ADDENDUM #1

To: All Companies Interested in Submitting a Proposal
From: Rebecca Johnson, CPPB, Purchasing Agent
RFP: Managed Security Services (RFP #PUR0917-055); Dated: October 25, 2017
Subject: Addendum #1 (8 pages)
Date: December 15, 2017

PLEASE NOTE
The deadline for submittal of proposals has been extended to Friday, December 29, 2017.
All proposals must be date and time stamped in the Office of the City Clerk
before 3:00 p.m. CST on Friday, December 29, 2017.

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. Question: Does the City of Cedar Rapids currently have any of the following policies and standards defined?

- Patch Management
- Configuration Management
- Mobile and Bring-Your-Own-Device (BYOD) policies
- Incident Response Plan
- Information Security Policy
- Data Classification Policy
- Risk Management Policy
- Vendor Risk Assessment Plan
- Asset Inventory
- Application Inventory

Answer: For Patch Management, Configuration Management, Mobile and BYOD, Incident Response Plan, Information Security, Data Classification, Risk Management and Vendor Risk Assessment Plan the City does have policies but not in a written format. Written policies for each of these are included in the deliverables the City is seeking with this RFP.

Asset Inventory and Application Inventory are currently in process. The City is converting from application catalog to service catalog.

2. Question: How many firewalls does the City manage? What makes/models?

Answer: The City currently manages five (5) firewalls. All are Palo Alto 3000 series.

3. Question: Does the City have a tool for vulnerability scanning? If so, what make/model?

Answer: The City uses Tripwire, managed by the State of Iowa.

4. **Question:** What is the percentage of application environments and systems that are managed in the cloud versus City owned datacenters?

   Answer: 95% are on City premises.

5. **Question:** Will blind bios and qualifications suffice in our proposal, as we are not authorized to provide specifics for our personnel? Will a description of engineer's qualifications and credentials suffice?

   Answer: Yes

6. **Question:** For annual pen testing:
   a) How many hosts are in the scope?
   b) What is the number of Internal and External IPs?
   c) How many Applications will be in the scope?

   Answer:
   a) 12 external hosts
   b) 32 external IPs available (not all used); many internal IPs
   c) Seven (7) Applications including external website hosting, application web server, GIS reverse proxy, citizen self-service portal, OnBase citizen portal, CR Mobile App, and VPN

7. **Question:** The RFP covers several service lines that we can facilitate. If our response to the RFP breaks down the services into their respective categories will it be in alignment with your expectations?

   Answer: Yes

8. **Question:** How many sets of information security policies do you maintain? What sorts of policies do you have today and how are they structured?

   Answer: N/A. the City desires to have new information security polices created.

9. **Question:** What is the size of the City's information security policies (# of pages) and are they mapped to any particular controls standard (ISO, NIST, Cobit, etc.)?

   Answer: N/A. The City desires to have new information security policies created.

10. **Question:** What type of information is of most importance within the organization?

    Answer: Criminal Justice Information Systems (CJIS), Financial Information, Human Resources Information, and PCI

11. **Question:** Describe the City's risk management team and capabilities in place today. Do you have defined risk roles and responsibilities? When was the last time a risk assessment was conducted?

    Answer: N/A. the City is seeking assistance setting up an IT risk management team. The last risk assessment was conducted in 2016 for the SQL Server production environment.

12. **Question:** How large is your organization? (# of employees, # of geographic locations, # of business units)

    Answer: The City currently has approximately 1400 employees located in 43 physical locations. Staff is organized in twelve (12) departments.

13. Question: How many people will the selected consultant need to interview in order to understand the current state of controls on the systems in-scope and what are their job functions?

Answer: The selected consultant shall interview a minimum of five (5) employees including Infrastructure Manager, EAS Manager, Sr. Information Engineer, CIO, and Database Analyst.

14. Question: Briefly describe the City's key business processes.

Answer: To provide services to the citizens of Cedar Rapids.

15. Question: Briefly describe the systems supporting the City's key business processes.

Answer:
a) Number of servers and type (database, AD, file server, etc.) – 200 servers which are 75% virtualized including database, DNS, file, print, AD and applications servers
b) Over 200 applications with various functions
c) There are approximately twelve (12) systems that handle PII data

16. Question: Does the City have an existing Information Security Program? Is this plan based on a specific security framework?

Answer: The City's preferred security framework is NIST.

17. Question: Do information security policies and procedures need to be based on a specific security framework or regulatory standard? If so, please provide a list of the required standards.

Answer: The City's preferred security framework is NIST.

