CITY OF MEMPHIS

REQUEST FOR PROPOSAL

#71740

SECURITY PENETRATION TESTING

Addendum One (1)

Questions & Answers

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

•		Section	Question / Answer
1	Q		What is the required timeframe to complete each item per year?
1	A		*The City requires the vendor to provide a proposed schedule as stated in section 2.2 that best addresses the requirements in section 2.4*
2	Q		Is there a priority order in which you would like to complete each assessment?
2	A		NO
3	Q		Are you willing to place Shanken equipment on your internal network for the internal assessment portion?
3	A		After vetting and approval from City Security team.
4	Q		What is the number of external IP addresses in scope for the penetration testing?
4	A		See section 2.4.1 of the Published RFP
5	Q		What is the number of internal IP addresses in scope for the penetration testing?
5	A		See section 2.4.3 of the Published RFP
6	Q		Are the external systems hosted by a third-party provider?
6	A		A combination of internally hosted and third-party hosted.

7	Q		How deep should testing go in the event of successful network penetration (i.e., just validation of vulnerability, network administrator access, server access, etc.)?
7	A		See Requirement Section 2.4
8	Q		Are VPN, Terminal Services, Remote Desktop, FTP and other remote services being tested?
8	A		See section 2.4 for services in scope.
9	Q		What firewall vendor(s) are in production?
9	A		Palo Alto Firewalls
10	Q		What is the tolerance for outage during the testing? (e.g., are there reliable backups if something fails)
10	A		There are reliable backups. Any intrusive test that might cause an outage will have to be approved by City IT as stated in section 2.4
11	Q		Can we perform credential harvesting via phishing campaigns?
11	A		Yes
12	Q		Will testers be granted any level of initial access prior to the start of the penetration test (e.g., standard user credentials to simulate insider threat)?
12	A		See section 2.4.3 of the published RFP
13	Q		Is the target organization’s infrastructure centrally managed (e.g., Active Directory, Jamf, etc)?
13	A		Yes

14	Q		Can remote internal networks be scanned via a primary location, or would it be necessary to perform field visits to each in-scope location?
14	A		Networks in scope can be scanned from a primary location
15	Q		Is an Active Directory (AD) account going to be provided for certain aspects of testing?
15	A		See section 2.4.3 of the published
16	Q		Are ‘private’ and ‘guest’ the only wireless networks (distinct SSIDs) that are in scope of penetration testing?
16	A		No
17	Q		Is the wireless network controller-based or access-point based?
17	A		Controller-Based
18	Q		Will Wi-Fi testing be conducted at each location?
18	A		See section 2.4.3 of the published
19	Q		Please provide an estimate of the types of Wireless in use (microwave, 802.11x, proprietary, cell phone, blackberry, iPhone, Bluetooth, Point-to-Point, etc.).
19	A		802.11n
20			What wireless device vendor(s) are deployed?
20	A		Aruba Wireless
21	Q		For the wireless assessment, will we be able to send someone onsite with an escort?

21	A		Yes
22	Q		How many web applications require testing (this number was not included in “The Environment includes” statement?
22	A		See Section 2.4.2 of the published RFP
23	Q		Approximately how many pages per web application require testing?
23	A		See Section 2.4.2 of the published RFP
24	Q		How many user roles per each web application?
24	A		See Section 2.4.2 of the published RFP
25	Q		How many APIs are to be tested with each in scope web application?
25	A		See Section 2.4.2 of the published RFP
26	Q		What language(s) are the applications written in?
26	A		See Section 2.4.2 of the published RFP
27	Q		Will source code and documentation be made available to the testing team?
			If applicable
27	A		
28	Q		Are web applications on premise, public, or private cloud? Please detail this environment to include numbers, types, location, etc.
28	A		See Section 2.4.2 of the published RFP

