CITY OF MEMPHIS

REQUEST FOR PROPOSAL

#52136

Security Penetration Testing

Addendum #2

Questions & Answers

Except to remove vendor names and addresses, questions are provided exactly as submitted.

#		Section	Question / Answer
1	Q	2.4 Requirements	Under General Requirements, the RFP lists examples of relevant industry Cyber Security Certifications for proposed team members. Would the City accept other relevant industry certifications, such as Certified Information Systems Security Professional (CISSP), in place of the examples listed?
1	A		YES.
2	Q	RFP Terms & Conditions Instructions to Proposers	On pages 24 and 26, the RFP indicates that "This procurement may be subject to the requirements of Ordinance No. 5114 which establishes a local preference for local businesses located within the City of Memphis. A copy of your current Memphis and Shelby County Tennessee Business Tax Receipt must accompany the proposal for consideration of this ordinance." And that "the successful proposer, whose principal business address is located within the limits of the city of Memphis, will be required to submit, along with the required insurance and other required documentation, a copy of (1) the tax-exempt ruling or determination letter from the Internal Revenue Services; or (2) its current Memphis and Shelby County Business Tax Receipt/License." Would the City consider awarding this contract to a business that is not located in Memphis or Shelby County?
2	A		YES.
3	Q	2.4.1 External Network Penetration Testing	How many Firewalls are in use?
3	A		2 in scope .
4	Q	2.4.1 External Network Penetration Testing	How many external internet domains are in use?
4	A		1 in scope.
5	Q	2.4.1 External Network	What is the minimum about of external IPs that are anticipated being tested?

		Penetration Testing	
5	A		Not more than 100.
6	Q	2.4.2 Web Application Penetration Test	How many web applications are in-scope for testing?
6	A		10.
7	Q	2.4.2 Web Application Penetration Test	How many are hosted internally vs by a 3rd party?
7	A		8 internally, 2 3rd Party.
8	Q	2.4.2 Web Application Penetration Test	Will the testing be performed via authenticated or unauthenticated means?
8	A		Unauthenticated.
9	Q	2.4.3 Network Security Assessment	Does the City use Microsoft Cloud / Azure for their Active Directory?
9	A		Yes.
10	Q	2.4.3 Network Security Assessment	How many total network segments are in place?
10	A		100 +.
11	Q	2.4.3 Network Security Assessment	How many active AD accounts are in use on the network?
11	A		8000+.
12	Q	2.4.3 Network Security Assessment	How many active devices are on the total network?
12	A		Selected Specific subnets totaling less than 5000 active devices will be provided.
13	Q	2.4.3 Network Security Assessment	How many wireless access points are in use?
13	A		More than 30 Access points but only four (4) unique SSIDs are in scope. The Unique SSIDs can be accessed from 2 Locations.

14	Q	2.4.4 Physical Security Assessment	How many locations are required to test?
14	A		5.
15	Q	2.4.4 Physical Security Assessment	How many attempts are expected for this test per location?
15	A		2.
16	Q	2.4.4 Physical Security Assessment	Are any methods considered “black listed” and should not be attempted?
16	A		Yes – Public Safety Officer Impersonation.
17	Q	2.4.5 Social Engineering	Vishing – how many calls are required?
17	A		10.
18	Q	2.4.5 Social Engineering	Pre Texting – How many calls are required?
18	A		10.
19	Q	3.4 Pricing	What is the budget set for this contract?
19	A		This information can not be disclosed at this stage.
20	Q	3.4 Pricing	Do you have a preference for how the pricing is presented? (per hour pricing/per service pricing/etc.)
20	A		NO.
21	Q	Section 2.4.2	How many applications are in scope?
21	A		See Response to Question 6.
22	Q	Section 2.4.2	If a traditional web application: • Are you looking for authenticated or non authenticated testing or both? • Number of unique user profiles in scope for testing • Number of dynamic/input pages accessible to authenticated users • Number of API endpoints in scope
22	A		• Unauthenticated testing for Web applications • N/A • N/A • 3
23	Q	Section 2.4.2	If a Single Page Application (SPA)

			• Number of unique user profiles in scope for testing • Number of unique routes handled by the SPA • How does the SPA keep state? Externally or Internally • Number of API endpoints in scope
23	A		N/A
24	Q	Section 2.4.3	Are you looking to "time box" both phases of the internal testing? If yes, how long for each phase?
24	A		Phases will not be “Timeboxed”.
25	Q	Section 2.4.3	Is Wireless in scope? • Number of SSIDs • Number of locations
25	A		See response to question 13.
26	Q	Section 2.4.3	Internal Applications: • How many applications are in scope? • Are you looking for authenticated or non authenticated testing or both? • Number of user profiles in scope • Number of dynamic/input pages accessible to authenticated users • Number of API endpoints in scope
26	A		• See response to question 6 • See response to question 8 • Details will be provided during execution • N/A • 3
27	Q	Section 2.4.5	Please clarify: Social Engineering tests done internally... or is this a standalone testing scenario?
27	A		Targets of Social Engineering will be internal City of Memphis staff.
28	Q	1.2 Objective	Is the City using the penetration testing to address any specific compliance requirements (e.g., PCI DSS, HIPAA, CMMC, etc.)?
28	A		No.
29	Q	2.4.2 Web Application Penetration Test	Does the City want unauthenticated (e.g., penetrate outside it to the web application), authenticated (e.g., test the internal security of the web application), or both?
29	A		See response to Question 8.
30	Q	2.4.2 Web Application Penetration Test	Approximately how many web applications are in-scope for testing?
30	A		See response to Question 6.

