Administrative Office of the Courts

Operations Division

Questions/Responses No. 2 to the

Request for Proposals (RFP) K21-0023-29

JIS Vulnerability Assessment

Ladies and Gentlemen:

The following questions for the above referenced RFP were received by e-mail and are answered and posted for all prospective Offerors. The statements and interpretations contained in the following responses to questions are not binding on the Maryland Judiciary unless the RFP is expressly amended. Nothing in the Maryland Judiciary's response to these questions is to be construed as agreement to or acceptance by the Maryland Judiciary of any statement or interpretation on the part of the Offeror asking the question.

8. Question: Is compliance with the State of Maryland IT Security Manual v1.2 a component/requirement of this RFP response?

   Response: No.

9. Question: Can you clarify your number of IP addresses? The RFP states "(20) CIDR blocks." Are these /24 CIDR blocks, or another size?

   Response: 16 blocks.

10. Question: Noting the required electronic version for each proposal, I'd like to confirm that a USB flash drive is sufficient given the potential risks it may have.

    Response: Yes, USB is accepted.

11. Question: Is it possible to know total assets within the organization?

    Response: 13,000.

12. Question: Is there an internal IT team within your organization?

    Response: Yes.

13. Question: Is it possible to know the total subnetworks within the organization.

    Response: 16.

14. Question: In regard to the requirement of registering with the Department of Assessments and Taxation, do we need to be a Maryland in-state legal entity?

Response: Maryland law requires certain foreign (i.e., out-of-state) businesses to register in Maryland depending on the nature of their relationship and connections with the State of Maryland. The Administrative Office of the Courts cannot advise you whether you need to register. For further information, vendors may try contacting the Maryland State Department of Assessments and Taxation or seek legal counsel for assistance.

15. Question: Regarding 1.26 Verification of Registration and Tax Payment (page 10 Does this apply to out of state limited liability partnerships as well as corporations?

Response: Yes.

16. Question: Is testing to be conducted during or after hours for the internal network environment?

Response: During business hours as it is not intended to bring down anything.

17. Question: What is the expected deliverable from a retest? Nothing is specified in the RFP.

Response: To validate any changes or updates made based on a discovered vulnerability.

18. Will AOC be able to provide network architecture or a list of endpoints and its associated details that are in scope of this RFP?

Response: Agency can provide list of endpoints.

19. For vulnerability assessment, does AOC have any preference for a Risk Assessment Methodology like NIST CSF, NIST 800-30, CVE, CWE, etc or is the contractor free to choose one that serves AOC needs in the RFP.

Response: We try to closely align with NIST framework.

20. Referring to section 2.12 (L), it says Judiciary may provide the Contractor with a laptop to perform the work. Please confirm if it will be provided and whether the Contractor staff are allowed to install software required to perform the work as mentioned in the RFP.

Response: VDI session or device VPN.

21. Can the Agency state the overall purpose of the assessment (e.g., compliance, evaluation of security posture and maturity, periodic security assessment)?

Response: Periodic security assessment.

22. Will code execution be permitted (e.g., to validate vulnerability, gain system access)?

Response: Not for the vulnerability scan portion.

23. Is the web application protected by a Web Application Firewall (WAF)? If so, do you desire testing with the WAF enabled, disabled, or both?

Response: Each application is behind a firewall but no web application firewall.

24. Provide the estimated number of employees that will be in-scope.

Response: 5,000.

25. How many different physical locations are in scope? If possible, please list the locations and any geographical considerations.

Response: 70.

26. Will on-site access be required to conduct the assessment? (VPN or other remote access methods are acceptable alternatives.

Response: VPN or VDI is required as location is not open to the public.

27. Does AOC have Nessus installed on their network?

Response: Yes.

28. Is the application a third-party commercial product or a product developed by your company?

Response: This will depend on the application selected.

29. Will the Agency please list the name and purpose of the web application(s) in scope.

Response: Determined upon award.

30. How many unique wireless networks are in-scope? What is the purpose of each (e.g., corporate, guest, store wireless)?

Response: 2 public and private.

31. What is an estimated number of workstations in the network?

Response: 6,500.

32. For web application penetration testing, can we use OWASP Top 10 for risk rating?

Response: Yes.

33. Will AOC share the SDLC to the contractor who gets awarded?

Response: No.

34. On page 25 you ask for evidence of the offeror's financial capacity to provide the services via profit and loss statements and balance sheets. We are a privately held corporation and do not normally release our financial statements. In lieu of these statements will you accept a copy of our Dun & Bradstreet Supplier Qualifier Report.

Response: Yes.

35. Will JIS be providing the scanning tools? Nessus and CIS Benchmark are a couple of the tools that would be necessary.

Response: No, vendor supplies tools.

36. Will all the pen test findings be retested in during the retest?

Response: No just remediated actions.

37. The insurance requirements have auto listed separately for bodily injury and property damage— if our insurance has this as a combined single limit, will this satisfy the requirements?

Response: Yes.

38. Upon contract award, does both AOC as well as the contractor need to perform a background check of the contractor staff. If so, what specific background check needs to be performed by the contractor?

Response: The AOC cannot comment on a Contractor's internal processes. Upon Contract award, the AOC will perform background checks as needed.

39. Could the customer provide the number of firewalls, routers, switches, load balancers, DNS servers, web/application services and all other inventory counts to assist with identifying accurate workload?

Response: 13,000.

40. Will both retests occur during the same window?

Response: Separate window.

41. Regarding the penetration test, will credentials be provided to assess the application?

Response: Yes.

Issued by: Valerie L. Mitchell

Procurement Officer

September 11, 2020