29	Q		For applications that require authenticated testing, how many user roles would be in scope for each application, on average? For example, read-only, basic, supervisor, admin, etc.?
29	A		Basic and admin roles
30	Q		Social Engineering: Do you require credential harvesting during this campaign?
30	A		Yes
31	Q		Social Engineering: Do you require physical access to buildings during this testing?
31	A		See section 2.4.4 of the published RFP
32	Q		Will the web application penetration test be performed on production environments, or will a test environment be provisioned?
32	A		See Section 2.4.4 of the published RFP
33	Q		Will the API endpoint sin the web application penetration test portion be authenticated or unauthenticated?
33	A		See Section 2.4.2 of the published RFP
34	Q		The RFP states, that “the penetration test style should assess the security of all critical networked assets including servers, desktops, firewalls, network devices, wireless infrastructure, cloud exposures,

			and network monitoring and management." Are these assets provided or is it up to the penetration test team to note these?
34	A		All assets specified in section 2.4.3 will be provided. The vendor will be required to do a discovery of other assets in scope as stated in section 2.4.3
35	Q		Is the intention to provide a health check of the active directory environment?
35	A		See Section 2.4.3 of the published RFP
36	Q		Are there any specific goals or objectives for the internal test, except for findings vulnerabilities? (i.e. gain access to certain systems or certain level of access)
36	A		See Section 2.4.3 of the published RFP
37	Q		Will an authorization letter from a project sponsor be provided to the vendor selected for this test in the event of a tester being caught?
37	A		If the question is in reference to the section 2.4.4 - YES
38	Q		Are all of the techniques provided in the RFP (Phishing, Vishing, Spear Phishing, BEC, Whaling, PreTexting) all in scope or will we choose a subset of those?
38	A		See Section 2.4.5 of the published RFP
39	Q		What MBE WBE and/or Small Business Enterprises does the City of Memphis leverage today?
39	A		The City leverage all MBE WBE enterprises that are registered to do business with the City. Please find more information here: https://www.memphistn.gov/business/doing-business-with-the-city/

40	Q		Would the City be willing to share their information?
40	A		Please find more information here: https://www.memphistn.gov/business/doing-business-with-the-city/
41	Q	General Requirements	Are we to provide the results of our employees background checks in our proposal response?
41	A		Upon Request by the City.
42	Q	EBO Program	May we request a waiver?
42	A		No. This is a requirement
43	Q	EBO Program	What is the M/WBE participation goal for this solicitation?
43	A		This is determined by our Office of Business Diversity and Compliance (OBDC) Office at time of award
44	Q	Proposal Submissions	Do you want the six copies to be tabbed and in binders?
44	A		Yes
45	Q	Exhibits	Under which Section/Tab are we to include Exhibit 2 – Criminal And Civil Proceeding Disclosure?
45	A		All exhibits are to be attached separately independent of the Sections unless explicitly stated
46	Q	Exhibits	Was Exhibit 6 – Evaluation Criteria intentionally left blank?
46	A		Please refer to Section 5.9 of the published RFP
46			
47	Q	2.4.5	Do you want all of these to be tested, or to down-select a group? If down-selecting, how many tests?
47	A		All stated methods are in scope when they do not overlap

48	Q	2.4.2	Is there a possibility that that application crawling step of these can be performed off-site since it is highly time-consuming and should be done off-hours?
48	A		Please refer to Section 2.4.2 of the published RFP
49	Q	2.4.3	Is wireless to be tested?
49	A		Yes
50	Q	2.4.5	Do you want all of the 6 identified areas social engineering tested?
50	A		Section 2.4.5 specifies that tests MAY include the 6 identified methods.
51	Q	2.4.2 Web Application Penetration Test	If the vendor has a secure and well established and certified means of conducting this task offsite, thus saving the city time and money, would the city consider off-site execution?
51	A		Upon review and approval of the vendors process, this can be considered.
52	Q	2.4.3 Internal Network Security Penetration Test	If the vendor has a secure and well established and certified means of conducting this task offsite, thus saving the city time and money, would the city consider off-site execution?
52	A		See specified requirement in section 2.4.3
53	Q		What is the City's budget for this project?
53	A		This information can not be disclosed at this stage. Vendor should provide estimated budget in accordance with the Requirements stated in section 2.4 of the published RFP
54	Q		How many unique databases are in scope for database-specific testing?
54	A		See section 2.4.3
55	Q		If databases are in different locations, can all locations be reached from one central location?
55	A		Yes

