



Addendum #2
Date: March 10, 2014

City of Memphis Network Penetration Services

RFQ # SAIC CoM 2014 RG R85393

Issue Date: January 31, 2014

Original Response Date: February 21, 2014

New Response Date: March 21, 2014

This addendum has been issued to replace the previous answer sheet in its entirety. Answers to questions 7, 11, 14, 15, 16, 20, 21, 27a & 31 have been revised.

Note: All other terms and conditions remain the same.

City of Memphis Network Penetration Services
RFQ # SAIC CoM 2014 RG R85393
Response Accepted At: ATTN: SAIC Procurement
c/o City of Memphis, ITS
5125 Elmore Road, Ste. 6
Memphis, TN 38134

E-Mail Inquiries and Responses Accepted At: City_of_Memphis_Bids@saic.com

**City of Memphis
Network Penetration Services
RFQ # SAIC CoM 2014 RG R85393
Answers to Questions**

	<u>RFQ Section</u>	QUESTION	Response
1.		<p>On page 8, it indicates this is a government contract and we are required to comply with the FAR. However, there seems to be conflicting statements below this section which wouldn't require respondents to comply with FAR?</p> <p>Can you confirm if this is listed as a commercial request or a government request - which would require FAR's?</p>	Government. The FAR regulations are not applicable to this RFQ.
2.		What are the primary drivers to have this engagement completed	Network security testing.
3.		<p>How many External Hosts and IP addresses will be included in this engagement? If actual numbers have not been collected, approximations are sufficient.</p> <p>·External Hosts and IP Space –</p>	Approximately 125 hosts/IP's.
4.		Ideally, what time of day will this testing occur?	Testing will occur after business hours (Mon. – Fri.).
5.		Will on-site testing be required for any component of this testing?	Yes.
6.		<p>For the City of Memphis' external facing website, please describe the size and complexity of this application. Information typically provided includes, but is not limited to:</p> <ul style="list-style-type: none"> · Number of Total Pages: · Number of Dynamic Pages: · Critical Functions: 	<p>797</p> <p>20</p> <p>Citizen information and payments.</p>

**City of Memphis
Network Penetration Services
RFQ # SAIC CoM 2014 RG R85393
Answers to Questions**

	<u>RFQ Section</u>	QUESTION	Response
7.		<p>For the internal penetration test (option year 2):</p> <p>How many Internal Hosts and IP addresses will be included in this engagement? If actual numbers have not been collected, approximations are sufficient.</p> <ul style="list-style-type: none"> · Internal Hosts and IP Space – 	Approximately 5000.
8.		How many locations are included for this testing?	130+
9.		Will on-site testing be required for any components of this engagement?	Please see the response to question #5.
10.		<p>Are there any web applications in scope for this engagement? If so, please provide the following information for all in scope applications:</p> <ul style="list-style-type: none"> · Please describe the application and its' functionality. · Which environment does the application site in: internal, external, or both? · Please describe the application architecture: <ul style="list-style-type: none"> i. Front-end: ii. Business iii. Back-end: 	Yes. All 40+ applications that are used to support the City of Memphis.
11.		If authenticated testing is in scope for any application, please list the application and the roles to be tested.	48 Applications.

**City of Memphis
Network Penetration Services
RFQ # SAIC CoM 2014 RG R85393
Answers to Questions**

	<u>RFQ Section</u>	QUESTION	Response
12.		<p>Please describe the size and complexity of this application. Information typically provided includes, but is not limited to:</p> <ul style="list-style-type: none"> i. Number of Total Pages: ii. Number of Dynamic Pages: iii. Critical Functions: 	Please see the response to question #6.
13.		In which of these environments will testing occur: Production, Development, QA, other (please state).	All.
14.		How large is the internet point of presence?	For security reasons we will not provide the information at this time.
15.		What applications does the City have in place?	Please see response to question #14.
16.		Can you provide more details on the internal assessment and what the City wants covered in the assessment?	Please see response to question #14.
17.		Is there an incumbent and if so, can they bid on this project?	No.
18.		What is the business driver of the assessment?	Please see the response to question #2
19.		Is there a certain compliance mandate driving the assessment?	No.
20.		<p>Is this testing focused on the external perimeter, internal network, or both?</p> <ul style="list-style-type: none"> a. The scope/requirements on page 9 of the RFP specify external testing only, but other sections of the RFP mention internal testing (Page 10 - Period of Performance, Page 11 – Cost) 	Both.
21.		How many external hosts are estimated to be in scope?	Approximately 125.
22.		How many internal hosts are estimated to be in scope, if applicable?	Please see the response to question # 22.

