	CITY OF O'FALLON, MISSOURI ***PURCHASING DEPARTMENT*** **100 North Main Street** **O'Fallon, MO 63366** **T: (636) 379-5527**		
RFP NUMBER:	**22-064**	**RFP ISSUE DATE:**	**06/10/2022**
RFP DESCRIPTION:	**MANAGED CYBER SECURITY SERVICES**		
RFP OPENING DATE:	**06/30/2022**	**RFP OPENING TIME:**	**12:00 P.M. CST**

June 23, 2022

ADDENDUM #1

The purpose of this addendum is to address questions received on or before 06/22/2022 at 12:00 P.M. CST. The time period for questions is closed. The due date/time remain the same.

Questions:

1. How can we become your listed supplier for informal/regular/budgetary quotes?

   Answer: *Please send an introductory email to the IT Director at phuff@ofallon.mo.us*

2. Could you please tell us about the dollar threshold under which bids aren't posted and are requested to the listed suppliers only?

   Answer: *Any purchase/transaction under $15,000.00 is not required to go through the formal bid process.*

3. To avoid bidding process do you accept a quote under contract vehicle? If yes, then is there any preferred contract?

   Answer: *The City does purchase under a contract vehicle. There are no preferred contracts.*

4. How many total servers (physical, virtual and including appliance servers) are there in the environment?

   Answer: *45, 11 physical servers and appliances, 34VMs.*

5. How many active IP assets are there on the external perimeter?

   Answer: *18*

6. How many web applications are in scope for semi-annual web application testing?

   Answer: *10*

7. Please confirm that you are requesting full, monthly external penetration testing, to include attempts to gain internal access to the environment, as opposed to vulnerability testing?

   Answer: *Vulnerability testing only.*

8. For “Full 7-Layer Packet Inspection,” does the City currently have a solution that is performing this level of analysis, or must the vendor include this in its price? If in its price, will the City perform the installation, or should the vendor also include installation costs?

   Answer: *The City’s current vendor uses a proprietary software for this, another vendor will need to replace and install new solution.*

9. For “Full 7-Layer Packet Inspection,” does the City want encrypted traffic to be included in this inspection? If so, does the City have an SSL intercept solution in place, or is one required from the vendor, to be included in its price? If in its price, will the City perform the installation, or should the vendor also include installation costs?

   Answer: *The current solution is behind the firewall and does not perform SSL inspection, if vendor’s solution requires an SSL intercept it should be included in the bid or bid as an option.*

10. For “Full packet analysis,” does the City want encrypted traffic to be included in this inspection? If so, does the City have an SSL intercept solution in place, or is one required from the vendor, to be included in its price? If in its price, will the City perform the installation, or should the vendor also include installation costs?

    Answer: *Please propose this as an optional feature.*

11. Will the City provide VMWare VM resources for the required onsite event collectors, scanners, and any other required onsite appliances?

    Answer: *Yes*

12. Please provide additional context and detail on the requirement, “Ensure business continuity and network hygiene in near real-time” with regard to EDR services.

    Answer: *SentinelOne is monitored by current vendor’s SOC and if any issues are detected that require attention or action, the City is notified.*

13. Does the City intend for all “24/7/365 Advanced Endpoint (Endpoint Detection and Response)” services to be delivered with its SentinelOne product? If not, which are to be provided by that solution, and which by the vendor?

    Answer: *Yes, the City’s SentinelOne dashboard is tied to the current vendor, it is expected that the winning bidder will be required to work with the City to move the dashboard to their SOC.*

14. For “Includes annual maintenance / licensing of SentinelOne endpoint protection software for up to 525 endpoints (includes ransomware warranty from endpoint software vendor),” does that mean the City will provide this tool, the vendor is expected to include the cost of this solution in its bid, or other meaning?

    Answer: *It means that the prospective respondent provide/include the cost of licensing SentinelOne as part of the bid.*

15. The “Format and Contents of the Proposal” does not require the bidder to provide any technical or management approach to meeting the requirements. Will the City add this as a requirement, or does the City not desire this information to evaluate proposals?

    Answer: *This is up to the respondent to include as completeness of proposals is a criteria.*

16. Are these services all new, or are some/all being provided by a current vendor? If a current vendor, please provide the vendor's name.