31	Q	2.4 Requirements	Under "General Requirements" on page 7, the RFP states the total testing window may only be 10 continuous business days. Is there an operational or business impact that is driving this, or perhaps based on timelines provided by previous penetration testing firms?
31	A		This was determined based on schedule of current and upcoming projects.
32	Q	2.4 Requirements	Page 7 of the RFP states that the assessment will be conducted in four independent phases, however, page 8 goes on to say that it will take place in five phases. Also, Is it expected that the deliverable (penetration testing report) will simply address each phase specifically, or that phase 1 will be conducted and completed before moving to phase 2 and so on. Can the City of Memphis clarify their intent?
32	A		Assessment, as stated on page 8, should be performed in 5 phases. Assessment can be performed concurrently. Deliverable should address each phase specifically. Pricing can be itemized by Phase and a total can be provided for the entire assessment.
33	Q	General Question	Are the request services being conducted to fulfill the requirement of a compliance framework, such as PCI-DSS?
33	A		Partly to fulfil NACHA, CJIS requirement.
34	Q	2.5 Reporting	Section 2.5, 3h of the RFP suggests segmentation testing should be performed to validate segmentation controls, but it was not mentioned anywhere else in the RFP. Is segmentation from every network segment, to every network segment, being requested? Or is the intent to test segmentation controls put into place to reduce PCI-DSS scope, thus segmentation testing only needs to be performed to validate the non-CDE networks are properly segmented from the CDE networks?
34	A		The Network Segmentation Validation is part of Section 2.4.3 in the RFP. That part of the assessment is to test security controls implemented by the City to prevent unauthorized access to restricted networks.
35	Q	2.4.5 Social Engineering	For social engineering, will the City of Memphis be providing the targets for the phishing/vishing/spearphishing/etc, or will the vendor be responsible for discovering this information on their own?
35	A		The City of Memphis will provide random targets if vendor is unable to perform discovery.
36	Q	2.4.4 Physical Security Assessment	For physical testing: ▪ How many locations? ▪ Are there armed guards? ▪ Will physical security assessment/on-site social engineering be conducted during or after business hours, or both?

			▪ What physical security controls have been implemented? ▪ What is the ultimate objective? (Are there specific things you would like us to try, specific areas you would like us to attempt to gain access, particular departments you would like us to focus on, etc.?) ▪ Are there any activities that are strictly prohibited?
36	A		• See response to question 14 • In some locations – Yes • Business hours • Cameras, Boulders, Security Personnel, Key Card Entry • Objective is to test the effectiveness of Physical Security Controls implemented by the City of Memphis – Details of locations will be provided after contract is awarded.
37	Q	2.4.2 Web Application Penetration Test	How many web applications will be tested, and what are the purposes of each application?
37	A		See Response to question 6. Purpose of application will be provided after contract is awarded.
38	Q	2.4.2 Web Application Penetration Test	Are the applications Commercial Off the Shelf (COTS), or custom coded by a third party, or custom coded in house?
38	A		There are COTS, custom and third party applications. Details will be provided after contract is awarded.
39	Q	2.4.2 Web Application Penetration Test	What software or coding languages are used?
39	A		See response to question 162.
40	Q	2.4.2 Web Application Penetration Test	How many unique dynamic pages (pages that change based on user inputs) for each application? (e.g., an e-commerce site that sells products may have hundreds of dynamic pages, but each dynamic page is the same underlying code) For scoping purposes, only provide the number of unique pages with dynamic content.
40	A		See response to question 47, 48.

41	Q	2.4.2 Web Application Penetration Test	Is authenticated testing being requested? Authenticated testing typically provides for more thorough testing, however often takes quite a bit more time. ▪ If authenticated testing is requested, how many and what types of user roles would be tested? (i.e. Three - user, manager, administrator)
41	A		See response to Question 8.
42	Q	Section 2.4	How many post remediation reviews do you anticipate and what is the expected timeline to complete the reviews?
42	A		Remediation steps should be provided in the Pentest report as stated in Section 2.5 of the RFP.
43	Q	Section 2.4	Are the five phases to take place over 10 business days? Can they run concurrently?
43	A		See response to question 32.
44	Q	Section 2.4.2	How many web applications are in scope?
44	A		See response to question 6.
45	Q	Section 2.4.2	Do they have authenticated users with roles? More than a basic user and admin?
45	A		See response to question 8.
46	Q	Section 2.4.2	Is testing the authenticated portion of the apps needed?
46	A		See response to question 8.
47	Q	Section 2.4.2	How many unique pages or "flows" make up the applications?
47	A		25.
48	Q	Section 2.4.2	Estimated number of input forms on the applications.
48	A		50.
49	Q	Section 2.4.3	How many locations are in scope for the network security assessment?
49	A		Assessment will be performed from a central location.
50	Q	Section 2.4.3	How many datacenters are in scope for the network security assessment?
50	A		1.
51	Q	Section 2.4.3	Are any cloud services in scope for the network security assessment?
51	A		No.
52	Q	Section 2.4.4	How many locations are in scope for the physical security assessment?
52	A		See Response to Question 14.