**City of Memphis
Network Penetration Services
RFQ # SAIC CoM 2014 RG R85393
Answers to Questions**

	<u>RFQ Section</u>	QUESTION	Response
23.		<p>Does the customer own the hardware, network, and all assets associated with the in scope assets?</p> <p>a. Many websites and other hosts are hosted in outsourced environments. This will require signoff of a CBI signoff waiver from the associated outsourced parties.</p>	<p>Yes – 99%.</p> <p>There are hosted items like hosted items like the new Golf Solution and 1010.</p>
24.		<p>Is Social engineering in scope?</p> <p>a. If so, our general recommendation is to sample the environment with up to 25-50 targets. A Rules of Engagement meeting will be conducted to ensure the utmost caution and diligence is conducted during these tests.</p>	<p>No.</p>
25.		<p>Is Web Application Assessment testing in scope? If so, how many web applications are estimated to be in scope?</p> <p>a. Does the in scope web applications to be assessed require authentication?</p> <p>b. If so, will the City of Memphis be able to provide associated testing credentials?</p> <p>c. If so, does the application/s require any two factor authentication mechanisms?</p> <p>d. Is there an available development or testing area for the associated in scope web application/s?</p>	<p>Please see the response to question #10.</p>
26.		<p>The scope is defined as City of Memphis’s Internet points of presence including agency networks, assets, and applications and the requirements state this will be a “no previous knowledge” penetration test, with that in mind can you elaborate on the following questions:</p> <p>a. The City of Memphis will not be providing a network scope or address space to target and the winning contractor will be required to identify these targets in the reconnaissance phase of the test. Is this correct?</p> <p>b. Can you provide the anticipated size of the address space that will be assessed in this external penetration test? Such as 100 live IPs or 4 Class C networks.</p>	<p>No.</p>

**City of Memphis
Network Penetration Services
RFQ # SAIC CoM 2014 RG R85393
Answers to Questions**

	<u>RFQ Section</u>	QUESTION	Response
27.		<p>The scope includes the City's external facing website, are there any other websites that will require a web application assessment?</p> <p>a. Will all web application assessments be performed as an unauthenticated attacker or will user authenticated level account testing be required as well? If so can you tell us how many different account levels and how many web applications will require this?</p>	<p>No</p> <p>a.48 applications 1 authentication level for web access and 1 for data base connectivity</p>
28.		<p>Will Social Engineering be allowed or in scope during the external penetration testing phase?</p>	<p>Please see the response to question #24</p>
29.		<p>Are wireless networks in scope for the external penetration test and if so can you disclose how many locations and how many wireless networks will need to be assessed?</p>	<p>No</p>
30.		<p>The period of performance and cost sections reference both internal and external penetration testing exercises, but no information is provided regarding the scope of the internal penetration testing exercise. Will information be shared with regards to the internal penetration test assessment and if so when?</p>	<p>Here are the recommended areas to be tested:</p> <ul style="list-style-type: none"> Internal Network Scanning Port Scanning System Fingerprinting Services Probing Exploit Research Manual Vulnerability Testing and Verification Manual Configuration Weakness Testing and Verification Limited Application Layer Testing Firewall and ACL Testing Administrator Privileges Escalation Testing Password Strength Testing Network Equipment Security Controls Testing Database Security Controls Testing Internal Network Scan for Known Trojans Third-Party/Vendor Security Configuration Testing Email
31.		<p>How many IPS addresses are to be included in the external testing?</p>	<p>Please see the response to question #21.</p>
32.		<p>Estimated number of systems on the internal network?</p>	<p>This information will not provided at this time.</p>

**City of Memphis
Network Penetration Services
RFQ # SAIC CoM 2014 RG R85393
Answers to Questions**

	<u>RFQ Section</u>	QUESTION	Response
33.		Is social engineering to be included in the scope of the external testing? This would include Email phishing or spear phishing to gain user credentials or phone based methods as well.	Please see the response to question #24
34.		Is social engineering to be included in the scope of the internal testing? This would include media drops and physical security access.	Please see the response to question #24
35.		Since testing is non-destructive in nature will we be able to test during regular business hours or will testing be required to be scheduled after normal working hours?	Please see the response to question #4.
36.		Should the external penetration testing scope include Web Application security testing or should the scope be limited to network and system level exploits?	Please see the response to question #30.
37.		Cost and Fees: Does the City of Memphis expect the fixed fee bid to include expenses (Hotel, meals, travel, etc.) or are you open to expense reimbursement?	All costs associated with this RFQ should be identified in your response.
38.	Section 4.1 item 4	Section 4.1 item 4 indicates that the EBO form should be completed and returned as content of the RFQ response. Section 4.4 and the EBO form indicated not a requirement. Please confirm if EBO form is to be completed.	The EBO forms are not applicable for this RFQ.