    Answer: *All are provided by an existing vendor. For current vendor information, please use the following link to make a request for public records. https://www.ofallon.mo.us/requests-for-public-information*

17. Will existing vendors providing IT, network, development, or other operational IT services be excluded from providing these services, due to a Conflict of Interest?

    Answer: *No*

18. For the requirement, "Each proposal shall consist of one original (identified as such). . ." does this mean the bidder is to provide a single, printed version of its proposal?

    Answer: *Yes*

19. As the City anticipates answering questions on June 24, and sealed hardcopy and softcopy proposals are due in 4 business days from then, will the City extend the due date by a week to allow bidders time to incorporate these substantive answers into their proposals?

    Answer: *At this time, the City chooses not to extend beyond the initial deadline.*

20. What is the required timeframe to complete each item per year?

    Answer: *This information is listed in the RFP. Please refer to the document.*

21. Is there a priority order in which you would like to complete each assessment?

    Answer: *No*

22. Are you willing to place equipment on your internal network for the internal assessment portion?

    Answer: *Yes*

23. What is the number of external IP addresses in scope for the penetration testing?

    Answer: *18*

24. What is the number of internal IP addresses in scope for the penetration testing?

    Answer: *Approximately 1,000*

25. Are the external systems hosted by a third-party provider?

    Answer: *No*

26. How deep should testing go in the event of successful network penetration (i.e., just validation of vulnerability, network administrator access, server access, etc.)?

    Answer: *Validation of vulnerability*

27. Are VPN, Terminal Services, Remote Desktop, FTP and other remote services being tested?

    Answer: *Any protocol / service seen on the LAN and perimeter should be tested.*

28. What firewall vendor(s) are in production?

    Answer: *IT will provide the logs and polices for review.*

29. What is the tolerance for outage during the testing? (e.g., are there reliable backups if something fails)

    Answer: *There is no tolerance for outages during vulnerability scans*

30. Can we perform credential harvesting via phishing campaigns?

    Answer: *Yes*

31. 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)?

    Answer: *Yes*

32. Is the target organization's infrastructure centrally managed (e.g., Active Directory, Jamf, etc)?

    Answer: *Yes*

33. Can remote internal networks be scanned via a primary location, or would it be necessary to perform field visits to each in-scope location?

    Answer: *Primary location*

34. Is an Active Directory (AD) account going to be provided for certain aspects of testing?

    Answer: *Yes*

35. Are 'private' and 'guest' the only wireless networks (distinct SSIDs) that are in scope of penetration testing?

    Answer: *Wireless is not called out in the RFP*

36. Is the wireless network controller-based or access-point based?

    Answer: *This is not in scope of the RFP*

37. Will Wi-Fi testing be conducted at each location?

    Answer: *This is not in the scope of the RFP*

38. Please provide an estimate of the types of Wireless in use (microwave, 802.11x, proprietary, cell phone, blackberry, iPhone, Bluetooth, Point-to-Point, etc.).

    Answer: *This is not in the scope of the RFP*

39. What wireless device vendor(s) are deployed?

    Answer: *This is not in the scope of the RFP*

40. For the wireless assessment, will we be able to send someone onsite with an escort?

    Answer: *This is not in the scope of the RFP*

41. How many web applications require testing (this number was not included in “The Environment includes” statement?

    Answer: *10*

42. Approximately how many pages per web application require testing?

    Answer: *This is not in the scope of the RFP*

43. How many user roles per each web application?

    Answer: *This is not in the scope of the RFP*

44. How many APIs are to be tested with each in scope web application?

    Answer: *This is not in the scope of the RFP*

45. What language(s) are the applications written in?

    Answer: *This is not in the scope of the RFP*

46. Will source code and documentation be made available to the testing team?

    Answer: *This is not in the scope of the RFP*

47. Are web applications on premise, public, or private cloud? Please detail this environment to include numbers, types, location, etc.

    Answer: *The vendor’s scans will look for vulnerabilities that exist on the LAN and perimeter, not specific applications called out by IT.*

48. 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.?

    Answer: *This is not in the scope of the RFP*

49. Social Engineering: Do you require credential harvesting during this campaign?

    Answer: *In certain cases, yes.*

50. Social Engineering: Do you require physical access to buildings during this testing?

    Answer: *In certain cases, yes.*

51. Monitoring Section: Do you have software or hardware in place already for full packet analysis?

    Answer: *Yes*

52. Monitoring Section: For Full 7-layer packet inspection and analysis, are these the same 525 endpoints count as stated regarding Sentinel One in the Advanced Endpoint Section?

