



ADDENDUM #2

To: All Companies Interested in Submitting a Proposal
From: Rebecca Johnson, CPPB, Purchasing Agent
RFP: Managed Security Services (RFP #PUR0118-110); Dated: February 20, 2018
Subject: Addendum #2 (8 pages)
Date: March 8, 2018

The following questions and/or clarifications were asked relative to the above-listed Request for Proposal. This memo is sent for clarification to all companies to whom the RFP was sent.

1. Can some of the services be performed remotely? We have solutions that drive cost savings that allow for some of the services to be performed remotely.

Response: Yes, some services can be performed remotely. Please provide this detail in your proposal submittal.

2. Approximately how many systems are on the Internal network(s)? This could be communicated in terms of a CIDR range (example: two /16s would give us a general idea of size).

Response: Please see section 4.1 of the RFP.

3. How many physical locations would be in the scope for services? And would services need to be performed at each physical location, or are the systems all connected?

Response: Please see section 4.1 of the RFP.

4. Has the City of Cedar Rapids had a Penetration Test before? If so, were you pleased with the results?

Response: Yes, the City has had some Penetration Tests.

5. Is the required assigned resource in section 4.6.1 to be on-site or can they be a remote?

Response: On-site is not required. If remote please specify this in your proposal submittal.

6. Are there any specific compliance requirements driving the need for these services?

Response: Please see section 4.6.2 of the RFP.

7. For requirement 4.7, can employees in other states provide this support (largely over VPN), and if onsite services are required we could fly someone out within a few days?

Response: The selected Consultant shall have the ability to provide remote support via the City's VPN within one (1) hour. Consultants who are unable to be on site within an hour should note this in their proposal submittal.

8. By IP address testing, we understand you need a live IP scan, for which we will need a VPN connection from our offices to one of your network locations from where all the internal IP addresses can be scanned. Please mention the approximate count of IP addresses or subnet details for estimation.

Response: Items within the required scope of services are detailed in section 4.1 of the RFP.

9. For the 7 apps in the scope, please bifurcate the count of apps for which Black Box only tests are required and for how many Gray Box tests are needed?

Response: The Consultant selected will need to advise and assist.

10. Social Engineering – Would you like to put a target user count or should we propose 100 user spear phishing and sample subset of users for various social engineering attempts?

Response: No response is needed for Social Engineering because the method will be agreed upon at a later date.

11. What is your estimate of total internal IP addresses?

Response: Please see section 4.1 of the RFP.

12. What is the number of users, emails, or phone numbers to be tested?

Response: The Consultant selected will need to advise and assist.

13. Is the City interested in onsite social/physical penetration testing?

Response: Not at this time.

14. Is the intent of the Virtual CISO to have one full time point of contact to create these programs and policies for the City or could these services be provided by various consultants (all coordinated under one vendor)?

Response: The goal is to have one (1) consultant create these programs and policies for the City. However, the City reserves the right to award multiple vendors if deemed to be in the best interest of the City.

15. Is the City looking for a managed security service to provide a full solution to the scope of work?

Response: Yes

16. Will the City consider a vendor who can provide all services with the exception of the requested services outlined in section 4.3.2 c, "Provide notification to City of cyber threats as they develop" to maintain independence over a specific managed service or hardware/software solution.?

Response: The City may consider it. Please specify in your proposal submittal.

17. Does the City currently contract with a managed security services provider?

Response: No

18. Has the City determined a budget for this project? If so, can it be shared?

Response: Please see section 4.1 of the RFP.

19. Does the City have target dates for certain project milestones? If so, can they be shared?

Response: The City does not currently have target dates or project milestones. We are seeking a managed service provider so that the City can utilize the services as soon as possible.

20. Does the City desire that the selected consultant give and/or facilitate presentations during the project? If so, at what milestones and to what audiences?

Response: Unknown at this time.

21. Does the City have a preference for the ratio of on-site versus remote work?

Response: No

22. Can documentation be provided for offsite analysis if needed?

Response: Yes

23. Does the City anticipate the selected consultant will need to meet with the various departments that receive IT support services? If so, with how many departments and at what organizational level (e.g., agency leadership, management, end users) does the City expect the consultant to coordinate these meetings?

Response: The consultant selected will need to advise and assist.

24. Will the City provide a list of the existing core set of policies and procedures currently in place post-award and prior to beginning of onsite work?

Response: Yes, this information will be provided to the selected consultant following award.

25. Is an inventory of systems currently in use available? If so, can that be shared to aid proposers in developing a response?

Response: This information will be shared with the selected consultant following award.

26. Does the City envision that meetings with department staff will be conducted at a central location or at multiple locations throughout the City?

Response: The consultant selected will need to advise and assist.

27. Are there any third-party vendors providing IT or security related services?

Response: No

28. Are there any services in the cloud?

Response: Yes, about a half dozen.