**City of Memphis
Network Penetration Services
RFQ # SAIC CoM 2014 RG R85393
Answers to Questions**

	<u>RFQ Section</u>	QUESTION	Response
1.		<p>On page 8, it indicates this is a government contract and we are required to comply with the FAR. However, there seems to be conflicting statements below this section which wouldn't require respondents to comply with FAR?</p> <p>Can you confirm if this is listed as a commercial request or a government request - which would require FAR's?</p>	Government. The FAR regulations are not applicable to this RFQ.
2.		What are the primary drivers to have this engagement completed	Network security testing
3.		<p>How many External Hosts and IP addresses will be included in this engagement? If actual numbers have not been collected, approximations are sufficient.</p> <p>·External Hosts and IP Space –</p>	Approximately 125 hosts/IP's
4.		Ideally, what time of day will this testing occur?	Testing will occur after business hours (Mon. – Fri.).
5.		Will on-site testing be required for any component of this testing?	Yes.
6.		<p>For the City of Memphis' external facing website, please describe the size and complexity of this application. Information typically provided includes, but is not limited to:</p> <ul style="list-style-type: none"> · Number of Total Pages: · Number of Dynamic Pages: · Critical Functions: 	<p>797</p> <p>20</p> <p>Citizen information and payments.</p>

**City of Memphis
Network Penetration Services
RFQ # SAIC CoM 2014 RG R85393
Answers to Questions**

	<u>RFQ Section</u>	QUESTION	Response
7.		<p>For the internal penetration test (option year 2):</p> <p>How many Internal Hosts and IP addresses will be included in this engagement? If actual numbers have not been collected, approximations are sufficient.</p> <ul style="list-style-type: none"> · Internal Hosts and IP Space – 	All.
8.		How many locations are included for this testing?	130+
9.		Will on-site testing be required for any components of this engagement?	See answer to #5.
10.		<p>Are there any web applications in scope for this engagement? If so, please provide the following information for all in scope applications:</p> <ul style="list-style-type: none"> · Please describe the application and its' functionality. · Which environment does the application site in: internal, external, or both? · Please describe the application architecture: <ul style="list-style-type: none"> i. Front-end: ii. Business iii. Back-end: 	Yes. All 40+ applications that are used to support the City of Memphis.
11.		If authenticated testing is in scope for any application, please list the application and the roles to be tested.	This information will not be provided at this time.

**City of Memphis
Network Penetration Services
RFQ # SAIC CoM 2014 RG R85393
Answers to Questions**

	<u>RFQ Section</u>	QUESTION	Response
12.		<p>Please describe the size and complexity of this application. Information typically provided includes, but is not limited to:</p> <ul style="list-style-type: none"> i. Number of Total Pages: ii. Number of Dynamic Pages: iii. Critical Functions: 	See answer to #6.
13.		In which of these environments will testing occur: Production, Development, QA, other (please state).	All.
14.		How large is the internet point of presence?	This information will not be provided at this time.
15.		What applications does the City have in place?	This information will not be provided at this time.
16.		Can you provide more details on the internal assessment and what the City wants covered in the assessment?	This information will not be provided at this time.
17.		Is there an incumbent and if so, can they bid on this project?	No.
18.		What is the business driver of the assessment?	See response to question #2
19.		Is there a certain compliance mandate driving the assessment?	No.
20.		<p>Is this testing focused on the external perimeter, internal network, or both?</p> <ul style="list-style-type: none"> a. The scope/requirements on page 9 of the RFP specify external testing only, but other sections of the RFP mention internal testing (Page 10 - Period of Performance, Page 11 – Cost) 	Both.
21.		How many external hosts are estimated to be in scope?	All.
22.		How many internal hosts are estimated to be in scope, if applicable?	All.