53	Q	Section 3	Can we submit as one document, including attachments?
53	A		YES.
54	Q		Is the City of Memphis using Z/OS Mainframe?
54	A		No.
55	Q		Which enterprise security manager do you use? RACF, ACF2 or Top Secret.
55	A		None of the Above.
56	Q		Since we could not verify the platform that the City of Memphis is using, may we please have an extension for the application submission date?
56	A		No.
57	Q	SOW	Approximately how many web application(s) will need to be pentested?
57	A		See response to question 6.
58	Q	SOW	Outside of the Physical Security Assessment and some social engineering attacks (i.e. usb key drops) can all the other phases be completed remotely?
58	A		Yes. Depending on Circumstances and Restriction levels at the time of contract award.
59	Q	SOW	Is the following mandatory or preferred as a timeline for execution? "Vendor shall specify the ability to perform and complete External, Internal, Web Application, Physical Security and Social Engineering tests within Ten (10) continuous business days."
59	A		Please refer to General Requirements section of the RFP posted.
60	Q	General	Under the "General Requirements" section it states, "City of Memphis Information Technology Security Assessment will be conducted in four independent phases (or City of Memphis can pick which phase is required) derived from known threats to City of Memphis." With this statement being said is the expectation that the 5 phases will be all conducted in one assessment or in phases?
60	A		See response to question 32.
61	Q	Pricing	For pricing should we price out each of the 5 phases requested as firm fixed price line items?
61	A		See response to question 32.
62	Q	1.1	Will you be willing to negotiate further terms and conditions after bid submission?
62	A		No.
63	Q	1.2	Is there a cybersecurity framework, like NIST CSF, that the City of Memphis has adopted as the foundation of its cybersecurity program?

63	A		The City of Memphis follows the NIST CSF.
64	Q	2.4.1	Please describe the current Internet architecture including any DMZ networks.
64	A		Will be provided after contract is awarded.
65	Q	2.4.1	Please provide details surrounding the City of Memphis's Internet points of presence.
65	A		Will be provided after contract is awarded.
66	Q	2.4.2	For Web Application Penetration Testing: • How many web applications are going to be included in the scope of testing? • Will both unauthenticated and authenticated testing be required in the scope of testing? • For each application in scope, please provide number of dynamic pages associated with each application.
66	A		• See response to question 6 • See response to question 8 • Between 25-50 per application
67	Q	2.4.3	For Network Security Assessment: • Are all 5000 IP addresses accessible from one network location (i.e., City of Memphis's central IT office)? • How are remote offices interconnected? • For remote-based testing, will the vendor be allowed to ship and connect one or more of our systems onto the internal City of Memphis network to perform the required testing?
67	A		• Yes (when specifically permitted) • The City's offices are primarily connected via dark fiber. Using OSPF for dynamic routing. • YES
68	Q	2.4.3	For Network Security Assessment, please clarify the scope of the "DMZ Network" testing: • Is the vendor expected to perform network segmentation testing as part of the scope? • If so, will this be limited to "DMZ network" to Internal network testing?
68	A		• Yes • Assessment will test Network security which includes security zones not limited to "DMZ network" to "Internal Network"
69	Q	2.4.3	For Network Security Assessment, please clarify the scope of the "wireless infrastructure" testing: • Please provide number of locations, number of floors, square footage of area to be tested. • Please estimate number of SSIDs.

69	A		See response to question 13.
70	Q	2.4.3	For Network Security Assessment, how many USB key drops should the vendor include as part of the scope?
70	A		5
71	Q	2.4.4	For Physical Security Assessment: • Please provide a count on the number of divisional offices/physical locations to be included in the scope of testing. • For physical access to the network jacks, does the City of Memphis implement any NAC solutions. • Please clarify or provide details regarding "restricted areas."
71	A		• See response to question 14 • Yes • Restricted Areas in this context are areas within the City of Memphis that require special access and/or protected by Law Enforcement.
72	Q	2.4.5	For Social Engineering, Phishing (general and targeted) • How many scenarios should the vendor include in the scope of testing? • How many employees does the City of Memphis want to test? • Are there any employees that the vendor is not to test? • Will the City of Memphis provide a target user list, or will vendor be expected to perform a discovery?
72	A		• 3 scenarios • 200 Random Targets • No • See response to question 35
73	Q	2.4.5	For Social Engineering, Pre-Texting • How many scenarios should the vendor include in the scope of testing? • Will the City of Memphis provide a target user list or will vendor be expected to perform a discovery?
73	A		See response to question 72.
74	Q	2.1	Are there specific regulatory compliance standards that the City of Memphis must comply/adhere to?
74	A		CJIS, PCI-DSS, NACHA, HIPAA, FISMA.
75	Q	2.2 & 2.4	For scheduling, the City of Memphis stated the following: "The proposed schedule should include planning for two tests annually, one external penetration test and one internal penetration test." However, in Section 2.4, the following is stated:

