

RFP Questions and Clarifications Memorandum

To: Vendors Responding to RFP Number 3735 for the Mississippi Department of Information Technology Services (ITS)

From: Craig P. Orgeron, Ph.D.

Date: July 31, 2014

Subject: Responses to Questions Submitted and Clarifications to Specifications

Contact Name: Debra Spell

Contact Phone Number: 601-432-8132

Contact E-mail Address: debra.spell@its.ms.gov

RFP Number 3735 is hereby amended as follows:

1. Section VII, Item 5, Statements of Understanding, is being modified add a new Item 4.9 as follows:

“4.9 Intended Use for this RFP

4.9.1 Throughout the life of this contract, ITS plans to perform multiple security assessments on the ITS IT infrastructure per year. The size and scope of each assessment will vary; however, the Awarded Vendor and ITS will work together to determine the size and scope of each engagement.

4.9.2 For contracts with other state agencies, the Awarded Vendor and each individual agency will work together to determine the size and scope of each engagement.

4.9.3 In the interest of security, Vendor must be aware that some information will not be disclosed prior to the award, but will be provided to the Awarded Vendor as stated in Item 4.5 above. Vendor must also be aware that any specific information disclosed prior to the award is subject to change during the life of this contract.”

2. Section VII, Item 5, Statements of Understanding, is being modified add a new Item 4.10 as follows:

- “4.10 Since a complete inventory of ITS systems and application configurations, and other agencies’ systems and applications configurations will not be provided prior to award, the Vendor is requested to provide pricing based on one instance. For example, if the Vendor provides the cost for one Windows server, then ITS can determine the cost for a specific number of Windows servers by multiplying the cost for one by the total number that will be included in the assessment (number may vary during each of multiple assessments).”

Vendor must include in their proposal a response to each amended requirement as listed above. Vendor must respond using the same terminology as provided in the original requirements.

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: Does the State intend to award one or multiple contracts?

Response: **The State’s intent is to award to one Vendor, but multiple contracts may result should these services be used by other state entities.**

Question 2: Has the State standardized on a particular security methodology (NIST, etc.)?

Response: **The State of MS Enterprise Security Policy is currently being aligned with the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the security controls defined in the 800 series of publications by NIST.**

Question 3: How many sites (locations) are in scope for the project?

Response: **ITS has two primary locations which include the ITS State Data Center (3771 Eastwood Drive, Jackson, MS) and the Robert E. Lee Building (239 North Lamar Street, Jackson, MS). There is the potential that multiple agencies may utilize the award from this RFP and these agencies are located all over the state of MS.**

Question 4: Section 7.1 – How many Windows (server, desktop) systems are in scope for the project?

Response: **See Amendments #1 and #2 above.**

Question 5: Section 7.2 – How many Solaris and Linux systems are in scope for the project?

Response: **See Amendments #1 and #2 above.**

Question 6: Section 7.3 – How many and what type of Mainframes are in scope for the project?

Response: **There are currently three IBM zEnterprise mainframes located in the State Data Center utilized by ITS, the Mississippi Department of Human**

Services, and the Mississippi Department of Finance and Administration. Throughout the life of this contract, ITS plans to perform multiple security assessments on the ITS IT infrastructure per year, including one mainframe. As stated in response to Question #3 above, there is the potential that multiple agencies may utilize this RFP and these agencies are located all over the State.

Question 7: Section 7.4 – Can the state provide a network diagram detailing the network devices and locations in scope for the project? If not can the state provide the number, type and locations of the network devices in scope?

Response: **No. See the response to Question #4 above.**

Question 8: Section 7.4 - How many internal and external IP addresses are in scope for the project?

Response: **See amendments #1 and #2 above.**

Question 9: Section 7.5 – How many and what type(s) of Virtual Hosts are in scope?

Response: **See amendments #1 and #2 above.**

Question 10: Section 7.6 – Can the state provide the number of wireless devices and access points by location?

Response: **No. See amendments #1 and #2 above.**

Question 11: Section 7.7 – Can the state provide the number and type of firewalls by location?

Response: **No. See amendments #1 and #2 above.**

Question 12: Section 7.13 – What type (SQL, Oracle, DB2, other) and how many databases are in scope for the project?

Response: **The scope of this project could include several of each to the databases mentioned. See amendments #1 and #2 above.**

Question 13: Section 7.16 – What type and how many applications are in scope for the project?

