ADMINISTRATIVE OFFICE OF THE COURTS

MARYLAND JUDICIAL CENTER
580 TAYLOR AVENUE
ANNAPOLIS, MARYLAND 21401

Pamela Harris, State Court Administrator
410-260-1295

Faye D. Matthews
Deputy State Court Administrator
410-260-1257

Mark Bittner
Assistant Administrator
Judicial Information Systems
410-260-1001

Louis G. Gieszl
Assistant Administrator
Programs
410-260-3547

Melinda K. Jensen, CPA
Assistant Administrator
Operations
410-260-1240

Julie R. Linkins, Esq.
Assistant Administrator
Education
410-260-3549

Kelley O'Connor
Assistant Administrator
Governmental Relations
410-260-1560

Kathleen E. Wherthey, Esq.
Assistant Administrator
Internal Affairs
410-260-3453

ADMINISTRATIVE OFFICE OF THE COURTS
MARYLAND JUDICIAL CENTER
580 TAYLOR AVENUE
ANNAPOLIS, MARYLAND 21401

Questions/Responses No. 1 to the Request for Proposal (RFP)
JIS Vulnerability Assessment
January 21, 2015

Ladies and Gentlemen:

The following questions for the above referenced RFP were received and are answered and posted for all prospective Contractors who received the RFP. 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 Contractor asking the question.

Question: Is the Maryland Judiciary looking for a vulnerability assessment or a penetration test? Sometimes, the terms are used interchangeably, so we wanted to confirm.

Response: vulnerability assessment only

Question: Does the stated 50 IPs Total mean 50 IPs per VLAN, or 50 IPs across all 6 VLANS – 50 vs 300 total count?

Response: The Administrative Office of the Courts is issuing this Request for Proposals to award one contract to a qualified firm to perform an External Vulnerability Assessment Scan on a class "B" IP range with a maximum of 500 IP addresses. If additional IP's are identified, the vendor will notify the Maryland Judiciary and provide a cost for each additional IP to be scanned prior to any work being performed. The vulnerability scan is to be performed externally (offsite) (response 2)

Question: Does the COBIT requirement mean that the winning vendor is certified in the COBIT Framework or just that the scan reports and analysis be tailored to use the COBIT framework?

Response: scan reports and analysis be tailored to use the COBIT framework

Question: Is the stated COBIT framework expected to be COBIT 4.1 or COBIT 5?

Response: COBIT 4.1 or later (response 16)
Question: Do past experiences require specific COBIT framework implementation or just like experience using other similar IT & Security Frameworks like NIST 800-53 or ISO 27001?

Response: YES

Question: Is the expected IP space inclusive of wireless and wireline connected devices?

Response: YES

Question: Are the passive and active scans of the six (6) VLANs to be done during normal business days/hours or will the JIS provide a specified time window or "Green Zone"?

Response: Green Zone

Question: If a specified "Green Zone" time window for the passive and active scans of the six (6) VLANs is to be utilized, will this "Green Zone" be after hours during the week or weekend?

Response: YES

Question: Based on the responses during the Pre-Proposal conference it was stated that the requirement for Drupal experience is no longer mandatory. Will the RFP be modified to reflect the removal of Drupal?

Response: Yes. Please see Addendum.

Question: Based on the responses during the Pre-Proposal conference it was stated that the vulnerability scans were only to be performed on the external systems. Will the RFP be modified to reflect that all vulnerability scans are to be performed on only the external systems?

Response: JIS request the language reflect external only. Please see Addendum.

Question: Based on the responses during the Pre-Proposal conference it was stated that the vulnerability scans were to be performed remotely. Will the RFP be modified to reflect the change to remote only vulnerability scanning?

Response: JIS request the language reflect remote. Please see Addendum.

Question: Is a penetration test to validate the potential exposures raised through the vulnerability assessment going to be part of the scope of this review? At this point, the scope refers to a vulnerability assessment only.

Response: NO

Question: Are you looking for an external vulnerability assessment only or is there an expectation for an internal assessment as well?

Response: External only

Question: In section 3.4.7 of the RFP, References, it states that the following must be provided for each client reference: "The services provided, scope of the contract, geographic area being supported, and performance objectives satisfied, and **number of employees serviced**"

Response: See Section 3.4.7.

Question: As it pertains to that last requirement, what exactly is the State of Maryland looking for? Is this the number of end users/stakeholders affected by our work, or the number of our employees that we will be providing to support this task?

Response: Please explain the steps you plan to take to safeguard the site content throughout this project.

Question: Would the Administrative Office of the Courts consider amending the RFP to allow use of ISO 27002 or NIST as the standard of measurement?

Response: NO

Question: If the answer to the above is no, would the Administrative Office of Courts consider amending the RFP to allow of ISO 27002 or NIST as the standard of measurement if a mapping to COBIT is provided?