**City of Memphis
Network Penetration Services
RFQ # SAIC CoM 2014 RG R85393
Answers to Questions**

	<u>RFQ Section</u>	QUESTION	Response
23.		<p>Does the customer own the hardware, network, and all assets associated with the in scope assets?</p> <p>a. Many websites and other hosts are hosted in outsourced environments. This will require signoff of a CBI signoff waiver from the associated outsourced parties.</p>	Yes – 99%.
24.		<p>Is Social engineering in scope?</p> <p>a. If so, our general recommendation is to sample the environment with up to 25-50 targets. A Rules of Engagement meeting will be conducted to ensure the utmost caution and diligence is conducted during these tests.</p>	No
25.		<p>Is Web Application Assessment testing in scope? If so, how many web applications are estimated to be in scope?</p> <p>a. Does the in scope web applications to be assessed require authentication?</p> <p>b. If so, will the City of Memphis be able to provide associated testing credentials?</p> <p>c. If so, does the application/s require any two factor authentication mechanisms?</p> <p>d. Is there an available development or testing area for the associated in scope web application/s?</p>	See answer to #10.
26.		<p>The scope is defined as City of Memphis's Internet points of presence including agency networks, assets, and applications and the requirements state this will be a "no previous knowledge" penetration test, with that in mind can you elaborate on the following questions:</p> <p>a. The City of Memphis will not be providing a network scope or address space to target and the winning contractor will be required to identify these targets in the reconnaissance phase of the test. Is this correct?</p> <p>b. Can you provide the anticipated size of the address space that will be assessed in this external penetration test? Such as 100 live IPs or 4 Class C networks.</p>	No.

**City of Memphis
Network Penetration Services
RFQ # SAIC CoM 2014 RG R85393
Answers to Questions**

	<u>RFQ Section</u>	QUESTION	Response
27.		<p>The scope includes the City's external facing website, are there any other websites that will require a web application assessment?</p> <p>a. Will all web application assessments be performed as an unauthenticated attacker or will user authenticated level account testing be required as well? If so can you tell us how many different account levels and how many web applications will require this?</p>	No
28.		Will Social Engineering be allowed or in scope during the external penetration testing phase?	Please see the response to question #24
29.		Are wireless networks in scope for the external penetration test and if so can you disclose how many locations and how many wireless networks will need to be assessed?	No
30.		The period of performance and cost sections reference both internal and external penetration testing exercises, but no information is provided regarding the scope of the internal penetration testing exercise. Will information be shared with regards to the internal penetration test assessment and if so when?	<p>Here are the recommended areas to be tested:</p> <ul style="list-style-type: none"> Internal Network Scanning Port Scanning System Fingerprinting Services Probing Exploit Research Manual Vulnerability Testing and Verification Manual Configuration Weakness Testing and Verification Limited Application Layer Testing Firewall and ACL Testing Administrator Privileges Escalation Testing Password Strength Testing Network Equipment Security Controls Testing Database Security Controls Testing Internal Network Scan for Known Trojans Third-Party/Vendor Security Configuration Testing Email
31.		How many IPS addresses are to be included in the external testing?	All.
32.		Estimated number of systems on the internal network?	This information will not be provided at this time.

**City of Memphis
Network Penetration Services
RFQ # SAIC CoM 2014 RG R85393
Answers to Questions**

	<u>RFQ Section</u>	QUESTION	Response
33.		Is social engineering to be included in the scope of the external testing? This would include Email phishing or spear phishing to gain user credentials or phone based methods as well.	Please see the response to question #24
34.		Is social engineering to be included in the scope of the internal testing? This would include media drops and physical security access.	Please see the response to question #24
35.		Since testing is non-destructive in nature will we be able to test during regular business hours or will testing be required to be scheduled after normal working hours?	See answer to #4.
36.		Should the external penetration testing scope include Web Application security testing or should the scope be limited to network and system level exploits?	Please see the response to question #30.
37.		Cost and Fees: Does the City of Memphis expect the fixed fee bid to include expenses (Hotel, meals, travel, etc.) or are you open to expense reimbursement?	All costs associated with this RFQ should be identified in your response.
38.	Section 4.1 item 4	Section 4.1 item 4 indicates that the EBO form should be completed and returned as content of the RFQ response. Section 4.4 and the EBO form indicated not a requirement. Please confirm if EBO form is to be completed.	The EBO forms are not applicable for this RFQ.