Response: **The type and scope will vary. See amendments #1 and #2 above.**

Question 14: Section 7.16.3 – What webservers (IIS, Apache, etc.) are hosting the JAVA and .NET applications? How are these application hosted (internally, third party)?

Response: **Webserver hosting information will not be provided prior to award. See Item 4.9.3 in amendment #1 above. Applications may be hosted internally or with third parties.**

Question 15: Section 7.19 and 7.20 – Will the vendor have the ability to review documentation from a remote location (vendors offices)? Can the State provide the documentation electronically?

Response: **ITS will not allow source code to be reviewed offsite. ITS will develop procedures for providing the awarded vendor with access to the source code documentation.**

Question 16: Pricing Tables – Section 7 Technical/Functional Requirements list 20 requirements 7.1 to 7.20. Pricing Tables 1 and 3 (starting on page 58) request pricing on a subset of the Technical/Functional Requirements (Table 1 sixteen requirements and Table 3 five requirements). Can the State clarify how they would like to receive pricing? Should we provide line item pricing for Technical/Functional Requirements 7.1 to 7.20 in Table 1 and 3?

Response: **Responses in Section VIII, Cost Information Submission, should be a fixed cost on items where the service can be provided on a “per instance” basis. An hourly rate should be provided for services that cannot be priced on a “per instance” basis.**

Question 17: How many physical sites do you have?

Response: **See the response to question #3 above.**

Question 18: What is the address of the location(s)?

Response: **See the response to question #3 above.**

Question 19: If more than one site, will Awardee need to travel to identified remote sites?

Response: **Travel costs should be reflected in the vendor’s response. Since individual assessments might require travel, it should be incorporated into all of the pricing submitted except the Base Rates in Table 4 of Section VIII, Cost Information Submission.**

Question 20: Brief description of your organization’s Mission or Business Operations:

Response: **The Mississippi Department of Information Technology Services provides statewide leadership and services that facilitate cost-effective information processing and telecommunication solutions for agencies and institutions.**

Question 21: Are there any regulations or legislation that governs your business operations from a security or privacy perspective? (please list)

Response: **State agencies (including ITS) are subject to the State of MS Enterprise Security Policy. Also, state agencies are subject to various laws and regulations depending on the type of data each entity stores and processes. These laws and regulations include but are not limited to: IRS 1075, CJIS, HIPAA, PCI/DSS, FERPA, The Privacy Act, CIPA, FISMA, Social Security Administration, etc.**

The size and scope of each engagement will determine which laws and regulations may be applicable.

Question 22: Who will be the Primary point of contact (POC) at your organization for this work?

- a. Name:
- b. Phone:
- c. Cell:
- d. Email:
- e. Job Title

Response: For security assessments performed on the ITS IT infrastructure, a team member from the ITS Information Security Division will be the POC. This information will be provided prior to each engagement.

For contracts with other state agencies, each individual agency will designate a POC.

Question 23: Approximately how many total active users are there?

Response: ITS has approximately 150 employees.

For contracts with other state agencies, the total active users will vary.

Question 24: Are there any known operational limitations Awardee needs to be aware of? (i.e., shift work, batch processing, etc.)

Response: The operational limitations will depend on the size and scope of each assessment; however, the awarded vendor and ITS will work together to identify operational limitations for each engagement.

For contracts with other state agencies, operational limitations will vary.

Question 25: Do you have a date the work must be started by/completed by?

Response: There are no specific dates. See amendments #1 and #2 above.

Question 26: Are you looking for a Fixed Price proposal/quote or Time and Materials?

Response: A fixed cost should be proposed for services that can be provided on a “per instance” basis. An hourly rate should be provided for services that cannot be priced on a “per instance” basis as reflected in the tables.

Question 27: Please provide a description of the work you want accomplished, what your expectations are for the work, and the deliverables you wish to receive during and at the end of the effort.

Response: See Section VII, Item 6 for an overview of the work, Item 7 for the actual work, and Item 9.4 of the RFP No. 3735 for deliverables.

Question 28: Do you wish to have an organizational vulnerability analysis accomplished as part of the work? (These are related to vulnerabilities that result from policy, procedures, organizational structure, etc.) This work is generally based on the NSA INFOSEC Assessment Methodology (IAM).

Response: **Desired assessments have been included in Section VII, Item 7 of the RFP. The Vendor is not precluded from offering services as options that were not included in the RFP. Also, see Section VII, Item 4.7 of the RFP.**

Question 29: Do you have documented Security Policies and Procedures? Please list those that you know exist: (disaster recovery, overall security policy, etc.)