Response: NO

Question: Understanding that the contractual basis for the awarded contract will be JIS' terms and conditions, will (i) JIS object to accepting a the vendor's including their standard commercial terms and conditions for the proposed services in its proposal and (ii) can those terms, as negotiated, be incorporated into the awarded the contract?

Response: Please see section 1.20.

Question: Does the JIS currently follow the COBIT 5 framework?

Response: currently still using 4.1

Question: Does the JIS want the vendor to scan the entire 6 Class B Networks (65,000 IP's) or does JIS plan to provide 50 active IP addresses and have the vendor scan just those IPs?

Response: Scan entire range.

Question: Please provide total number of endpoints, routers, firewalls and servers

Response: Not a part of what we are asking for.

Question: Is there any limitation to the hours in which scanning / penetration testing can be performed?

Response: JIS will identify a Green Zone for the testing.

Question: How many Active Directory Domain Controllers does JIS have in its network?

Response: Not a part of what we are asking for.

Question: 2.1 The scope of target systems to be scanned is not clear.

Response: The Administrative Office of the Courts is issuing this Request for Proposals to award one contract to a qualified firm to perform an External Vulnerability Assessment Scan on a class "B" IP range with a maximum of 500 IP addresses. If additional IP's are identified, the vendor will notify the Maryland Judiciary and provide a cost for each additional IP to be scanned prior to any work being performed. The vulnerability scan is to be performed externally (offsite) (response 2)

Question: Are these externally facing hosts only to be tested from external and internal network connections (e.g., on both sides of the firewalls)? Are we to scan no more than 50 hosts in total? Are AD domain controllers the only internal systems to be tested?

Response: The Administrative Office of the Courts is issuing this Request for Proposals to award one contract to a qualified firm to perform an External Vulnerability Assessment Scan on a class "B" IP range with a maximum of 500 IP addresses. If additional IP's are identified, the vendor will notify the Maryland Judiciary and provide a cost for each additional IP to be scanned prior to any work being performed. The vulnerability scan is to be performed externally (offsite) (response 2)

Question: 2.2.4 In conjunction with me inquiry about 2.1, is this a list of the types of hosts that would likely be found and tested during the vulnerability scans - internally, externally?

Response: YES and external only

Question: 2.3.1 I am very familiar with COBIT, but it is not considered to be a measure of vulnerability or criticality. What exactly are the specifics/details of your criticality scales for evaluating vulnerabilities in this project?

Response: Vendor supplied ranking

Question: 2.4.2 Based on our experience of over 20 years in doing vulnerability scans, it is not realistic to be able to produce a draft report of vulnerabilities if there are a lot of vulnerabilities encountered during the scan. Please clarify the nature of what a "draft report" should contain.

Response: Identify critical vulnerabilities found during the scan and recommended remediation; List non-critical vulnerabilities found during the network scan.

Question: 2.5 I question the need for the amount and types of insurance for this type of work. I would be doing the work as a single consultant exclusively, so I don't understand the requirement for Workers Compensation or liability for personal or bodily injury, as this work is not dangerous or physically harmful and mostly involves sitting near a computer to execute vulnerability scans. Also, I would not be driving any automobiles to deliver this work defined in this RFP. Is it possible to get a general waiver for what we consider irrelevant insurance coverage requirements for this type of work?

Response: Please see section 1.20.

Question: .3.4.7 We do not consider "the number of employees serviced" to be valid criteria for providing vulnerability testing services which are reported to a single point of contact for the client being serviced. Can you please review this requirement to determine if it should be ignored.

Response: No.

Question: 3.4.8 Please clarify why or to what extent a single person delivery of professional services needs to demonstrate the financial capacity to deliver those services. Can an IRS Schedule C be used to meet this requirement if necessary?

Response: Please see section 3.4.8, 1 and 2.

Question: In section 3.4.2 of the RFP, it states that "Section 2 of this RFP provides requirements and Section 3 provides reply instructions…in addition to the instructions below, the Offeror's technical proposals shall be organized and numbered in the same order as this RFP." In section 3.2.5 part 2, it states that, "The Offeror shall submit a response to each item listed under section 2.3 through 2.4." Furthermore, at the industry day, the instructions were given that the numbering of the Proposal should match the numbering in the RFP. If that is the case, sections of the Proposal would not begin sequentially. A. Are the instructions to match the RFP numbering ONLY to include Section 2? B. Should the rest of section 2 be addressed so as to provide a sequential proposal?

Response: The numbering of the Proposal should match the numbering in the RFP.

Question: In the RFP it states that Offerors will have 48 hours to submit various reports when necessary. Does 48 hours mean 2 BUSINESS days or 2 CALENDAR days?

Response: 2 BUSINESS days

Question: NSG received the sign-in sheet from the industry day; are the vendors listed on the sign in sheet inclusive of the call-in participants from the industry conference?

Response: Daniel Redding, Saint Security Services and Laural Hargadon, NIT Services.