    Answer: *Yes*

53. Advanced Endpoint Section: Do you already have Sentinel One from a prior consultant, or this is a new deployment of Sentinel One?

    Answer: *It is existing.*

54. 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?

    Answer: *There is an incumbent company, and they are eligible to bid. For current vendor information, please use the following link to make a request for public records.* *https://www.ofallon.mo.us/requests-for-public-information*

55. How many physical locations?

    Answer: *22*

56. Do you manage your own data Center, or do you utilize any 3rd-party/colocation facilities?

    Answer: *We manage just our own data center.*

57. Are any security products installed? If yes, please provide product name.
    a. Security Incident & Event Management (SIEM)? If yes, which SIEM product name and is it internally or externally managed?

       Answer: *The existing SIEM solution is externally managed, but the product name* is not relevant to the scope of the RFP.

b. Endpoint Detection and Response (EDR)

Answer: *This is specified in the RFP. Please refer to the document.*

c. Vulnerability management

Answer: *No*

d. Email security

Answer: *Not applicable*

e. Network threat analytics

Answer: *No*

58. Can you provide the number of the security devices and other log sources to be monitored per the categories listed below? Just need the Device Qty for each.

Endpoint:

- Number of endpoints?

  Answer: *Approximately 1000 nodes on the network.*

- Count of Windows/Mac/Linux Desktops/servers (rough)?

  Answer: *Approximately 525*

Network:

- Number of ingress/Egress Points

  Answer: *2*

- Type of media connectivity

  Answer: *Fiber*

- Average and Max Mbps at each Ingress/Egress point

  Answer: *1gb*

- High Level network diagram, if available

  Answer: *This is not available.*

Email:

- How many mailboxes?

  Answer: *This is not in the scope of the RFP.*

- Are you currently using Office 365? If so are you using EOP/ATP?

  Answer: *This is not in the scope of the RFP.*

Current and projected number of users:

- How many network users (at a workstation most of the day)?

  Answer: *350*

- How many users are not on the network most of the day, but authenticate with a domain controller (such as remote workers, maintenance staff, etc)?

  Answer: *200*

Servers/Desktops:

- Windows Servers - HIGH EPS (~50 eps)
- Windows Servers - Low EPS (~2 eps)
- Windows Workstations (5 / 1k users)
- Windows AD Servers
- Linux Servers
- DNS (enter # per 1000 users)

Answer: *Information in this section is not needed for vulnerability scan.*

Network Infrastructure (# of devices):

- Routers

  Answer: *2*

- Switches (netflow not supported)

  Answer: *45*

- Wireless LAN

  Answer: *100*

- Network Load-Balancers

  Answer: *0*

- WAN Accelerator

  Answer: *0*

- Other Network Devices

  Answer: *0*

Security Infrastructure:

- Firewall - Internet (Enter # in 1000's of users)
- Network Firewalls (Partner / extranets)
- Network Firewalls (DMZ)
- Network IPS/IDS
- Network VPN - Enter # in 100's of users
- Email AntiSpam - Enter # in 100's of users
- Network Web Proxy (enter # in 100's of users)
- Other Security Devices

  Answer: *The city would prefer not to answer this section in an addendum due to security concerns. However, you may use the following link to make a request for public records.* *https://www.ofallon.mo.us/requests-for-public-information*

Applications (Device count assumed with numbers above):

- Web Servers (IIS, Apache, Tomcat)
- Database (MSSQL, Oracle, Sybase - indicate # of instances)
- Email Servers (Enter # in 1000's of users)
- AntiVirus Server (Enter # in 1000's of users)
- Other Applications (Email, DB, AV, etc)

  Answer: *This section is not in the scope of the RFP.*

59. Is there a funding/financial/budget range estimated that can help us to provide a quotation for this project?

    Answer: *No. Please provide your best proposal.*

60. What is the total number of employees?

    Answer: *725*

61. Can bidders respond only to certain sections regarding General Requirements? E.g. We do not resell SentinelOne, so we would not bid on that section

    Answer: *The City prefers a proposal for all items in the RFP. Another endpoint protection solution can be proposed as an alternative.*