Response: **See Section IV, Item 32 and Section VII, Items 7.19, 7.20 and 9.3 of RFP No. 3735.**

Question 30: Is an organization chart available for Awardee review?

Response: **Information of ITS organizational structure can be found at the following links:**
http://www.its.ms.gov/Publications/Documents/ITS_services_catalog.pdf
http://www.its.ms.gov/Documents/annual_report.pdf

Question 31: Will network discovery need to be conducted to see what systems exist within the environment?

Response: **Vendor is asked to provide the requirements outlined in Section VII of the RFP, particularly Items 7.6.2.2 and 7.17. Vendor is not precluded from offering services as options that were not included in the RFP. Also, see Section VII, Item 4.7 of the RFP.**

Question 32: Has any previous assessments been conducted and are the results available for review if Awardee is selected to support your defined work?

Response: **Previous assessments have been performed on the ITS IT infrastructure. Depending on the size and scope of the specific engagement, ITS may be willing to provide some information.**

For contracts with other state agencies, access to previous assessment information will vary.

Question 33: Has critical information been identified in your environment and is this information available for review if Awardee is selected to support your defined work?

Response: **ITS will provide information as needed dependent on the size and scope of each engagement.**

For contracts with other state agencies, access to critical information will vary.

Question 34: Has any criticality analysis been accomplished to determine the impact of critical information related to confidentiality, integrity, and/or availability? Is it documented and available for Awardee review?

Response: **This has not been done for ITS systems.**

Question 35: Do you wish to have a technical vulnerability analysis accomplished as part of the work? (these are vulnerabilities associated with technical configurations, system patches, network architecture, firewalls, etc) This work is generally based on the NSA INFOSEC Evaluation Methodology (IEM).

Response: **See the requirement in Section VII, Item 7.4 of the RFP.**

Question 36: Are you utilizing a domain architecture?

Response: **Yes.**

Question 37: Are you utilizing a Windows Active Directory based architecture?

Response: **Yes.**

Question 38: Do you have wireless networking?

Response: **Yes.**

Question 39: What brand and configuration?

Response: **This information will not be provided prior to award. See Item 4.9.3 in amendment #1 above.**

Question 40: What Networking Protocols are you running? (TCP/IP, etc.)

Response: **The scope of this project could include several networking protocols. See amendments #1 and #2 above.**

Question 41: Are you utilizing any IPv6?

Response: **IPv6 is not in use at this time; however, IPv6 may be used within the ITS network prior to the end of the awarded contract.**

Question 42: How many internal IP addresses are to be evaluated, total?

Response: **ITS has approximately 2,000 internal IP addresses; however, the total number of IP addresses evaluated will be determined on an individual project basis. See amendments #1 and #2 above.**

Question 43: How many internal IP addresses at each site (if applicable)?

Response: **See the response to question #42 above.**

Question 44: How many external IP addresses are to be evaluated, total?

Response: ITS has approximately 40 external IP addresses; however, the total number of IP addresses evaluated will be determined on an individual project basis. See amendments #1 and #2 above.

Question 45: How many external IP addresses are to be assessed at each site (if applicable)?

Response: See the response to Question #44 above.

Question 46: Do you have a firewall(s)?
a. How Many?
b. What Kind?

Response: This information will not be provided prior to award. See Item 4.9.3 in amendment #1 above.

Question 47: Do you have intrusion detection/prevention in your environment (IDS/IPS)?
a. How many network based IDS/IPS? How many host-Based IDS/IPS?
b. What Kind?

Response: This information will not be provided prior to award. See Item 4.9.3 in amendment #1 above.

Question 48: How many servers at each site?

Response: See the response to question #42 above.

Question 49: What operating systems are on the servers?

Response: The scope of this project could include several types of operating systems. See amendments #1 and #2 above.

Question 50: What services are running on the servers? (Web, DNS, etc.)

Response: The scope of this project could include several types of services running on servers. See amendments #1 and #2 above.

Question 51: How many web servers are active and accessible to the public?

Response: See the response to question #44 above.

Question 52: What type of web servers (Apache, IIS)?

Response: The scope of this project could include several types of web servers. See amendments #1 and #2 above.

Question 53: How many web servers are active and for internal use only?

Response: See the response to questions #42 above.