56	Q		Is a Server Configuration Review in scope and if so: How many unique server brands are in scope for testing? What devices does the Security Configuration Review cover?
56	A		Not in Scope
57	Q		Is City’s wireless network controller-based or access-point-based? How many locations are in scope for wireless network testing?
57	A		See Answer to Question 17; see section 2.4.3
58	Q		How many targets are in scope for the following social engineering tests: Business email compromise Phishing Spear phishing Whaling
58	A		See section 2.4.5 of the published RFP
59	Q		How many endpoints are in scope?
59	A		See section 2.4.3 of the published RFP
60	Q		What are the primary business drivers for issuing this RFP?
60	A		Competitiveness, Transparency
61	Q		Can we please have details regarding the IT/System landscape at the city?
61	A		Will be provided to selected vendor after contract is awarded
62	Q		Can you please share the current support team structure for IT support at city?

62	A		Will be provided after contract is awarded.
63	Q		Are all the resources required to work onsite? Or remote/offshore work is an option?
63	A		Remote/Onsite as per the RFP Requirements. Offshore is not an option.
64	Q		Can you please share the Current and To-be landscape details?
64	A		Will be provided after contract is awarded.
65	Q		Please share details regarding customizations and interfaces
65	A		Will be provided after contract is awarded.
66	Q		Are systems currently hosted on-premises or on Cloud?
66	A		Hybrid
67	Q		Does city plan to select a single vendor or multiple vendors for this RFP?
67	A		Single Vendor
68	Q		Is this a new RFP or there are any incumbents?
68	A		New RFP for Calendar year 2022.
69	Q		If there are incumbents, can we have the names and if possible, a copy of their past contract with city?
69	A		Not for Calendar Year 2022. Past contract was with Securance Consluting - https://www.securanceconsulting.com/
70	Q		Can we submit separate cost options for onsite vs. offsite/offshore as city is not yet sure if this remote project can convert to onsite?

70	A		Cost can be itemized with a Grand total reflecting the cost for the entire engagement
71	Q		Our company is certified as an MBE NSMDC. Are we good to suffice requirements for DBE?
71	A		This will have to be clarified with the City's Office of Business Diversity and Compliance (OBDC)
72	Q		Do we need to submit details/resumes regarding identified resources?
72	A		Yes
73	Q		Do you need complete resume or summary only?
73	A		Summary
74	Q		We are not yet sure of when the project will start for each specific skill and hence the submitted resources might not be available at that time. Can we submit representative resumes or city needs specific resumes of individuals?
74	A		Representative Resumes identified to work on the project.
75	Q		Are there any specific taxes that the vendor should be aware of while submitting the cost proposal
75	A		Please refer to https://www.memphistn.gov/business/doing-business-with-the-city/
76	Q		Please provide the Diverse Business List of subcontractors which can be considered for participating in this RFP.
76	A		Please refer to: https://www.memphistn.gov/business/doing-business-with-the-city/

77	Q		What compliances are being sought, if any. For example, PCI, SOC1/2/3, CMMC etc. and what levels, if any and what periodicity they need renewed?
77	A		See Section 2.1 of the published RFP
78	Q		Approximate team strength in IT or the CISO office who will be dedicated to this effort and their expertise?
78	A		The City will make available dedicated IT staff to assist vendor through the engagement
79	Q		Has a CISA/NIST maturity test been conducted by the city - will you be willing to share the same
79	A		Yes – Not at this stage
80	Q		What is the scope of vulnerability scanning, what would be the period of testing would it be monthly, quarterly, or annually?
80	A		Vulnerability scans are performed weekly by City internal Team. For the scope of this exercise, vendor will perform scan only during engagement.
81	Q		Do you need to cover other areas such as phishing, and any other specific requirements?
81	A		See section 2.4.5 of the published RFP
82	Q	2.4.1	For the social engineering exercise for the external network, will the vendor find the targets from OSINT and obtain approval of targets from the City, or will the City provide the approved targets?
82	A		Social Engineering is covered under section section 2.4.5 of the published RFP
83	Q	2.4.1	Does the external network test include email services and the security of the configuration?