18. Question: What does the City consider to be security information assets (firewall, IDS, etc.)? At a high level, what does the City consider to be the overall asset count for security information assets?

Answer: The City currently manages five (5) firewalls. All are Palo Alto 3000 series.

19. Question: How many systems are in the City's infrastructure? Are they virtualized? If so, what virtualization platform is used? How many physical hosts? How many IP addresses are associated? Is there SAN technology used? If so, what platform?

Answer: The City has 200 servers which are 75% virtualized. The virtualization platform is VMWare. There are twenty-four (24) physical hosts. There are hundreds of associated internal IP addresses. The City used NetApp SAN technology.

20. Question: Please provide the total number of External IPs and External Web apps.

Answer: There are 32 external IPs available (not all used) and seven (7) external web apps.

21. Question: Does the City want internal network penetration testing and if so, how many IP addresses will be tested annually?

Answer: Only external penetration testing is required for this phase of the engagement.

22. Question: What is the City expecting as a deliverable for the executive summary that is due upon execution of contract?

Answer: An executive summary is expected as part of the final deliverable. Upon execution of the contract the City expects the Consultant commence services requested in the RFP.

23. Question: Does the City desire awareness training to accompany the newly developed security policies?

Answer: No. The City is contracting with KnowBe4 to provide the awareness training.

24. Question: Regarding Ongoing Security Monitoring and Alerting, does the City want the consultant to develop a plan, budget, and approach for security monitoring? Or is the City expecting the consultant to quote security monitoring as part of the scope for the RFP response? If so, how many and what types of devices need to be monitored? If the RFP does not include security monitoring, what is the security dashboard for?

Answer: Yes, the City expects the Consultant to develop a plan, budget, and approach for security monitoring as part of the engagement as described in the RFP.

25. Question: Regarding the Incident Response Plan (IRP), is the City expecting the consultant to review the IRP and make recommendations for improvement or asking the consultant to rewrite/create a new IRP?

Answer: The City is expecting the consultant to review the informal plan the City currently has, make recommendations, and provide a formalized plan.

26. Question: What type of incident would require one (1) hour response? How many of these types of incidents have occurred in the past two (2) years? Does the City have flexibility on how the Security Incident response requirement is managed?

Answer: The type of incident that would require a one (1) hour response is one that involves an external attack that could compromise City systems or data. The City has not had any of these types of incidents that we are aware of, which is why the City is seeking a provider to monitor.

27. Question: Does the City currently scan their network? If so, how often and what technology is used?

Answer: No

28. Question: For IP Address Testing, how many IP addresses? Please indicate how many are internal IPs and external IPs.

Answer: 32 external IPs available (not all used); many internal IPs

29. Question: For Application Testing, how many unique URLs, Applications, and User-Roles has the City deemed in scope?

Answer: Seven (7) Applications including external website hosting, application web server, GIS reverse proxy, citizen self-service portal, OnBase citizen portal, CR Mobile App, and VPN

30. Question: Does the City have a preference for the social engineering exercises, whether that be phishing, vishing, or physical intrusions?

Answer: KnowBe4 will be the City's vendor for IT security awareness to provide and conduct training in this area.

31. Question: Has the City ever conducted a gap assessment? If so, what framework was used? Do you have a preference on frameworks?

Answer: No, the City has not conducted a gap assessment. The City's preferred security framework is NIST.

32. Question: Does the City currently have an incident response plan in place? If so, is the plan integrated with the ticketing system? What kind of ticketing system is being used?

Answer: Yes, the City has a plan but it is not documented. The ticketing system is Manage Engine.

33. Question: Approximately how many pages of documentation does the City have in regard to policies as it relates to IT, IT Security and Compliance?

Answer: Approximately 100 pages

34. Question: How many stakeholders will be involved in this project?

Answer: Seven (7) stakeholders (the internal IT team that created this RFP)

35. Question: What is the main objective of the security services for this RFP (audit, compliance, security controls testing, testing current security, weaknesses, establish or mature the current security program)?

Answer: Audit, compliance, security controls testing, testing current security, weaknesses, establish or mature the current security program are all objectives of the security services requested with this RFP.

36. Question: How much time or resources are available for implementation from the City of Cedar Rapids and how much implementation resources will the vendor be expected to provide?

Answer: The City will provide whatever resources are necessary to make this effort successful. However, the intent is to establish a contract with a managed service vendor to handle implementation of the program and maintenance of this function.

37. Question: What percentage of time will the technical resources from the City be available during the engagement to assist in testing or implementation? (for example, dedicated resource or 10% of one (1) person's week)

Answer: The City will implement the security recommendations. The City expects the Consultant to audit, recommend policy/programs, and monitor for security concerns.