			"Vendor shall specify the ability to perform and complete External, Internal, Web Application, Physical Security and Social Engineering tests within Ten (10) continuous business days." • Could you please clarify if the external testing and internal testing will be conducting during two different time periods over the course of the year or is the request to perform all external and internal testing at the same time? • Is the intent to perform the entire scope (5 activities) twice a year? Or, to perform all of the external testing separately from all of the internal testing (so each activity is performed only once during the course of the year)?
75	A		• All 5 Phases of the assessment listed in Section 2.4, Pg 8 (which covers both internal and external testing) will be performed during the scheduled timeframe listed in the RFP • Penetration Testing engagement will be performed once a year unless otherwise determined.
76	Q	2.4.1 2.4.2 2.4.3 2.4.4 2.4.5	For all of the in-scope elements, will there be any time restrictions (testing windows) in terms of when testing can be performed, or will vendor be allowed to perform testing 24 hours a day?
76	A		2.4.1 – No time restrictions 2.4.2 – No time restrictions 2.4.3 - Business Hours 2.4.4 – Business Hours 2.4.5 - No time restrictions
77	Q	4.3	Will the City of Memphis consider an extension to allow for more time to respond to the RFP?
77	A		No.
78	Q	4.9, Exhibit 4	Are deviations or exceptions to the requirements in the City of Memphis Service Agreement Sample Contract incorporated in Exhibit 4 of the RFP permissible? If so, please clarify in which format the City would like to receive such exceptions.
78	A		To ensure all vendors submit proposals based on the same information, no changes to the contract template will be considered. Please prepare your proposal and cost accordingly.
79	Q	4.9, Exhibit 4 (sections regarding indemnification	As the terms and conditions are silent in regard to any limitation of respondent's liability or a damage cap with respect to respondent's indemnity obligations as set forth in the City of Memphis Service Agreement Sample Contract incorporated in Exhibit 4 of the RFP, are you willing to negotiate some limitation or damage cap of respondent's liability?

		obligations of contractor)	
79	A		To ensure all vendors submit proposals based on the same information, no changes to the contract template will be considered. Please prepare your proposal and cost accordingly.
80	Q	4.9, Exhibit 4	For clarification, will you consider respondent's standard master service agreement with the inclusion of applicable service schedules as a baseline for developing any contract between the parties?
80	A		To ensure all vendors submit proposals based on the same information, no changes to the contract template will be considered. Please prepare your proposal and cost accordingly.
81	Q	2.4.3	1. What software/service is currently being used for Vulnerability Management?
81	A		Nessus.
82	Q	2.4.3	2. What software/service is currently being used for network monitoring and management?
82	A		Extreme NMC.
83	Q	2.4.3	3. What software is being used for Endpoint detection and Response?
83	A		Crowdstrike EDR.
84	Q	2.4.3	4. Does the City utilize any cloud assets such as AWS, Azure or Google?
84	A		Cloud Assessment is out of scope.
85	Q	2.4.2	5. For each Web Application please answer the following:
			a. Is the application Multi-Tenant?
			b. Is there a REST API / AJAX
			c. If 'Yes' to REST API / AJAX, are there more than 20 methods?
			d. Is there a shopping cart / payments?
			e. Is there a login form?
			f. Does the app have customizable reporting?
			g. Does the app have a complex ecosystem?
			h. Is after hours work required?
85	A		N/A.
86	Q	2.4.5	6. Please confirm Social Engineering requirement
86	A		Confirmed.
87	Q	2.4.4	7. Are you looking for us to breach a particular physical location for you? If so, how many?

87	A		Physical security assessment is to test the security controls implemented by the city of Memphis. 5 locations are in scope.
88	Q	2.2	The RFP discusses scheduling 2 annual tests, an external and internal test. Section 2.4 Requirements discuss Web Application Testing, Physical Security Assessment and Social Engineering tests and re-tests of the Network Penetration Tests in addition to the Network Penetration Tests. Are there schedule requirements for these tests as well and if so, how many?
88	A		See response to question 75.
89	Q	2.4	Regarding Segmentation testing: a. What are the technical controls used to restrict access to/from the secured segment to/from non-secured segments in the organization (Ex. VLAN, Firewall, Access Control List (ACL), Air Gap, Other (specify))? b. Approximately, how many segments have access to the secured segment(s)? c. How many separate geographic locations have segments which can access the secured segment(s)? d. Is a network diagram available of the in-scope environment?
89	A		a. Firewall zoning, ACL b. Approximately 25 c. Approximately 15
90	Q	2.4.2	1. Regarding Web Application Testing a. How many applications are to be tested? b. For each application: i. What is the application name? ii. What is the primary function of the application? iii. What is the type of application (ex. Web/Browser-based, Mobile, Thick Client, API/Web Service, Other (specify))? iv. Is the application available over the Internet? v. What type(s) of authentication is required (ex. Password, One-time Token, Certificate, Other (specify))? vi. What is the total number and type of authorization levels in scope for this assessment (ex. Anonymous, Administrative, Workflow, Other (specify))? vii. Was the application purchased from a vendor, developed in-house, or the result of an outsourced development project? viii. What languages are used?

			ix. What is the development platform? x. Which application server or middleware is used? xi. What Database server is used? xii. What is the network transport utilized (ex. Raw, TCP/TLS, Other (specify))? xiii. If API/Web Services: 1. Approximately how many API/web service end points are there? 2. How many of these API/web service end points are publicly available (i.e.: published to the Internet)? 3. Are you requesting the direct testing of the stand-alone API/Web Services? 4. Are all API/Web Services executed by the user interface? 5. Approximately how many methods exist for each service? Because some API/web services support multiple operations with a single method, the total number of operations is required to scope. For example, if a single method can support add, modify and delete functionality - that would count as three operations. 6. How many URLs are required to access the application components? 7. Purpose of the API (ex. Basic, Application Functions, Administrative, Other (specify))? 8. What other technologies are involved in the web application's n-Tier architecture? xiv. If Native Mobile Applications: 1. What platforms (ex. Apple/iOS, Android, Blackberry, Other (specify))? 2. Does the application have a minimum platform version requirement? (i.e.: Android 4.4 KitKat, iOS 9 only, iOS 10 or above) 3. Approximately how many views are available in the application? 4. How many of those views take input from the user?