- Question 54:** What type of web servers (Apache, IIS)?
- Response:** **The scope of this project could include several types of web servers. See amendments #1 and #2 above.**
- Question 55:** How many workstations at each site?
- Response:** **ITS has approximately 150 workstations; however, the total number of IP addresses evaluated will be determined on an individual project basis. See amendments #1 and #2 above.**
- Question 56:** What operating systems are on the workstations?
- Response:** **This information will not be provided prior to award. See Item 4.9.3 in amendment #1 above.**
- Question 57:** Do you have mainframe environments?
- Response:** **See the response to question #6 above.**
- Question 58:** If so, how many and what types of mainframes?
- Response:** **See the response to questions #6 above.**
- Question 59:** Do you currently utilize a RAS server for external access? If so, what product?
- Response:** **ITS does not currently utilize a RAS server.**
- Question 60:** Do you currently utilize a remote VPN product for external access (i.e. Altiga VPN concentrator)? If so, what product?
- Response:** **Yes. Specific product information will not be provided. See item 4.9.3 in amendment #1 above.**
- Question 61:** Are you using Voice over IP (VoIP) or IP telephony? How many stations?
- Response:** **Yes. The number of stations will not be provided prior to award.**
- Question 62:** Will you require “war-dialing” at any/all sites to detect rogue modems? If so, what sites?
- Response:** **No.**
- Question 63:** Do you require any tests on Denial of Service (DOS) vulnerabilities?
- Response:** **Depending on the scope of a particular engagement, DOS testing may be required. See Amendments #1 and #2 above.**
- Question 64:** Is there anything else about your technical environment that you believe we should be aware of?

Response: **ITS is not aware of anything else. See Section VII, Item 4.7 of the RFP.**

Question 65: Are there existing standards (Router, Switch, FW hardware, software, & IOS standards), baseline definitions, or SLAs defined that we need to use as benchmarks as part of the network performance assessment?

Response: **Yes.**

Question 66: Are there any compliance law requirements that must be taken into consideration when performing the network assessment as it relates to any network security requirements (e.g., HIPAA, PCI DSS v2, FERPA, etc.)?

Response: **See the response to question #21 above.**

Question 67: Is the network (Layer 2 / Layer 3) a multi-vendor or a single vendor network (e.g., all Cisco)?

Response: **This information is not being provided prior to award. See amendments #1 and #2 above.**

Question 68: Does the network infrastructure have the ability to enable flow data (i.e., Netflow, Jflow, Sflow)?

Response: **This information will not be provided prior to award. See Item 4.9.3 in amendment #1 above.**

Question 69: Does all deployed hardware & software that is within the scope of the assessment have active support?

Response: **There is no guarantee that all hardware & software have active support.**

Question 70: Are there any known equipment that are End of Life or End of Support?

Response: **ITS may have some devices that are at the End of Life or End of Support.**

Question 71: Are there other security devices/solutions currently employ other than Firewall, VPN concentrator or IPS (Proxy, DLP, SIEM, cloud based etc.) and from what vendor?

Response: **This information will not be provided prior to award. See Item 4.9.3 in amendment #1 above.**

Question 72: Who is your ISP?

Response: **AT&T is the ISP.**

Question 73: How many ISP Circuits are there?

Response: **There are two circuits.**

Question 74: Is there 3rd Party Connectivity? How many?

Response: This information will not be provided prior to award. See Item 4.9.3 in amendment #1 above.

Question 75: Is there a provider-managed or internally managed MPLS?

Response: Yes.

Question 76: What is the IGP / internal routing protocol currently in use?

Response: This information will not be provided prior to award. See Item 4.9.3 in amendment #1 above.

Question 77: What Layer 2 and Layer 3 protocols are in use?

Response: This information will not be provided prior to award. See Item 4.9.3 in amendment #1 above.

Question 78: Is Layer 2 security-enabled or in use (802.1x, mac, radius, etc.)?

Response: This information will not be provided prior to award. See Item 4.9.3 in amendment #1 above.

Question 79: Is the network currently capturing / sniffing and storing traffic from the network (Network Tap, Switches or full packet capture appliance)?

Response: This is not currently being done at ITS.

Question 80: Are we allowed to bring in our own tools, and apps to perform network performance data collection and analysis?

Response: ITS may consider allowing Vendor tools to be used prior to each assessment engagement. For contracts with other state agencies, this answer will vary.

Question 81: Are there out of band connectivity to the devices?

Response: This information will not be provided prior to award. See Item 4.9.3 in amendment #1 above.

Question 82: How are the devices currently accessed / managed in band?

Response: This information will not be provided prior to award. See Item 4.9.3 in amendment #1 above.