62. Does a vulnerability management program exist?

    Answer: *No*

63. Does the City use maintain any vulnerability scanning tools that are to be used for assessments?

    Answer: *No*

64. How many hosts or network segments are within scope for internal vulnerability assessment?

    Answer: *Approximately 1,000*

65. Does internal assessment include wireless or IoT devices?

    Answer: *No*

66. What is the current events per second (EPS) rate?

    Answer: *This is not in the scope of the RFP*

67. Have certain risk and/or compliance frameworks been adopted? If so, which ones.

    Answer: *No, not formally*

68. Does the City have a current SIEM solution in place?

    Answer: *No*

69. What cloud services are within scope of assessments?

    Answer: *None*

70. What firewall is in place?

    Answer: *The City will provide logs and policies for the assessment to the awarded vendor.*

71. What endpoint protection is currently in use?

Answer: *This is specified in the RFP. Please refer to the document.*

72. How many domain controllers make up Active Directory?

Answer: *The city would prefer not to answer this section in an addendum due to security concerns. However, you may use the following link to make a request for public records. https://www.ofallon.mo.us/requests-for-public-information*

73. Does the City use Azure Active Directory too?

Answer: *No*

74. How many web applications are in scope?

Answer: *8*

75.External Network Vulnerability Assessment / Penetration Testing:

- Confirm total number of public facing / external network IP addresses to be tested (If providing an IP range, please indicate the estimated number of live IPs).
  Answer: *18*

- Are 3rd Parties required to comply with or be aware of and agreeable to the Penetration Testing?
  Answer: *No*

- Number of Web based applications/ services to test (dynamic pieces of websites that users or other application authenticate to – client portal, sales quote system).
  Answer: *10*

- VPN, Terminal Services, Remote Desktop, FTP, and other remote services to be tested?
  Answer: *All protocols and services detected on the LAN / perimeter should be scanned for vulnerabilities.*

- Is an objective of this test to also assess the Company's intrusion detection capabilities?
  Answer: *No*

- How deep should testing go in the event of successful network penetration (i.e. just validation of vulnerability; network administrator access; server access, etc.)?
  Answer: *Just validation of vulnerability*

- Are the external systems hosted by a third-party provider?
  Answer: *No*

- Does your organization own and manage the network equipment at your external perimeter?
  Answer: *Yes*

76.Internal Network Vulnerability Assessment / Penetration Testing:

- Confirm total number of internal network IP addresses to be tested (If providing an IP range, please indicate the estimated number of live IPs).
  Answer: *Approximately 1,000*

- How deep should testing go in the event of successful network penetration (i.e. just validation of vulnerability; network administrator access; server access, etc.)?
  Answer: Validation of vulnerability only

- Are internal web based applications / services in scope, if so, please provide an indication as to the anticipated number of web based applications/services that may need to be assessed.
  Answer: This is not in the scope of the RFP

- Is it desired to evaluate the strength of mobility environments (iPhones, BlackBerry, home VPN access)?
  Answer: No

- Are corporate build / configuration standards in place for various platforms (network devices, operating systems, etc.) and if so, is it desirable to evaluate against those standards, etc. This will determine the amount of time required to perform additional analysis and tuning of evaluation criteria.
  Answer: No

- Can remote internal networks be scanned via a primary location or would it be necessary to perform field visits to each in-scope location?
  Answer: Yes, via a primary location.

- Are any of the internal application a third-party providers?
  Answer: Yes

77. Wireless Security Assessment:
- Will Wi-Fi testing be conducted at each location? If so, how many SSIDs and which locations?
  Answer: No

- Please provide an estimate of the types of Wireless in use (microwave, 802.11x , proprietary, cell phone, blackberry, iPhone, Bluetooth, Point-to-Point, etc.).
  Answer: 802.11x, iPhone, Bluetooth

- Are formal wireless security policies in place?
  Answer: No

78. For assessments and penetration testing, how many IP addresses would be in scope?

Answer: Approximately 1,000

79. If possible, please break these out by networking equipment, servers (virtual and physical), locations, and end-user devices.

Answer: 150 networking equipment, 11 physical servers, 34 virtual, 450 end users devices across 22 locations.

80. How many systems would be in scope for PCI scanning?

Answer: Approximately six.

81. How many firewalls, and what vendor?

Answer: The City will provide firewall logs and policies to the awarded vendor.