			5. Does the mobile application implement root/jailbreak detection? 6. Does the mobile application implement certificate pinning? xv. If Thick Client: 1. Approximately how many pages/screens accept user input? 2. On average, approximately how many user input fields are on each page? (Usually 10-20)
90	A		See response to question 6, 8, 66, 107, 161, 162, 163.
91	Q	2.4.5	1. Regarding Social Engineering: a. How many total users have access to the City's electronic resources? b. Typically, sampling of users is performed. This helps to keep the total costs of the exercise down and minimizes disruption to your workforce. If sampling is acceptable, please provide guidance on the number of users for each type of test (no more than a 20% sample size is recommended, 5% - 10% is typical): i. Phishing: ii. Vishing: iii. Spear Phishing: iv. Business Email Compromise: v. Whaling: vi. PreText: vii. USB Drop: c. For the physical social engineering, how many locations are in scope? d. For each physical location, what is the approximate size of the building in square feet?
91	A		a. Depends on function – details will be provided after contract is awarded b. Response i. See response to question 72 ii. See response to question 17 iii. 20 iv. Same number as Phishing v. 20 vi. See response to question 18 vii. See response to question 70 c. See response to question 14 d. N/A; not testing coverage.

<table>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td>92</td><td>Q</td><td>2.5</td><td>1. Section 2.5 Reporting requires the report to “Suggest best practices for device(s) and/or service configurations” based on the results of the penetration testing. Results will generally address specific vulnerability findings but lack the context of the function of the device to determine an overall configuration. If configuration reviews and recommendations are required, a count of the number of devices will be needed. If so, complete the table below:
<table>
<tr><th></th><th>Number of Devices</th><th>Make</th><th>Model</th></tr>
<tr><td>Firewalls</td><td></td><td></td><td></td></tr>
<tr><td>Routers</td><td></td><td></td><td></td></tr>
<tr><td>Switches</td><td></td><td></td><td></td></tr>
<tr><td>Windows Servers</td><td></td><td></td><td></td></tr>
<tr><td>Unix Servers</td><td></td><td></td><td></td></tr>
<tr><td>Windows Workstations</td><td></td><td></td><td></td></tr>
<tr><td>IDS/IPS</td><td></td><td></td><td></td></tr>
<tr><td>Other:</td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>92</td><td>A</td><td></td><td>Device configuration Reviews are out of scope.</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td>93</td><td>Q</td><td>2.4.1</td><td>Please provide the number of active external IP’s to be considered in-scope.</td></tr>
<tr><td>93</td><td>A</td><td></td><td>See response to question 5.</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td>94</td><td>Q</td><td>2.4.1</td><td>Please list any third parties that own systems or networks that are in-scope, as well as which systems they own. (Please note that permission must be obtained by the third-party prior to conducting any testing on these systems)</td></tr>
<tr><td>94</td><td>A</td><td></td><td>N/A.</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td>95</td><td>Q</td><td>2.4.3</td><td>Please provide the number of active internal IP’s to be considered in-scope.</td></tr>
<tr><td>95</td><td>A</td><td></td><td>See response to question 12.</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td>96</td><td>Q</td><td>2.4.3</td><td>Is The City of Memphis amenable to performing this testing remotely?</td></tr>
</table>

96	A		See response to question 58.
97	Q	2.4.3	If yes, would The City of Memphis be amenable to connecting a tester-owned laptop to the internal network that calls back via OpenVPN to a tester-owned server? The tester would interact remotely and use tools on the laptop (verses the limitations of testing through a VPN endpoint with no actual presence on the subnet).
97	A		If a remote method is agreed on, the City of Memphis will provide VPN solution for the Client.
98	Q	2.4.3	Please advise if all internal systems respond to Ping Echo requests.
98	A		Not all.
99	Q	2.4.2	Please provide the number of application(s) to be tested.
99	A		See response to question 6.
100	Q	2.4.2	Describe in your own words what functionality the application(s) provides end-users.
100	A		See response to question 141.
101	Q	2.4.2	Please provide any specific concerns/why is the application(s) being tested?
101	A		Security Risks, vulnerabilities, API exposures, Unauthorized access, application security.
102	Q	2.4.2	What type of data is the application(s) responsible for protecting (PII, PHI, PCI, etc.).
102	A		PII, PCI.
103	Q	2.4.2	Are any of the in-scope applications a custom-built application?
103	A		Yes.
104	Q	2.4.2	Do any of the applications in-scope utilize an application server such as JBoss, Websphere, WebLogic, etc?
104	A		No.
105	Q	2.4.2	Please list any other third-party products if they are utilized with the in-scope application(s), such as a Content Management System, Business Intelligence, etc.
105	A		N/A.
106	Q	2.4.2	Please advise if the live testing will be conducted on a production environment or if testing will be in a development/testing environment per application being tested.
106	A		Production Environment.

