

RFP Questions and Clarifications Memorandum

To: Vendors Responding to RFP Number 3606 for the Mississippi Department of Information Technology Services (ITS)

From: David L. Litchliter

Date: October 20, 2009

Subject: Responses to Questions Submitted and Clarifications to Specifications

Contact Name: Melinda Simmons

Contact Phone Number: 601-359-9535

Contact E-mail Address: Melinda.Simmons@its.ms.gov

RFP Number 3606 is hereby amended as follows:

1. Section VII: Technical Specifications, Item 6.9 – Vendor is precluded from providing *security/risk assessment* services on networks where the Vendor has *an existing contract to perform* installation, maintenance, and/or support services.
2. Section VII: Technical Specifications, Item 7.1.9 - If requested, Vendor must review the entity's existing security policy, *compare it to the State's Enterprise Security Policy (ESP)*, and make recommendations as well as provide examples of additional policy statements relative to the following areas of security.
3. Section VII: Technical Specifications, Item 11.3 – The current table in the RFP is replaced by the following table:

NUMBER OF DEVICES	DESCRIPTION	ESTIMATED NUMBER OF HOURS
Computer Systems		
1	Windows External Vulnerability Scan	
1	Solaris/Unix/Linux External Vulnerability Scan	
1	Mainframe Vulnerability Scan	
1	Windows Internal Vulnerability Scan	

NUMBER OF DEVICES	DESCRIPTION	ESTIMATED NUMBER OF HOURS
	Examples: Internal Vulnerability Assessment Scan, OS Security Configuration Settings Review, etc...	
1	Solaris/Unix/Linux Internal Vulnerability Scan	
1	Mainframe Internal Vulnerability Scan	
1	Workstation Internal Vulnerability Scan	
	Other Computer Systems (describe)	
Network Systems		
1	Firewall Vulnerability Scan	
1	Firewall Analysis	
1	External Router Analysis	
1	Internal Router Analysis	
1	Switch Analysis	
1	Wireless Access Point Analysis	
1	VPN Assessment	
	Other Network Systems (describe)	
Remote Access Testing		
1	Remote Access Server Assessment	
	Other Remote Testing (describe)	
Security Services		
1	Penetration Services	
1	Security Policy Review	

4. Section VIII Cost Information Submission – The current table in the RFP is replaced by the following table:

NUMBER OF DEVICES	DESCRIPTION	PRICE
Computer Systems		
1	Windows External Vulnerability Scan	
1	Solaris/Unix/Linux External Vulnerability Scan	
1	Mainframe Vulnerability Scan	
1	Windows Internal Vulnerability Scan Examples: Internal Vulnerability Assessment Scan, OS Security Configuration Settings Review, etc...	
1	Solaris/Unix/Linux Internal Vulnerability Scan	
1	Mainframe Internal Vulnerability Scan	
1	Workstation Internal Vulnerability Scan	
	Other Computer Systems (describe)	
Network Systems		
1	Firewall Vulnerability Scan	
1	Firewall Analysis	
1	External Router Analysis	
1	Internal Router Analysis	
1	Switch Analysis	
1	Wireless Access Point Analysis	
1	VPN Assessment	
	Other Network Systems (describe)	
Remote Access Testing		
1	Remote Access Server Assessment	
	Other Remote Testing (describe)	
Security Services		
1	Penetration Services	
1	Security Consulting Services (hourly rate)	
1	Security Policy Review	
	Other Security Services (hourly rate) (describe)	
Other Services		
	Travel (Vendors may propose charges for travel, travel time, lodging, per diem, etc. The State will not be responsible for	

	any travel charges for engagements within 50 miles of any of the Vendor's offices. All other expenses will be based on the Mississippi Department of Finance and Administration's travel policies.)	
	Other (describe)	

The following specification has been added to RFP Number 3606:

1. Section VII: Technical Specifications, Item 6.11 – Vendor must describe if and how the severity of vulnerabilities are rated, providing the scale used to rank the vulnerabilities and the qualifying factors for ranking each vulnerability.

The following questions were submitted to ITS and are being presented as they were submitted, except to remove any reference to a specific vendor. This information should assist you in formulating your response.

Question 1: Can we take exceptions to the Standard Contract (Exhibit D)?

Response: **No exceptions to Exhibit D: Standard Contract will be accepted. See Section VII: Technical Specifications, Item 13.1.3**

Question 2: Can vendors submit pricing in alternate formats from the one shown in section VIII as long as the alternate format satisfies the requirement that the State can calculate pricing for a security/risk assessment regardless of the size and complexity of the network? For example, there are multiple efficiencies gained as the number of systems increases for a vulnerability assessment, so the price for an assessment consisting of 25 systems would not be 25 times the cost of assessing 1 system. Likewise, the price for an assessment of 50 systems would not necessarily be twice the cost of assessment of 25 systems.

Response: **Vendors may include additional formats to show discounts or different pricing options; however, each vendor must provide pricing in the format that was requested in the RFP as their primary cost proposal.**

Question 3: Reference page 36 Section 6 Subsection 6.5- if selected for an oral presentation, will you allow a conference call/WebEx in lieu of an onsite visit?

Response: **The agency and Vendor may agree upon an alternate method of presenting the findings, such as a conference call or video conference in lieu of an onsite visit. However, it is the preference of ITS that the Vendor make an onsite presentation.**

Question 4: Reference pages 39/40 Subsection 11.3- can you provide a more detailed description of what the State is looking for in terms of Penetration Services and

Security Consulting Services or can we describe in detail our services in addition to an estimated number of hours?

Response: **The Vendor may provide a detailed description of the proposed services in addition to the estimated number hours to perform those services.**

Question 5: Reference page 39 Subsection 10.2- certain security services we provide require a base cost to set up and configure equipment and software, can we provide a base (fixed cost) for certain services and then a unit cost?

