Administrative Office of the Courts

Operations Division

Questions/Responses No. 3 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.

1. Question: Do you want the consultant to conduct credentialed vulnerability scans?

   Response: Yes, Credentials will be supplied.

2. Question: Besides vulnerability scanning, do you want the consultant to perform manual tests, such as reviewing configuration settings and interviewing IT personnel in order to address the second bullet under 2.4.1?

   Response: yes, meetings should be via Teams or Skype and coordinated through the PM.

3. Question: The assessment appears to be only focused on internal systems, not internet-facing systems, is that correct?

   Response: Yes.

4. Question: What is the expected deliverable of the assessment (e.g., user click statistics, code execution, and lateral movement potential)?

   Response: Task 1 identify any existing vulnerabilities Task 2 pen ten internal application for vulnerabilities.

5. Question: Understanding that the application hasn't been chosen yet, how many user roles are to be used for testing within the target application?

   Response: Single standard user.

6. Question: Can the AOC better define the scope for web security assessments-servers, applications, cloud/on premise?

   Response: Target of task 2 is dependent of the information from task 1.

7. Question: Regarding confidential information included in our proposals (RFP Section 3.4.3), in order to comply responders should note all confidential sections on yellow paper after the title page. Should we also note other instances of confidential information on a case by case basis as they appear throughout the proposal? (IE. clearly mark our client reference pages as confidential, clearly mark technical methodology pages as confidential, etc.)

   Response: If it's behind the title page. We would recommend putting all confidential information together if possible.

8. Question: Does JIS have existing Venerability assessment and Pen test tools (software/hardware) that can be used or have to be leveraged? If so, can you please share the tools info.

   Response: No tools are to be supplied by the vendor.

9. Question: If the contractor is expected to procure the software /hardware tools, JIS will need to grant us access to install, configure the tools as required.

   Response: Scans would be run from either a VDI session from which the vendor will have the ability to load programs or from the vendor's device that they have admin rights to.

10. Question: The Cyber Security/Data Breach insurance specifies a $10,000,000 coverage "for any service offering hosted by the contractor." We understand that we may be in possession of some sensitive data as the result of our scans, however we would not be hosting any services under this RFP. Would the minimum $10,000,000 coverage still apply even though we would not be hosting any services?

    Response: Yes.

11. Are all systems located in one location or will the scans need to be done over network connections to remote offices, as well?

    Response: Remote scans

12. Regarding the target systems to be assessed, how much information will the Agency provide regarding those systems to the levels of providing us: i.e.
    zero knowledge about the systems, some knowledge about the systems, or full knowledge about the systems?

    Response: Some knowledge about the systems.

Issued by: Valerie L. Mitchell
Procurement Officer
September 16, 2020