107	Q	2.4.2	Please provide, per application, what language the application is developed in.
107	A		Variety - PHP, .Net, JavaScript.
108	Q	2.4.2	Do any of the in-scope application(s) rely on client-side technologies such as ActiveX, Flash, Java, etc.?
108	A		No.
109	Q	2.4.2	Do any of the in-scope application (s) leverage frameworks such as AJAX, AngularJS, etc.?
109	A		No.
110	Q	2.4.2	Please provide how many different types of roles exist within each in-scope application such as standard user, client manager, administrative user, etc.
110	A		Standard, Administrative User.
111	Q	2.4.2	Please provide the number of user interface screens within the in-scope applicaition(s).
111	A		N/A.
112	Q	2.4.2	Do any of the in-scope application(s) interface with single sign-on (SSO) solutions?
112	A		No.
113	Q	2.4.2	If YES, please list all solutions:
113	A		N/A.
114	Q	2.4.2	If YES, are the single sign-on servers accessible from the internet, internally accessed only, or restricted access?
114	A		N/A.
115	Q	2.4.2	Do any of the in-scope application(s) use a thick client that talks to the application?
115	A		No.
116	Q	2.4.2	If YES, please advise if the thick-client will be in-scope and what language it is written in.
116	A		N/A.
117	Q	2.4.2	Please advise if there are any associated mobile applications.
117	A		No.
118	Q	2.4.2	If YES, should the listed associated mobile applications be considered in-scope?
118	A		N/A.

119	Q	2.4.2	If the listed associated mobile applications are in-scope, what platforms (iOS, Android) are the builds available for?
119	A		N/A.
120	Q	2.4.2	For the in-scope application(s), are there any system to system API's, such as SOAP, exposed by the application that will be in-scope?
120	A		Yes.
121	Q	2.4.2	If YES, how many distinct API's are there?
121	A		3.
122	Q	2.4.2	If YES, can you provide WSDL (API definition) files for scoping inspection?
122	A		Will be provided after contract is awarded.
123	Q	2.4.4	Please provide the number of locations that will be in-scope for physical penetration testing.
123	A		See response to question 14.
124	Q	2.4.4	Please list all location addresses to be tested.
124	A		Will be provided after contract is awarded.
125	Q	2.4.4	Please list a site description for all in-scope locations to be tested.
125	A		Will be provided after contract is awarded.
126	Q	2.4.4	Will Site Security Architecture be in-scope?
126	A		No.
127	Q	2.4.4	Will Physical Perimeter Access Control be in-scope?
127	A		No.
128	Q	2.4.4	Will Sensitive Area Access be in-scope?
128	A		Yes – Guidance will be provided regarding sensitive areas.
129	Q	2.4.4	Will Document Control be in-scope?
129	A		No.
130	Q	2.4.4	Will Network/Device Access be in-scope?
130	A		Yes.
131	Q	2.4.4	Will Internal Sensitive Information Handling be in-scope?
131	A		Yes.
132	Q	2.4.4	Will USB Device Drop be in-scope?
132	A		Yes.

133	Q	2.4.5	Please list the number of total users to be in-scope for Email Phishing Assessment.
133	A		See response to question 72.
134	Q	2.4.5	Will a Credential Landing Page associated with the phishing email be considered in-scope, to provide analysis on employees who have entered employee credentials?
134	A		Yes.
135	Q		Regarding project scheduling, RFP section 2.2 refers to two engagements, whereas RFP section 2.4 calls for four phases, and then five phases. Please confirm whether we should provide itemized pricing for each of the five phases, per RFP 2.4, or define how they should be broken up differently. Is the City looking for this engagement to be done as one or as separate engagements throughout the course of a year?
135	A		See response to question 32.
136	Q		Given this line of section 2.4 "*Vendor shall specify the ability to perform and complete External, Internal, Web Application, Physical Security and Social Engineering tests within Ten (10) continuous business days,*" should vendors plan to conduct all five phases within ten business days? Or are you asking whether we can perform <u>each</u> of the five phases within ten business days?
136	A		See response to question 32.
137	Q		RFP section 2.7 states: "*Upon the conclusion of all aforementioned information technology security assessment, Insert Location Here will be provided the following…".* Considering the potential of completing phases separately, should respondents' price for one set of reporting deliverables, or for the separate reporting deliverables for each phase?
137	A		See response to question 32.
138	Q		Should our response to RFP 52136 include a signed copy of the 4-page PFD titled "52136?"
138	A		NO.
139	Q		Could you please elaborate on the compliance objectives the City has for this project? Is this compliance to City's existing security policies, an established cybersecurity framework, or to local/state or federal regulation?
139	A		See response to question 63 and question 74.
140	Q	2.4.1 EXTERNAL NETWORK PENETRATION TEST	Will this pen test include on Prem and cloud environments that the City has?
140	A		Cloud Environment out of scope.