82. Is the City of O'Fallon looking for phishing or some other service?

Answer: *Any form of social engineering in addition to phishing.*

83. How many users would be part of campaigns?

Answer: *Approximately 750.*

84. What information does the City of O'Fallon get from current "Active Directory Scans" and/or what is the City of O'Fallon looking for?

Answer: *Password reset, failed login attempts, membership change in privileged account groups.*

85. How many web applications would need semi-annual scans? Are they custom developed or 3rd party tools?

Answer: *This is not in the scope of the RFP*

86. Please list recurring activities performed by current vCISO role or security consultant apart from regular monthly calls (e.g., policy revision/development, vendor risk assessments, vulnerability triage/management, executive reporting, risk management, etc).

Answer: *Just monthly meetings*

87. Is the City of O'Fallon already subscribed to CISA Cyber Hygiene services from DHS?

Answer: *No*

88. What SIEM platform is currently in place for event aggregation/collection?

Answer: *There is no SIEM in place under control of the City of O'Fallon.*

89. What platform currently facilitates simulated social engineering and security awareness training, if any? Is it licensed separately by the City of O'Fallon, or provided per contract by the security services provider?

Answer: *Security awareness training is not in scope.*

90. Can you provide us with a network walkthrough and network documentation?

Answer: *The city would prefer not to answer this section in an addendum due to security concerns. However, you may use the following link to make a request for public records. https://www.ofallon.mo.us/requests-for-public-information*

91. How many IP's in scope for the ASV scans

Answer: *Approximately 6*

92. What manufacture & model number of the firewalls

Answer: *City staff will provide event logs and policies to the awarded vendor*

93. What are you looking for delivery on Active Directory Scan

Answer: *Monitoring changes in privileged access group membership, password lockouts, failed logins.*

94. Computer based security awareness training acceptable

Answer: *Yes.*

95. At the main headquarters, how many people work out of that location?

Answer: *125*

96. At the main HQ and Datacenter, please tell us how many of the following items are located there:
    a. AV/EDR Brands (ie Crowdstrike, Symantec, Carbonblack)

        Answer: *This is specified in the RFP. Please refer to the original document.*

    b. Database Brands (Ie MS SQL, My SQL)

        Answer: *Not needed for vulnerability scan*

    c. Email – Are you using an on-premise server like Exchange or a cloud-based service like O365?

        Answer: *Not needed for vulnerability scan*

    d. Vulnerability Scanner Brand (ie Tenable.io, Nessus, Nexpose) – Please list each brand

        Answer: *The City does not manage a vulnerability scanner*

    e. Web Server Brand (ie IIS, Apache)

        Answer: *Not needed for vulnerability scan*

    f. Cloud Services and Number of Instances in Cloud (ie. Azure with 20 instances)

        Answer: *This is not in the scope of the RFP*

    g. Number of Linux/Unix Servers

        Answer: *2*

    h. Number of Windows Domain Controllers

        Answer: *1*

    i. Number of Windows Servers

        Answer: *41*

    j. Number of Firewalls at Ingress/Egress Points (Count HA Pairs as 1 Firewall)

        Answer: *1*

    k. Number of Firewalls between network segments (east/west traffic)

        Answer: *0*

    l. Number of Wireless Controllers

        Answer: *0*

    m. Number of Wireless Access Points

        Answer: *100*

97. How many remote locations do you have?

Answer: *21*

98. What are the average employee count at those locations?

Answer: *This information is not readily available*

99. At each location, please tell us how many of the following items are located at each location. Note: If the location does not have an item, please list the number at 0 (so if you only have domain controllers at the DC or Main HQ, list the count as 0 at each location):
    a. Number of Linux/Unix Servers -
    b. Number of Windows Domain Controllers -
    c. Number of Windows Servers -
    d. Number of Firewalls at Ingress/Egress Points (Count HA Pairs as 1 Firewall) -
    e. Number of Firewalls between network segments (east/west traffic) –
    f. Number of Wireless Controllers
    g. Number of Wireless Access Points

    Answer: *Information in this section is not readily available.*

100. What current EDR vendor

Answer: *SentinelOne.*

101. # of Endpoints & Servers

Answer: *525*

102. Looking to keep current/renew EDR tool

Answer: *Yes*

103. How many live internal & external IP's

Answer: *Approximately 1,000 internal / 18 external*

104. SIEM and MDR Services Questions:

a) What is your requirement for log retention?

