number of networks/VLANs in scope?
Answer: approx. 10

39. Is there any Wireless capability?
Answer: none in scope for Level 1 testing.

40. Number of Access Points?
Answer: N/A

41. Number of SSIDs broadcasted?
Answer: N/A

42. What types of authentication are in use, if any?
Answer: Details of authentication for payment environments will be provided winning bidder.

43. Where is geographical location of the internal environment?
Answer: see updated device counts above.

44. Can all locations be accessed from one main site?
Answer: No, and we seek affordable approaches to providing the required Internal and External pentests, to include the use of remote access devices.

45. Number of Firewalls including brands?
Answer: Details of firewall brands will be provided to the winning bidder.

46. Details of any corporate remote access systems e.g. Outlook Web Access, SSL VPN etc.
Answer: None in scope for Level 1 testing.

47. Number of staff per location?
Answer: The University publishes updated staffing statistics at: https://www.maine.edu/about-the-system/ums-data-book/

48. Number of devices per location
Answer: see updated device counts above.

49. Are the locations within a shared campus environment?
Answer: No.

General Questions:

50. Have any previous penetration tests been conducted before? Does the awarded vendor have access to those reports?
Answer: PCI Penetration tests have been conducted for more than five years. The results of prior tests are not available to the awarded vendor.

51. Do you have any special timeframe requirements for the engagement?
Answer: The Target Timeframes for the first engagement are identified on Page 33 of the RFP. However, the bidder can propose a different timeframe.

52. Are these targets production or dev/UAT (user acceptance testing)?
Answer: Production.

53. Are there any firewalls, IDS, or IPS in place?
Answer: Yes.

54. Are there any 3rd parties that need to be contacted in advance of the pen test (hosting providers, 3rd party security monitoring service providers, etc.)
Answer: No.

55. Have all systems been recently backed up?
Answer: Yes.

56. Is it possible to perform the assessment via a remote testing appliance?
Answer: External and internal penetration testing is required, and bidders may propose both these types be done remotely.

Internal Scope Questions:

57. Please provide the total number of IP addresses in scope:
Answer: see updated device counts above.

58. Please provide an approximate amount of server/network devices:
Answer: Each merchant consists primarily of workstation/client devices. A final break-down of client & server device count will be provided to the winning bidder.

59. Please provide an approximate number of workstations.
Answer: Each merchant consists primarily of workstation/client devices. A final break-down of client & server device count will be provided to the winning bidder.

60. What kind of technologies are in scope (Database Servers, Operating Systems, Routers, ERP Applications, etc.)?
Answer: Each merchant consists primarily of workstation/client devices protected by a firewall. A final break-down of client & server device count will be provided to the winning bidder.

61. Are there predefined targets, high-priority assets we should consider for this project? a. Could you please describe them briefly?
Answer: Yes, predefined targets at the locations & approx. device count as updated above.

External Scope Questions:

62. Please provide the total number of external IP addresses in scope.

Answer: Each location has at least 1 external IP. Details of expected behavior of these IPs will be provided to the winning bidder.

63. How many of those external IP addresses are expected to be alive?
Answer: Each location has at least 1 external IP. Details of expected behavior of these IPs will be provided to the winning bidder.

64. Are there Unauthenticated Web Applications hosted on any of these hosts?
Answer: There are no web application in scope for Level I testing. As testing needs arise, the University will develop testing requirements in conjunction with the winning bidder at rates contained in their proposal.

65. Are there external Web Services or APIs hosted on any of these hosts?
Answer: No.

66. Is there an Intrusion Prevention System in place?
Answer: Yes.

67. Are any of the IPs in scope hosted on AWS or similar cloud provider
Answer: No.

Web Application Scope Questions:

68. For each application expected to be in scope, please provide the following: i. Number of Dynamic Pages
    a. Number of API Endpoints
    Answer: Details provided to the winning bidder.

    b. Number of User Roles
    Answer: Details provided to the winning bidder.

69. What type of payment devices/assets will be tested?
Answer: Each merchant consists primarily of workstation/client devices. A final break-down of client & server device count will be provided to the winning bidder.

70. Are the institutions interconnected from a network infrastructure standpoint?
Answer: Yes.

71. How many web applications are in scope of Level I Penetration Testing?
Answer: None.

72. Would it be possible to get the RFP in a Word Document?
Answer: Yes.

73. Will Bids outside of the traditional penetration testing cost structure (Driven by hours and an hourly rate) be accepted?
Answer: Yes, we will review proposals using innovative approaches.

74. Providing an overview and a demonstration of our platform helps drive home the understanding of our value/differentiation from traditional penetration testing. Would it be possible to schedule an abbreviated 30-minute session with stakeholders prior to the RFP Submission Date of December 13th?
Answer: No.

75. Scoping is required to verify whether the asset is a single web application assessment versus a collection of multiple applications. The following questions will help you and Synack outline key milestones and requirements to execute the penetration test.

Answer: There are no web application in scope for Level I testing. As testing needs arise, the University will develop testing requirements (in table below) in conjunction with the awarded Respondent at rates contained in their proposal.

Business Context	
Specify the primary purpose of the web application(s) to be tested.	{answer}
Specify whether the web application environment is a production or lower (non-production) environment.	{answer}
Technical Scope	
Specify the URL(s) to be tested.	{answer}
Specify any subdomains that are in scope.	{answer}
Environment Understanding	
Specify whether the in scope application(s) is public facing or within a closed/internal environment.	{answer}
Application Accounts* ***The Synack Red Team (SRT) will require application accounts to perform testing**	
Define the authentication process/workflow (i.e. username and password or something that differs).	{answer}
Specify the user account application roles (personas) that are in scope for testing.	{answer}
If multiple application roles (personas) are in scope, describe each role and the data each role is authorized to access.	{answer}

Host Infrastructure

Business Context	
Specify the primary purpose of the environment to be tested.	{answer}
Specify whether the environment is a production or lower (non-production) environment.	{answer}
Technical Scope	
Specify the IP network ranges that are in scope, including CIDRs for each.	{answer}
Specify the expected number of active IP addresses to be tested.	113 active IPs across 7 Locations
Specify whether any of the hosts or IP addresses in scope are in a Cloud Service Provider (CSP) such as Amazon Web Services, Microsoft Azure, and/or Google Compute Engine.	{answer}
Environment Understanding	
Specify if testing will be performed on an internal network, external network or both.	{answer}
If testing is to be internal would you want us to connect to your network device for the site-to-site VPN tunnel or would you use our VMware OVA or AWS AMI? • If connecting to your network device please describe.	{answer}