141	Q	2.4.2 WEB APPLICATION PENETRATION TEST	What types of web applications require pen testing and what are their main functions?
141	A		Variety – Fleet maintenance, payment systems, personnel management, primary website.
142	Q	2.4.3 NETWORK SECURITY ASSESSMENT	For the wireless testing, how many networks and how many locations are included?
142	A		See response to question 13.
143	Q	2.4.3 NETWORK SECURITY ASSESSMENT	For the wireless testing, and how many access points are included?
143	A		See response to question 13.
144	Q	2.4.3 NETWORK SECURITY ASSESSMENT	For the wireless testing, how many unique configurations exist among the access points?
144	A		See response to question 13.
145	Q	2.4.1 - External Network Penetration Assessment	The External Network penetration Assessment indicates 100 external IP addresses. How many of these targets are providing web based services (E.g. HTTP/HTTPS)?
145	A		90%.
146	Q	2.4.1-3 - All Assessment Sections	Are any of the in-scope information systems hosted by cloud service providers (i.e. Rackspace, Microsoft Azure, AWS, etc.) in-scope for the assessments? a. If applicable, please clarify the cloud services providers and the number of hosted systems?
146	A		No.
147	Q	2.4.3 - Network Security Assessment	How many internal wireless networks (SSIDs) will be in-scope for the Network Security Assessment?
147	A		See response to question 13.
148	Q	2.4.2 - Web Application Penetration Assessment	How many web-based applications are in scope for the web application penetration assessment?
148	A		See response to question 6.

149	Q	2.4.2 - Web Application Penetration Assessment	Will testing of all of the in-scope web applications require VPN access? Or are these applications externally accessible to the general public?
149	A		Some of the in-scope applications can only be accessed via VPN.
150	Q	2.4.2 - Web Application Penetration Assessment	Will the assessment team be provided with basic user credentials to perform authenticated web application penetration assessments, or will the web application penetration assessments be unauthenticated?
150	A		See response to question 8.
151	Q	2.4.4 - Physical Security Assessment	How many locations will be tested as part of the Physical Security Assessment?
151	A		See response to question 14 and 36.
152	Q	Social Engineering	How many District employees will be included within the security awareness phishing campaigns (Email)?
152	A		See response to question 72.
153	Q	2.4.3	Number of servers to be tested
153	A		20.
154	Q	2.4.3	Number of Microsoft Active Directories to be tested
154	A		2.
155	Q	2.4.3	Number of wireless physical locations to be tested? Approximate total travel time between locations (hours)?
155	A		See response to question 14 and 36. An approximate of 90minutes between locations.
156	Q	2.4.2	Can you provide the number application, URL and purpose of application?
156	A		See response to question 6 and 141. URL and purpose of application will be provided after contract is awarded.
157	Q	2.4.2	Is the Application avaiable for testing from the Internet ?
157	A		See response to question 149.
158	Q	2.4.2	Total number of pages per application?
158	A		See response to question 66.
159	Q	2.4.2	How many Applications store PHI, PII or other sensitive data
159	A		2.

160	Q	2.4.2	Is there a Web application firewall (WAF) in place
160	A		Yes.
161	Q	2.4.2	Are APIs/AJAX/Service calls being used and need to be tested? If so, how many?
161	A		3.
162	Q	2.4.2	What language(s) is it written in (e.g. .php, java, .Net, etc…)
162	A		Variety - .Net, php.
163	Q	2.4.2	What language is the back end database
163	A		MSSQL, OracleSQL, mariadb.
164	Q	2.4.5	Spear Phishing: How many different emails are to be sent?
164	A		See response to question 91.
165	Q	2.4.5	Spear Phising: How many email addresses/users are to be phished?
165	A		See response to question 91.
166	Q	3.4 Pricing	Please provide the Pricing Form, Exhibit 2, which was blank in the RFP document.
166	A		There is no standard pricing form, Vendor can provide their pricing an acceptable format.
167	Q	4.6 Proposal Submissions	What time are proposal submissions due on April 21, 2021?
167	A		12:00 pm/noon CT.
168	Q	2.4	Is there a defined budget for each of the 5 phases?
168	A		See response to question 32.
169	Q	2.4.2	How many web applications? Can you describe each and the user roles?
169	A		See response to question 141 and question 6.
170	Q		What type of databases?
170	A		See response to question 163.
171	Q		Is there a budget for each of the different engagements?
171	A		See response to question 19 and 32.
172	Q		How many locations are part of the physical test?
172	A		See response to question 14.
173	Q		Will we be testing vendor-owned systems as part of this engagement?
173	A		No.

174	Q		How many applications?
174	A		See response to question 6.
175	Q		How many locations for the physical security assessment?
175	A		See response to question 14.
176	Q		Are there any rules related to USB devices? Can they be mailed?
176	A		There are no specified rules. Yes.
177	Q		Do you have a current / preferred platform for any of the social engineering engagements? If so, would we be allowed to use your licensing?
177	A		We do have a current platform, but we prefer vendor to use their platform for the social engineering exercise .
178	Q	General	Considering the insurance coverage requirements are higher than usual for such solicitation, can the City please disclose its budget/budget range for this contract? We will need to consider our ability to bid based on insurance cost versus the contract amount.
178	A		See response for question 19.
179	Q	General	Is this contract a recompete?
179	A		Yes.
180	Q	General	Who is the current incumbent?
180	A		The services were completed on the last purchase order that was issued and that is why it's out for bid.
181	Q		Is the City of Memphis on the IBM Z/OS Mainframe? If so, are you utilizing RACF, ACF2 or Top Secret?
181	A		No.
182	Q	2.4	Is the network penetration testing required for regulatory compliance program(s)? (e.g. PCI, HIPAA etc.)
182	A		See response to question 63 and 74.
183	Q	2.4.1	Are the 100 public facing IPv4 addresses active or live IPs? Or is that the potential IP address range?
183	A		Estimated active IPs.
184	Q	2.4.2	How many web application(s) are in-scope? What are they?
184	A		See response to question 6 and 141.
185	Q	2.4.2	For the in-scope web application(s), are they owned, hosted, and maintained by the City?