Question 83: Is there a centralized network management software deployed and in use?

Response: Yes for ITS. This may vary with other agencies.

Question 84: Is there a centralized authentication server AAA/TACACS server to provide global access to the devices?

Response: **No. For contracts with other state agencies, this answer will vary.**

Question 85: Do you have all configuration files centrally located for review and assessment?

Response: **No. For contracts with other state agencies, this answer will vary.**

Question 86: Is SNMP currently enabled throughout the network?

Response: **Yes for ITS network devices. This varies for other ITS devices and other agencies' devices.**

Question 87: Can we enable SNMP during the assessment?

Response: **This will be dependent on the assessment, since ITS plans to perform multiple security assessments on the ITS IT infrastructure per year.**

Question 88: Are there any devices you do not have access / credentials to that will be part of the assessment?

Response: **No.**

Question 89: Will there be a configuration freeze during the assessment (non-assessment related configurations)?

Response: **There will not be a configuration freeze for ITS. This may vary with other state agencies.**

Question 90: Is there a specific outage or maintenance window during which we can make changes to the network?

Response: **There will not be specific outage or maintenance windows for ITS. This may vary for other state agencies.**

Question 91: Can we make changes to the network infrastructure to enable certain monitoring capabilities during the assessment (Syslog, Mirroring / Spanning, Flow, etc.)?

Response: **This will be dependent on the assessment, since ITS plans to perform multiple security assessments on the ITS IT infrastructure per year.**

Question 92: Will historical information from the Change Control Board (If one exists) be available for review?

Response: **This information will not be available for ITS. This may vary with other state agencies.**

Question 93: Is there an accurate IT asset and inventory documentation?

Response: Prior to each ITS assessment, ITS will provide the most accurate inventory documentations needed depending on the scope of the assessments. For contracts with other state agencies, this answer will vary.

Question 94: Is there an accurate IP addressing documentation or IP Address Management / IPAM solution?

Response: This is available for ITS. This may or may not be available for other state agencies.

Question 95: Is the contract from this RFP intended to be on an "as needed" basis or is there a particular project or immediate need? (Section VII, 2)

Response: The answer is yes to both questions. See amendment #1 and #2.

Question 96: For proof of certification, is a copy of certificate required or may we provide just the certification number? (Section VII, 5.3.3)

Response: It is preferred that a copy be included with the response.

Question 97: Does the password strength assessment include the entire environment, i.e. application password and router passwords? (Section VII, 7.15)

Response: Yes.

Question 98: The RFP states that the Contractor shall deliver such documents and work papers to Customer upon termination or completion of the Purchase Order. Is it the intent that all working documents shall be sent to the State?

Response: Yes, except as outlined in items (a), (b), and (c) of Article 33, Ownership of Documents and Work Products, in Appendix B, Standard Contract of the RFP.

Question 99: Is there a vendor currently doing this work?

Response: Pileum Corporation has provided similar services to ITS in the past.

Question 100: Will there be a complete inventory of infrastructure equipment with vendor name, make, model, corresponding operating systems and specifications made available to the bidders for scoping purposes?

Response: ITS will make the appropriate information available to the Awarded Vendor. This may vary with other state agencies.

Question 101: Will there be a complete inventory of current vulnerability management and penetration testing tools in use today made available to the bidders for scoping purposes?

Response: ITS will make every effort to provide the appropriate information for an assessment. This may vary with other state agencies.

Question 102: Does the State of Mississippi require the bidders to use a specific set of vulnerability management and penetration testing tools?

Response: **No. The requirements in Section VII, Item 7.18 of the RFP do not require the Vendor to use specific set of tools.**

Question 103: Does the State of Mississippi prefer the bidders to use a specific set of vulnerability management and penetration testing tools?

Response: **This is at the Vendor's discretion.**

Question 104: Is the State of Mississippi asking the bidders to recommend a specific set of vulnerability management and penetration testing tools?

Response: **See the response to question #102 above.**

Question 105: Section VII, Technical Specifications, Item 2, General Overview and Background, Page 31 - Can you clarify whether all State Agencies will be able to purchase off of this RFP, or just a subset of those (i.e., those that are collocated in the ITS datacenter)?

Response: **This RFP is for ITS' use, but ITS reserves the right to use for any state entity desiring these services. See Section III, Vendor Information, Item 10.**

Question 106: Section VII, Technical Specifications, Item 6.2, Page 36 - Typically we scan with two of our in-house business class vulnerability scanners. Would we be allowed to use our own scanning tools, or only the scanning tools already in place and owned by ITS? If we had our own copy of BeyondTrust Retina, would it be acceptable to scan with this from one of our machines, and provide the scan output files to the State?