Response: **Yes, Vendor may specify the base and/or unit costs for each line item in Section VIII: Cost Information Submission.**

Question 6: Reference page 44- please clarify “Change Order Rate (per hour)?

Response: **The Change Order Rate and Procedure are described in Exhibit D: Standard Contract, Article 39.**

Question 7: Reference page 39-Subsection 10.2-Do you consider Risk Assessment Services as part of Security Consulting Services as listed on the Chart on page 40?

Response: **No, the consulting services item that is listed in the services table is considered to be consulting services within the scope of security/risk assessment services. The consulting services item is meant to be an hourly rate for a consultant to provide the customer with assistance, expertise, recommendations, and guidance regarding security/risk assessment related items from the customer. This is not to be used as general consulting services for the customer.**

The security/risk assessment services referenced in Item 10.2 are the fixed-price deliverables listed in the first three sections of the table under Item 11.3. See the revised tables for 11.3 and the Cost Information Submission above.

Question 8: Page 43, Section VIII: Cost Information Submission - RFP Text: “Vendors must propose a summary of all applicable project costs in the matrix that follows... All assumptions, including travel related assumptions, must be documented fully in an attached spreadsheet.” Can ITS please verify the reimbursement rate the State is approved to pay for mileage, overnight, and per diem?

Response: **The State is allowed to pay rates not to exceed those specified by the Department of Finance and Administration, Office of Purchasing and Travel: <http://www.dfa.state.ms.us/Purchasing/Travel/Travel.html>.**

Question 9: In Section 11.3 of RFP 3606, page 39 – it requests that vendors propose a number of hours that it will take to accomplish each objective. Under what “assumptions” do we use to provide the number of hours that will be used for the Security Policy Reviews? Section 7.1.9 has a list of what is to be reviewed for the Security Policy Review; however, depending on the size of the agency and the regulations set by the ITS security policy and the level of complexity of the policy, the number of hours will vary. Do we base these hours on the smallest agency, who does not host their own email or web servers and simply has a fire wall an internal server and 50 workstations; or, is this should be based on an agency of 2500 users, with 5 mail servers, 10 web servers, 82 locations and 2500+ workstations?

Response: **Vendor may propose tier level pricing; however, the Vendor must provide a definition for each proposed tier. See the revised table for Item 11.3 above.**

Question 10: Pertaining to “Wireless Access Point Analysis” – what is ITS looking for here? Is this just to verify open and secure AP’s or is it to determine if there are rouge AP’s on the network?

Response: **The primary purpose of the “Wireless Access Point Analysis” is to review, analyze, and verify open and secure AP’s.**

Question 11: Will winning vendors be granted access to the ITS Security policy to make sure all security assessments are done in compliance with the state’s security regulations?

Response: **Each awarded Vendor may access the State’s Enterprise Security Policy by signing a specific Enterprise Security Policy Nondisclosure Agreement with ITS.**

Question 12: Regarding the SaaS System requirement for invoicing. What is involved in this process? Currently our operations department indicates that this is not something that our company is set up to do. Any specifics you can provide would be greatly appreciated.

Response: **Please contact the Department of Finance and Administration, Mississippi Management and Reporting System (MMRS) for more information: <http://www.mmrs.state.ms.us/ContactUs/index.shtml>**

Question 13: What is your mainframe platform?

Response: **Details regarding the State’s mainframe platform can be found in the Technology Infrastructure and Architecture Plan (http://www.its.ms.gov/docs/infrastructure_architecture_plan.pdf), beginning on page 11.**

Question 14: What is your firewall platform?

Response: The majority of agencies currently have Cisco firewalls. However, there are a number of agencies that have firewall equipment other than Cisco (e.g., Checkpoint, Sonicwall, Juniper).

Question 15: What is your network device platform?

Response: The majority of agencies currently have Cisco network equipment. However, there are a number of agencies that have network equipment other than Cisco (e.g., HP, Extreme, Brocade).

Question 16: What is defined by or what is your definition of Penetration Services?

Response: Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.

Pen tests can be automated with software applications or they can be performed manually. Either way, the process includes gathering information about the target before the test (reconnaissance), identifying possible entry points, attempting to break in (either virtually or for real) and reporting the findings.

The main objective of penetration testing is to determine security weaknesses. A pen test can also be used to test an organization's security policy compliance, its employees' security awareness, and the organization's ability to identify and respond to security incidents.

Question 17: Application testing is not mentioned, is that a need?

Response: Vendors may propose pricing for application assessment services; however, it is not a mandatory requirement.

Question 18: Billing preferences? Example, time and materials or fixed bid?

Response: Vendor must submit not-to-exceed fixed costs or hourly rates for each of the line items as directed in Section VIII: Cost Information Submission. See the revised Cost Information Submission table above.

Question 19: Do you have to be PCI certified to compete for this business? If yes, can we partner with another vendor for the PCI portion and do the rest on our own?

Response: It is not a requirement to be PCI certified to respond to this RFP. However, you may partner with another vendor for PCI services.

Question 20: Are there any requirements to provide remediation recommendations that correlate back to any specific regulatory requirements?

Response: **The primary purpose for the services requested in this RFP is to identify and provide feedback on standard security risks and vulnerabilities within a network. This contract is not the primary tool to be used for targeting specific regulatory requirements.**

RFP responses are due October 29, 2009, at 3:00 p.m. (Central Time).

If you have any questions concerning the information above or if we can be of further assistance, please contact Melinda Simmons at 601-359-9535 or via email at Melinda.Simmons@its.ms.gov.

cc: ITS Project File Number 38241