38. Question: What types of hosts are included in the scope?

Answer:
a) Servers (versions): Windows Server 2003 through 2016
b) Cloud storage (AWS/Azure/etc.): n/a
c) Workstations (versions): Windows 2007/2010
d) Networking equipment (firewalls, routers, switches, etc.): Firewalls – Palo Alto 3000 series; Routers/Switches – Avaya/Extreme
e) Wireless: Aruba/HP
f) Internet of Things (tablets, mobile devices, medical equipment, research instrumentation, industrial/SCADA equipment): Airwatch MDM
g) Printers: HP/Lanier

39. Question: Please provide more information on the major applications in scope for the City of Cedar Rapids:

Answer:
a) What percentage of the applications are custom versus off the shelf? 10% custom
b) How many web applications are there in scope? 7
c) How many internal applications are in scope? None
d) How are those applications hosted? n/a

40. Question: Should a review of logical and physical access controls be included in our proposal? If so, how much of the infrastructure, processes, technologies, or resources are centralized (shared) or decentralized (distributed)?

Answer: Yes, a review of logical and physical access controls should be included in proposal. The majority of the infrastructure, processes, technologies, or resources are centralized.

41. Question: Should proposals include all social engineering assessments such as: email phishing, phone phishing, spear phishing, whaling, smishing, pharming, and physical access social engineering as part of the social engineering testing scope or should the scope be limited to just email phishing?

Answer: No. The City has a separate vendor for social engineering.

42. Question: Are the penetration tests "blind" red team tests, or will the City provide network diagrams and technical data on the systems to be tested?

Answer: The penetration tests are blind.

43. Question: Please describe the involvement of each of the following stakeholders in the testing processes:

Answer:
a) Executives: None
b) IT: Involved
c) Security: Part of IT
d) Networking: Part of IT
e) Facilities: None
f) Legal: None
g) HR: None
h) Privacy: None

44. Question: Does the City currently have a log collecting/monitoring technology?

Answer: No

45. Question: How many windows AD, DNS, DHCP, and ESX instances do you have?

Answer: AD: 2; DNS/DHCP: 1 distributed network; ESX: 36

46. Question: How many Windows IIS and Exchange Services do you have?

Answer: IIS: 2; Exchange: 2

47. Question: How many Windows general purpose servers do you have?

Answer: 100

48. Question: How many Unix and Linux Servers do you have?

Answer: 6

49. Question: How many Antivirus servers so you have?

Answer: 1

50. Question: How many Database servers do you have?

Answer: 12

51. Question: How many Proxy Servers and Edge Firewalls do you have?

Answer: Proxy Servers: 1; Edge Firewalls: 5

52. Question: How many core and large firewalls do you have?

Answer: 5

53. Question: How many IDS, IPS, VPN, WAF, DAM, DLP, and LB do you own?

Answer: Only VPN: 1

54. Question: How many routers and switches do you have?

Answer: 200

55. Question: How many total workstations do you have on the network?

Answer: 1000

56. Question: How many total servers do you have on the network?

Answer: 200

57. Question: Do you do internal development? If so, how many applications, what type of languages, and what is the approximate size in lines of code per application?

Answer: No internal coding. Any custom coding is outsourced.

58. Question: Do you utilize external organizations to outsource development? If so, how many applications, what type of languages, and what is the approximate size in lines of code per application?

Answer: Yes, the City outsources development. Language is C#. Thousands of lines of code.

59. Question: Do you utilize open source software in your applications and servers?

Answer: No, as a rule; however there are about a half dozen exceptions.

60. Question: Do you require the primary delivery lead to be on location full time? If no, what duration is required and what is desired so that other logistical costs can be considered?

Answer: No. If the work can be accomplished remotely that is preferred.

61. Question: Will you consider scanning software or network routes to be made, allowing scanning over a secure VPN for internal scanning from remote personnel? If yes, do you desire to manage the system yourselves or have the consultant propose the system, and thus include its cost into the solicitation response?

Answer: Yes, VPN scanning will be allowed. You may propose a solution as part of your response.

62. Question: Do you have SIEM, 24x7 Security Operations and Device Management team for which integration of reporting and blue team activities are expected for the vulnerability management?

Answer: No

63. Question: Will the selected consultant be directly responsible for the MOU/ISA development for vendor interconnections? If yes, does the City plan on leveraging their legal representatives to handle the legal considerations of any interconnection agreements?

Answer: Not in Phase 1.

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, December 29, 2017 before 3:00 p.m. CST.