83	A		Business Email Compromise is covered under section 2.4.5 of the published RFP
84	Q	2.4.1	How many DNS names are in scope?
84	A		Not more than 50
85	Q	2.4.1	Are any external VPN aggregators in scope?
85	A		Yes
86	Q	2.4.1	Are any IPS/IDS systems in place, and is allow listing of the vendors' testing IP in scope?
86	A		Yes – IPS and IPS are in place. Allow listing of vendor IP can be discussed after contract is awarded
87	Q	2.4.2	Will the City be providing any developer documentation guide for the web application?
87	A		Yes – Upon request
88	Q	2.4.2	Will the vendors' IP addresses be allow listed so web application firewalls do not hinder testing?
88	A		See answer to question 86
89	Q	2.4.2	What is the exact environment the vendor would be testing? (DEV, SIT, UAT, PROD) Does this environment closely mirror PROD?
89	A		Test and Prod
90	Q	2.4.2	Will testing for the API be authenticated, and if so, which type of authentication is used? (OAuth, SAML, etc.)
90	A		Unauthenticated
91	Q	2.4.2	Can the City clarify if there are 3 APIs with additional endpoints or 1 API with 3 endpoints total, how many parameters are within each API, and do the APIs contain test data?
91	A		3 API Enpdoints. APIS contain test and prod data
92	Q	2.4.2	Will a swagger file or API documentation such as calls, and endpoint documentation be provided to the vendor? What format is the documentation in, and does this include test calls, including appropriate parameters?
92	A		Yes
93	Q	2.4.2	Are all input forms and the scoped 25-50 dynamic pages accessible without authentication?

93	A		A combination of Authenticated and Unauthenticated
94	Q	2.4.3	Is remediation testing expected, or is discussion-based remediation documentation all that is needed? If retesting is required, is it preferred this retest be performed on-site?
94	A		See Section 2.5 of the published RFP
95	Q	2.4.3	With the vendor using an un-trusted outsider methodology for the first test, will the City provide an “out of scope” or “do not touch” device listing for the engagement?
95	A		Out of scope list will be provided after contract award
96	Q	2.4.3	For low-level credentials testing, will a domain joined workstation or VM be made available to the vendor?
96	A		If needed by Vendor, this can be made available.
97	Q	2.4.3	Does the City have any testing needs for public SSIDs or are all in-scope SSIDs private production?
97	A		SSIDs in scope are both guest accessible and private SSIDs
98	Q	2.4.3	Does the scope for the wireless testing include wireless man-in-the-middle attacks, or is the scope limited to passive methods?
98	A		Wireless Man-in-the-middle is permitted
99	Q	2.4.3	Out of the 5000 endpoints, how many endpoints are IP cameras or NVRs?
99	A		Approximately 4%
100	Q	2.4.3	Is the Azure cloud tenant visible from the production network?
100		2.4.3	Can all production networks be accessed from an individual location for testing purposes?
	A		
101	Q	2.4.3	Is the City using an on-prem active directory instance or a cloud variant?
101	A		Hybrid
102	Q	2.4.3	Are any ICS (Industrial Control Systems) in scope? (Access Control, SmartHVAC, Elevator Control, Etc.)
102	A		No
103	Q	2.4.3	Is any VDI (Virtual Desktop Infrastructure) in scope?
103	A		No