Response: **No, this is not acceptable for ITS. ITS may consider allowing the Vendor to use other tools, but only in additional to the ITS tool. This may vary for other state agencies.**

Question 107: Section 6.1.7 – Does the state maintain, in a single location/document/process, all known and/or accepted vulnerabilities that would need to be excluded from the results of the testing?

Response: **ITS will provide documentation about accepted vulnerabilities for ITS systems prior to each engagement. For contracts with other state agencies, this answer will vary.**

Question 108: Section 6.2 – Is the vendor allowed to run their own internal/external vulnerability scanning tools, or will we be limited to data provided from the existing vulnerability scanning solution (currently BeyondTrust Retina)?

Response: **See the response to question #106 above.**

Question 109: Section 7.16 - Will these be services be scoped individually with statements of work issued on a per-engagement basis?

Response: Yes.

Question 110: Section 7.16 – Can you describe an average application for testing? Specifically, number of user roles, number of forms, and approximate field count.

Response: No. See amendments # 1 and #2 above.

Question 111: Section 7.16 – Is there a desire for application black-box testing (aka Dynamic Application Security Testing) in addition to static source code review?

Response: Dynamic Application Security Testing is an option that should be included in the RFP response. The Vendor is not precluded from offering services as options that were not included in the RFP. Also, see Section VII, Item 4.7 of the RFP.

Question 112: Section 7.16 – What are the most common applications that will be in scope?

Response: See amendment #1 above.

Question 113: Section 7.16 – Since source code reviews would rarely be allowed to occur off-site, can you provide the location of where the services would be delivered from?

Response: ITS has two primary locations which include the ITS State Data Center (3771 Eastwood Drive, Jackson, MS) and the Robert E. Lee Building (239 North Lamar Street, Jackson, MS). For contracts with other state agencies, this answer will vary.

Question 114: Section 7.18 – How many internal and external penetration tests would be in scope?

Response: See amendments #1 and #2 above.

Question 115: Section 7.18 - Can you provide technical details of a typical internal and external network for penetration testing purposes? (Network space being key here – ie: external class C 50% full and internal network has 8 class C networks 40% full).

Response: This information will not be provided prior to award. See Item 4.9.3 in amendment #1 above.

Question 116: Section 9.1 – How many projects are anticipated to be awarded under this RFP? Will each of these projects be scoped out and price quotes delivered at the time of award?

Response: Throughout the life of this contract, ITS plans to perform multiple security assessments on the ITS IT infrastructure per year. No, this will not be

scoped out at time of award. The project schedule, size and scope of each assessment will vary. The Awarded Vendor and ITS will work together to determine the project timeframe, size and scope of each engagement. Price quotes will be delivered at this time. For contracts with other state agencies, this answer will vary. See Amendments #1 and #2 above.

Question 117: Section 11 – The State is requesting fixed pricing for all services. Given that each assessment will differ and that these differences will have an impact on level of effort and associated price, what kind of information will the state provide to vendors to arrive at per-instance fixed pricing for the services requested?

Response: The Vendor should price the per instance cost based on the work that is required for each instance as outlined in Section VII, Item 7 of the RFP for each service.

Question 118: What type of VPN Concentrators are in scope?

Response: See the response to amendment #1 above.

Question 119: What type of Databases are implemented and in scope?

Response: See the response to question #12 above.

Question 120: Table 1, page 58. Is the Estimated Hours to Complete column intended to state how long it would take to complete 1 item under Functional/Expertise/Service (e.g., Estimated Hours to Complete a Windows System Review of 1 Windows server, or Per Instance Estimate of Hours)?

Response: Yes.

Question 121: What is the average firewall rule-set size and the typical make/model of firewall in scope?

Response: This information will not be provided prior to award. See Item 4.9.3 in amendment #1 above.

Question 122: For Policy Review, on average:
a. How many Resources in IT?
b. How many Resources in Security?
c. How many Security Policies?
d. How many SOPs and Procedures?

Response: The number can vary. Vendor may consider pricing based on factors other than number, such as length or components to review in each policy.

RFP responses are due August 19, 2014, 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 Debra Spell at 601-432-8132 or by email at debra.spell@its.ms.gov.

cc: ITS Project File Number 40561