Answer: *24 months.*

b) Please provide a breakdown of the below devices:

Servers	Linux 2	Windows 41
Workstations	350	
Firewalls	1	
Total no of sites for connectivity	22	
Total no of Network devices	Switches 50	Routers 2
SCADA Devices	0	

c) How many users are in the network? Or Employees?

Answer: *725 employees*

d) How many events (system events/syslog's/FW logs, etc.) per second/day are we looking at? (EPS)

Answer: *The City does not manage this metric*

e) What Endpoint Detection & Response (EDR) solution do you use (if any)?

Answer: *This is specified in the RFP. Please refer to the original document.*

f) Are all Servers/endpoints in the scope for SIEM and Monitoring?

Answer: *Yes*

g) How many Network devices do you have in the Network?

Answer: *150*

h) How Many Log sources do you have today in the Network?

Answer: *2*

i) What is the size of your IT Team?

Answer: *This is not in the scope of the RFP*

j) Do you have infrastructure hosted in the cloud (AWS, Azure, GCP, etc.)?

Answer: *This is not in the scope of the RFP*

k) Does the district require Network Traffic Analysis (NTA)?

Answer: *Respondents are required to ask the district*

l) How many total locations do you have and how are they connected today?

Answer: *22 locations. Various ways.*

m) Does any of the requirement need on site availability of personnel?

Answer: *No*

n) Do you need SOAR capabilities enabled?

Answer: *Yes*

o) What is the estimated budget for the project?

Answer: *Please submit your best proposal*

p) Is there an existing Incumbent partner providing these services?

Answer: *Yes*

q) Does the City need a SIEM solution as well or just manage the existing SIEM and provide 24X7 MDR services?

Answer: *The prospective vendor will need to assess if a SIEM is needed to meet the deliverables requested by the City.*

105. Pen test and Vulnerability Assessment Questions:

a) How many Internal and External IPs for Pen testing?

Answer: *1000 internal / 18 external*

b) How many applications are in the scope of Pen testing?

Answer: *The number is equal to the number of applications having vulnerabilities detected.*

c) Is there a requirement for Wireless Pen testing as well? If yes, how many SSID's are in scope?

Answer: *This is not in the scope of the RFP*

d) How frequently should Vulnerability scans have to be performed?

Answer: *This is specified in the RFP. Please refer to the original document.*

e) How many Servers are in the scope of Vulnerability Management?

Answer: 43

f) Is Vulnerability Scanning needed on both Servers and Workstations?

Answer: Yes

g) How frequently do you need the scans to be done?

Answer: This is specified in the RFP. Please refer to the original document.

h) Is Patch management a part of the scope?

Answer: This is specified in the RFP. Please refer to the original document.

i) How are you currently remediating the vulnerabilities found?

Answer: It depends on the vulnerability

j) Do you need any assistance with remediations as well?

Answer: Potentially

k) Do you need Web application testing?

Answer: No

l) Do you need an Incident response plan created?

Answer: No

m) Is there a need for a Tabletop exercise?

Answer: No

n) Are you using any Cyber security training tool? If yes, what?

Answer: No

106. Please provide the number of physical locations with DIRECT Internet access.

Answer: 1

107. Provide the total number of active users on the network.

Answer: 450

108. Does the City utilize Microsoft 365 or GSuite? If so, please provide the number of licensed users as well as the license type.

Answer: This is not in the scope of the RFP

109. The RFP specifically calls out firewall logs and DC events for monitoring. Are there other high priority or authentication systems that would require logging? If so, please describe.

Answer: No

110. Please describe the current Active Directory topology. Include trusts, replication to external systems such as AzureAD, and any other forests the City manages.

Answer: This is not in the scope of the RFP

111. For ongoing security assessments, please clarify the following:
    a) How many external facing IPs which are in scope for scanning and pen testing?

       Answer: 18

    b) How many internal IPs which are in scope for scanning and pen testing?

       Answer: Approximately 1,000

    c) How many IPs in scope for PCI-DSS ASV scanning?- approx.

       Answer: 6

    d) How many web applications (external facing)?

       Answer: This is not in the scope of the RFP

    e) How many firewalls? Are they same vendor or different vendors?

       Answer: Event logs and polices will be provided to the awarded vendor for analysis.

    f) How many users in Active Directory?

       Answer: 750

    g) How many users will participate in awareness training and phishing simulations?

