MARYLAND JUDICIARY

ADMINISTRATIVE
OFFICE OF THE COURTS

GOVERNMENT RELATIONS
INFORMATION TECHNOLOGY
INTERNAL AFFAIRS
JUDICIAL COLLEGE OF MARYLAND
OPERATIONS
PROGRAMS

Questions/Responses No. 4 to the

Request for Proposals (RFP) K17-0073-29

Cyber Security Program Assessment & Analysis

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.

29. Question: What is the size (number of devices and/or users and number of sites) of the system to be assessed?

    Response: Environment specifics will be provided post award. Please see response to Question # 20.

30. Question: What assessment tools will Maryland Judiciary make available for information security controls assessment?

    Response: The Maryland Judiciary will not make any tools available. The awarded Contractor will supply all tools.

31. Question: Will the contractor be required to purchase/own the information security controls assessment tools?

    Response: The awarded Contractor will supply all tools.

32. Question: What is the authorization process for granting non-government owned equipment on the network?

    Response: The process will be conveyed post award.

33. Question: As part of assessments we understand the scope includes the process and policy evaluation and also technical assessment too. For technology Penetration testing and Vulnerability Assessment as part of our technical assessment; we can provide more accurate estimates if you can share the number of IT assets (Virtual, Network, Database, Physical) etc. This helps to estimate the efforts and tools to use.

    Response: Environment specifics will be provided post award. Please see response to Question # 20.

34. Question: As part of gap analysis, we understand that there is already an established technical security setup, policy and controls based on defined Risk & Compliance baseline of Maryland Judiciary. Can you please confirm the statement? Or is there expectation to do the gap analysis based on as-is assessment against a new security baseline which needs to be created as per this engagement?

    Response: Confirmed; see section 2.5.1 of the RFP

35. Question: Will the successful bidder be allowed to view documents, i.e. policies and procedures, prior to performing on-site activities?

    Response: Post award and after all required background checks are complete, the awarded Contractor will be given access to the documentation while on site.

36. Question: Will the successful bidder be able to perform analysis and reporting activities off-site?

    Response: No, see section 2.7 of the RFP.

37. Question: Can the type of in scope operating systems be provided?

    Response: Windows, Linux, AIX, Mainframe

38. Question: Is there a compliance or regulatory objective trying to be met as part of the assessment?

    Response: See section 2.2 of the RFP.

39. Question: Should we provide our own equipment (laptops, etc.) to the consultant(s) we assign to the project?

    Response: The consultants assigned to the project will be issued a machine for use during the engagement. Any special equipment needs will be evaluated on a case by case basis.

40. Question: Is vulnerability scanning and/or penetration testing required or desired as part of this assessment?

    Response: No penetration testing is required as a part of this assessment. A vulnerability scan can be performed as a part of Task 1.

Issued by: Whitney Williams
Procurement Officer
May 1, 2017