			If not, does the City have approval/authorization from the third-party for a vendor to perform penetration testing on their web application(s)?
185	A		Hosted and managed by the City.
186	Q	2.4.2	For each in-scope web application: • Does the City want authenticated (credentials) web application penetration testing? • For authenticated based testing, please indicate the number of user types the City requires to be tested. (e.g. Admin, Power User, User, etc.) • How many environments (prod/staging/dev/test etc.) will be tested? • How many databases and servers? • How many webpages (dynamic and static)?
186	A		• See response to question 8 • N/A • Prod • 5 Databases and 20 servers • 1200 approximately
187	Q	2.4.3	How many web application(s) are in-scope? What are they?
187	A		See response to question 6 and 141.
188	Q	2.4.3	For the in-scope web application(s), are they owned, hosted, and maintained by the City? If not, does the City have approval/authorization from the third-party for a vendor to perform penetration testing on their web application(s)?
188	A		Hosted and managed by the City.
189	Q	2.4.3	For each in-scope web application: • Does the City want authenticated (credentials) web application penetration testing? • For authenticated based testing, please indicate the number of user types the City requires to be tested. (e.g. Admin, Power User, User, etc.) • How many environments (prod/staging/dev/test etc.) will be tested? • How many databases and servers? • How many webpages (dynamic and static)?
189	A		See response to question 186.
190	Q	2.4.4	How many physical locations are in-scope?
190	A		See response to question 14.

191	Q	2.4.1	Is the City of Memphis willing to allow a non-invasive external port scan to be conducted in advance of proposal submission as a qualification exercise in order to validate public-facing IP ranges and the # of active hosts (i.e. open/listening ports)?
191	A		Public facing address scope will be provided. See response to question 5 and 93.
192	Q	2.4.1	If not, how many active hosts (i.e. open/listening ports) are in scope out of the 100 public-facing IPv4 addresses identified under 2.4.1?
192	A		See response to question 5 and 93.
193	Q	2.4.1	Is the City of Memphis willing to disable specific security controls once their effectiveness has been substantiated during testing in order to increase the substance of the testing effort and maximize cost efficiencies?
193	A		When absolutely needed, the City of Memphis will work with the selected vendor to perform intended testing to validate security controls.
194	Q	2.4.1	Approx. how many recipients are in scope for the phishing requirement identified under 2.4.1?
194	A		See response to question 72.
195	Q	2.4.2	Please confirm the public-facing URL(s) of the website(s) in scope.
195	A		See response to question 6.
196	Q	2.4.2	Is the City of Memphis seeking authenticated or unauthenticated pen testing of the web application(s) in scope?
196	A		See response to question 8.
197	Q	2.4.2	If authenticated, is the City of Memphis willing to provide test user credentials with the desired privileges (i.e. end user, manager, admin, etc.) in order to qualify size/complexity of the site(s) from an authenticated perspective? The size/complexity (# of dynamic pages, forms/inputs, functional characteristics, etc.) of the site(s) post-authentication will directly impact the required production time and the subsequent costs involved.
197	A		N/A See response to question 8.
198	Q	2.4.2	If not, what are the total # of dynamic pages and total number of forms/inputs of the website(s) post-authentication? Please describe the overall functional attributes available to the user perspective that will be tested (links, radio buttons, drop-downs, report generation, etc.)
198	A		See response to question 47, 48.
199	Q	2.4.2	Is web application testing to be conducted against the live production server environment or a test server environment?
199	A		See response to question 106.

200	Q	2.4.2	If web application testing is performed on the live production server, are there portions of the site that should not be tested in order to avoid a potential interruption of service?
200	A		Yes. Details will be give after contract is awarded.
201	Q	2.4.2	Are the web applications in scope hosted on-premise or with a 3rd party hosting provider?
201	A		On Prem.
202	Q	2.4.2	If with a 3rd party hosting provider, has the City of Memphis received permission to test the web applications in scope?
202	A		N/A.
203	Q	2.4.3	Is the City of Memphis seeking an internal penetration test, internal vulnerability assessment, or both?
203	A		Refer to Section 2.1 (scope) of the published RFP.
204	Q	2.4.3	If an internal vulnerability assessment is in scope, is the City of Memphis willing to issue temporary administrative credentials to conduct an authorized vulnerability assessment against the internal network to ensure all required assets are accessible for scanning?
204	A		Yes.
205	Q	2.4.3	How many security domains are in scope? Are all domains in scope accessible from one physical location?
205	A		Two (2) Active directory domains. Yes.
206	Q	2.4.4	How many buildings are in scope for 2.4.4? What is the geographical proximity of the locations in scope?
206	A		See answers to question 14, 36.
207	Q	2.4.5	How many recipients are in scope for social engineering testing?
207	A		See answers to question 72, 91, 17 and 18.
208	Q	2.4.5	Does the City of Memphis require the attack vectors identified under 2.4.5 or is the vendor to propose on one or a combination of attack vectors for consideration?
208	A		All listed methods are to be attempted.