       Answer: Varies

112. Does the city currently have a SIEM software? If so, how many events are being ingested per day? Per month? What is the name of SIEM software?

    Answer: The city does not currently manage a SIEM

113. Does the city currently have an EDR software, SentinelOne deployed? If so, is the city expecting the MSSP to hold the license?

    Answer: Yes, and the city will hold the license.

114. Does the city currently have a cybersecurity dashboard, or will this be a brand-new creation of a dash?

    Answer: Yes the city has a cybersecurity dashboard and yes a new dashboard will have to be created.

115. Does the city currently have a SOC (either outsourced or internal or hybrid)?

    Answer: The SOC is outsourced.

116. Little more details on Monitor static and behavioral AI scope?

    Answer: The city is unable to answer this because the question is unclear to us.

117. Is agency open to use anything apart from SentinelOne (Such as Qradar or Checkpoint or so) and if not is the agency looking for any specific service from SentinelOne?

    Answer: The City is open to alternatives to SentinelOne but prefers to stay with SentinelOne.

118. Is there any specific budget for this opportunity?

    Answer: Please submit your best proposal.

119. Evaluation Criteria: Criteria for Scoring Proposals rates familiarity with the city's network at 30%. This familiarity does not reference the actual results from a vulnerability or penetration test. In reference to the following "Hack the Pentagon" event hosted by the Department of Defense that resulted in better results from penetration testers who knew nothing about the network they were attacking. In the most recent test 58 penetration testers found 138 network vulnerabilities and in the previous test 650 penetration testers found 3,000 network vulnerabilities. Utilizing individuals who are familiar with the organizations network will not provide results that benefit any organization. Department of Defense's 'Hack the Pentagon' Bug Bounty Program Helps Fix Thousands of Bugs | WIRED

    While our team utilizes some of the best in the industry, we have no familiarity with the City's network. Would the City consider the possibility of removing this criteria from the scoring methodology?

    Answer: *No, the city will not remove this criteria, as it is only worth 30% of the total score.*

120. Section 2 of the scope of work requires 24 x 7 x 365 Monitoring (Managed Detection and Response). The bullet point list would seem to point to leveraging a SIEM rather than the proactive approach to threat hunting and cybersecurity that a MDR provides. Would the City say that a XDR service SIEM with a SOC access is more of what the City is looking for rather than an MDR?

    Answer: *The city is open to any proposals from prospective vendors that meet the desired outcome.*

121. Regarding the City's EDR needs: The Specs sheet mentions that the City has 525 endpoints that require EDR coverage. Does that number include servers and could we get an estimate on how many servers there are inside the City's network?

    Answer: *Of the 525 endponts, 43 are servers.*

122. With regards to the endpoint detection- would the city like to have different pricing options for licensing, maintenance, and/or complete monitoring/management of endpoints? Asking this to confirm whether the city already has the SentinelOne licenses and needs the maintenance/monitoring on top of it? Or they would like the vendor to provide the full licensing along with the maintenance and monitoring?

    Answer: *The city would like the prospective vendor to provide full licensing (in the city's name) along with the maintenance and monitoring.*

123. With regards to Network monitoring- can the city provide a general layout of their current firewall infrastructure? Specific firewall brands they are using and # of network locations/users per location? Do they want the vendor to manage the firewalls or just ingest from their current infrastructure?

    Answer: *Firewall logs and policies will be provided to the awarded vendor for analysis. The city only requires the ingestion of the current infrastructure.*

124. I just wanted to confirm with you that this RFP is taking all or nothing approach? I know it states that the City of Fallon wants a single supplier for all services, but I wanted to confirm.

    Answer: *The city prefers that prospective vendors submit a single proposal that encompasses the criteria stated in the RFP.*

Reminder:

The due date and time remains the same for this project. This is to remind all respondents that sealed proposals for RFP #22-064 Managed Cyber Security Services must be submitted by 12:00 P.M. CST, June 30, 2022 to:

Julie Moellering, Purchasing Agent
City of O'Fallon, Missouri
100 North Main Street
O'Fallon, Missouri 63366

Addendum information will be available over the Internet at www.ofallon.mo.us. Adobe Acrobat® Reader may be required to view this document. We strongly suggest that you check for any addenda a minimum forty-eight hours (48) in advance of the bid deadline. Due to revisions, the bidders must acknowledge the Addendum(s) on the bid form.

END OF ADDENDUM #1