104	Q	2.4.3	Does the City need segmentation testing to include testing procedures performed in accordance with the PCI DSS "Requirements and Security Assessment Procedures" outlined in version 3.2.1 with specific reference to testing procedure 11.3.4b? Will the City need this testing performed twice a year?
104	A	2.4.4	Is unauthenticated entry limited to passive (RFID cloning, piggybacking, social engineering, etc.) in scope?
105	Q	2.4.4	Is non-destructive bypass entry (under door tools, J-hooks, Latch bypass tools, request to exit bypass, etc.) in scope?
105	A	2.4.4	Is Covert Entry in scope?
		2.4.4	Does the vendor need to maintain access to sensitive areas for a certain amount of time or leave a device plugged into a non-public port?
106	Q	2.4.4	What constitutes a successful stop for a City employee and an attempt by the vendor? For example, if the vendor is declined access by a receptionist but not detained and no testing authorization letter is shown, does that constitute a pass or fail for the City, and would this action be considered an attempt if the vendor was not asked to leave the premises?
106	A		See section 2.4.4 of the published RFP for requirements pertaining to the physical security testing.
107	Q	2.4.4	If attempts for social engineering bypass fail, is the City expecting escorted physical access and control security consultation and site visits/walk-throughs?
107	A		Yes
108	Q	2.4.4	Is gaining physical access to restricted areas and network jacks the only goal of the assessment, or is retrieving sensitive information (PCI, PHI, PII, HIPAA, etc.) and persistent network access also in scope?
108	A		Retrieving Sensitive data and persistent network access in scope
109	Q	2.4.5	Are there any specific threat actors or pretexts the City is actively trying to defend against and would like tested during this assessment by the vendor?
109	A		No
110	Q	2.4.5	Are any OSINT techniques out of scope, i.e., Dark web harvesting, LinkedIn scraping, etc.?
110	A		No

111	Q	2.4.5	Do targets found from OSINT need to be approved by the City?
	A		Approval is only needed for methods that might be destructive in nature or might cause a downtime.
112	Q	2.5.2	What constitutes a successful breach of the internal network?
113	A		Successful exploit/compromise of a CoM system, network, Wireless Network, BEC, etc
113	Q	3.8	Section 3.8 and other sections of the RFP state that there is a M/WBE participation goal but does not give a percentage for that goal. The City's EEO policy sets the goal for participation at 13% MBE and 2% WBE. Are these the goals for this RFP? If so, can the city provide a list of approved M/WBE companies? Are meeting these goals required to be awarded this contract?
113	A		The City's EBO policy does apply to this contract.
114	Q	2.3	Section 2.3 Insurance Requirements says if the proposer is unable to provide the required insurance (listed in the sample contract RFP Exhibit 5) to address those during the Q&A period. However, the sample contract doesn't have the insurance requirements. Further down, RFP Section 3.7 says to attach a current 2022 Certificate of Insurance. Even further down, the RFP says our ability to meet the RFP insurance requirements is part of our proposal score / the point weighed criteria. Can the City please clarify whether we need to provide Certificates of Insurance and what coverage is required?
114	A		Certificate of Insurance is required for City IT contracts.
115	Q	6	Section 6 RFP Terms and Conditions states "Only proposals submitted on the provided form(s) with no changes, additions or deletions to the terms and conditions will be considered. Proposals containing terms and conditions other than those contained herein may be considered nonconforming." Upon being selected as the successful bidder, a firm may require modification to the terms and conditions, as referenced in the RFP, to comply with professional standards and/or firm policies. Would these requested changes cause a proposal to be removed from consideration?
115	A		City IT will require City Legal department to review and approve requested changes
116	Q		Is there currently an incumbent company or previous incumbent, who completed a similar contract performing these services? If so - are they eligible to bid on this project and can you please provide

			the incumbent contract number, dollar value, and period of performance
116	A		See response to Question 69.
117	Q		Specify the VLAN details how many are included in the Scope?
117	A		Detailed information will be provided after contract is awarded to vendor
118	Q		Can you please provide the current number of infrastructure details (Physical Server, Virtual Server, Network Devices, etc?
118	A		See section 2.4.3 for in-scope infrastructure
119	Q		How much (%) of the infrastructure is in the cloud?
119	A		10%
120	Q		In the IT department/environment, how many employees work?
120	A		100+
121	Q		Do you manage your own data Center, or do you utilize any 3rd-party/colocation facilities?
	A		The City manages its own datacenters
121	Q		Is there a funding/financial/budget range estimated that can help us to provide a quotation for this project?
	A		See response to question 53.
122	Q		On page 13 of 57, in the paragraph entitled, Equal Business Opportunity Program, the M/WBE goal for the solicitation is not stated (shows as XX%). Could the City please clarify if there is, in fact, an M/WBE goal for this solicitation, and if there is, what the percentage might be; and if not, does the Equal Business Opportunity Program Compliance Form need to be submitted?
	A		See response to question 113
	Q		

	A		
	Q		
	A		
	Q		
	A		