29. Social Engineering is in the scope. Does the City require a physical penetration test through social engineering along with attempted divulging of passwords? If so, do the facilities have armed guards?

Response: No

30. Does the City require vulnerability testing in addition to the penetration tests requested in section 4.3.1 a? If so, will the selected contractor be allowed to use privileged access rights for vulnerability scanning to reduce false positives?

Response: No

31. Does the City desire external vulnerability scanning? If so, how many active external IP addresses are in the scope? How many external web applications are in the scope? What virtual architecture is in use?

Response: Please see section 4.1 of the RFP.

32. For Internal Vulnerability Scanning, how many internal IP addresses/subnets are in the scope? Are internal workstations included? How many internal web applications are in the scope? How many servers, databases, firewalls, routers, and switches? Is virtual architecture in use? What version? Are there any mainframes in the scope? How many databases are in the scope and what type?

Response: The information available is provided in section 4.1 of the RFP.

33. Are Wireless Access Points in the scope and if so, how many locations?

Response: Yes, 43 physical locations.

34. What regulatory standards does the City comply with?

Response: See section 4.3.2 in RFP.

35. Has the City adopted a risk management framework? If so, which one – NIST, ISO, etc.?

Response: NIST, however, the selected consultant will need to advise and assist.

36. Are the City network diagrams current and comprehensive?

Response: Yes

37. Are all services to be performed by one vendor or can specific phases of the engagement be bid on separately?

Response: The goal is to have one consultant create these programs and policies for the City. However, the City reserves the right to award multiple vendors is deemed to be in the best interest of the City.

38. How many IT staff people are currently in the organization?

Response: Approximately 30.

39. How many of the City's IT staff hold a security role or perform an IT security task?

Response: Only a few.

40. Does the City have any other managed security service providers (MSSP) other than the State of Iowa?

Response: No

41. Out of the 200+ applications, how many are accessible remotely?

Response: About half a dozen.

42. Out of the 200+ applications used, how many transmit, process, or store sensitive information?

Response: About have a dozen.

43. Does the City develop internally any of its used applications?

Response: Yes, a few.

44. Is the environment a mix of architectures and configurations or primarily one architecture and configuration, for example, Linux/Windows + Domain/Non-Domain systems or primarily Windows/Active Directory?

Response: Primarily Windows/Active Directory with a few Linux.

45. Would an internal penetration test also be included in the services?

Response: Yes, please detail this and the cost in your proposal submittal.

46. Would this include every single case infection or only if wide spread infection and/or possible network break is assumed?

Response: The selected consultant will need to advise and assist.

47. Will the City reimburse for actual travel expenses when directly related to the project?

Response: Pricing for items included in the Scope of Services shall include all expenses including travel. If additional services are requested by the City outside of the Scope of Services included in this RFP, compensation for travel expenses must be agreed upon in advance by both parties and the City will prepare an amendment to the contract.

48. Does the vulnerability scanning include all IP addresses outside the firewall (external) and inside the firewall (internal)? How many IT assets appear in the report?

Response: Please see section 4.1 of the RFP.

49. How frequent is the scanning process (weekly, monthly, annually)?

Response: The City will consider quarterly and annually. The selected consultant will need to advise and assist.

50. Are the current cloud systems Platform as a Service or Infrastructure as a Service?

Response: Software as a service.

51. Will the City provide a listing of the systems that are cloud hosted and the provider (Azure, AWS, etc.)?

Response: This information will be shared with the selected consultant following award.

52. Will the City provide a breakdown percentage of the operating systems for the server infrastructure (windows systems, Linux systems, UNIX systems, i-series systems)?

Response: Primarily Windows/Active Directory with a few Linux.

53. How many written information security policies and procedures are currently in place?

Response: This information will be shared with the selected consultant following award.

54. How does the City define security information assets?

Response: The selected consultant will need to advise and assist.

55. Are these applications off-the-shelf (OTS) or custom developed? If OTS, can you list the names of the applications?

Response: This information will be shared with the selected consultant following award.

56. Will the City be conducting the vendor risk assessments or is that also part of the intended scope for the RFP for contract award?

Response: This will be part of the scope of services for the selected consultant.

57. How many vendors does the City expect will fall into the scope of vendor risk assessments?

Response: Unknown

58. Is the City requesting a plan only or does it also expect to receive ongoing security monitoring as part of the Scope of Services?

Response: The Scope of Services for the selected consultant will include ongoing security monitoring.

59. If monitoring is required for the RFP response, how many assets are in the scope for monitoring and alerting?

Response: Details regarding the assets the City believes should be in the scope are provided in Section 4.0 of the RFP, however, the selected consultant will need to advise and assist.

All addenda that you receive shall become a part of the contract documents and shall be acknowledged and dated on the bottom of the Signature Page (Attachment C). The deadline for proposal submittal is Friday, March 16, 2018 before 3:00 p.m. CDT.