KENAI
City of Kenai | 210 Fidalgo Ave, Kenai, AK 99611-7794 | 907.283.7535 | www.kenai.city

ADDENDA NO. 1

This addenda consists of 12 pages

TO: All Participants

FROM: City of Kenai Public Works Department

DATE: March 25, 2020

SUBJECT: Cybersecurity Audit RFP

DUE DATE: April 2, 2020 at 5:00 PM

Proposers must acknowledge receipt of this Addenda in the appropriate place on the Bid Form. Failure to do so may result in the disqualification or rejection of the bid.

Note: Information in this addenda takes precedence over original information. All other provisions of the document remain unchanged.

The following questions were received through March 24, 2020:

1. Do we need to audit the PC's and laptops for compliance?
    a. The City will defer to the expertise of the proposer.
2. We understand that WebApp Scanning, Code Scan, Database Scan is not part of the scope, is this true?
    a. That is correct
3. We understand that Social Engineering is not in scope , Is this true?
    a. That is correct

4. Please provide us the device count by Network Device that are in scope (Firewall, Router, Switches, IDS/IPS etc)
    a. Please see section A.1
5. Please provide count of servers, would sampling be ok for servers.
    a. Please see section A.1
6. For Physical security, do we need to audit all 9 sites or if the processes are the same across all can we take a sample set.
    a. A sample set would be acceptable
7. Do we need to be contracted with the City of Kenai to apply?
    a. You do not need to be contracted to apply, however the successful applicant will need to be contracted before work can begin.
8. Given the impact of the COVID-19 pandemic, does the City anticipate the timeline shifting? If yes, what will be the revised dates for Notice to Proceed, work completion, etc.?
    a. The timeline is not currently changing. Given the current health crisis nationwide, some changes may be necessary in the future.
9. Given the impact of the COVID-19 pandemic on travel, does the City anticipate that remote data gathering techniques will be necessary to conduct the work?
    a. This is not known at this time
10. Since the Nationwide Cybersecurity Review (NCSR) leverages the NIST Cybersecurity Framework (NIST CSF) as the guiding industry-neutral cybersecurity best practice standard, is it expected that the vendor should audit the City using the NIST CSF?
    a. The City has selected CIS Control version 7.1 for the framework.
11. What is the number of IT policies and documented standard operating procedures (SOPs) that are currently in existence?
    a. Very few that are actually formalized. For the purposes of this response, assume that no policies currently exist.

12. Is it expected that the vendor assist with the creation of policies and procedures that are needed as part of this proposal? Or will the creation of policies and procedures be a separate engagement once the number of deficient policies and procedures is determined?

    a. It is expected that the vendor assist with the creation of policies and procedures as part of this engagement.

13. Does the City require network penetration testing in order to audit the network security? If yes, please provide the number of external target IP addresses, internal target IP addresses, and number of distinct SSIDs that make up the wireless networks in scope.

    a. The City will defer to the expertise of the proposer.

    b. Please see section A.1

14. What is the number of facilities that would need to be visited as part of the physical security review?

    a. Please see section A.1

    b. A representative sample would be acceptable.

15. Is all of IT centralized at City Hall or is it decentralized with “shadow IT” operations in various departments?

    a. IT is centralized at City Hall. Several departments are responsible for maintaining their own applications.

16. Does the City utilize third-party IT support providers or cloud-based service providers for management and administration of any aspect of IT operations? (e.g., AWS for server hosting, Dell for firewall monitoring, etc.) If yes, please list out name and purpose.

    a. Not at this time

17. How many FTE IT staff are there at the City? (Please list out position type and number of staff. E.g., Network Administrator – 1, Help Desk Technicians – 2, etc.)

    a. The city has a single IT Manager position.

18. In regards to your RFP request for a cybersecurity audit, are you accepting out of state offers or will this RFP require an Alaska business license?
    a. Out of state vendors will be considered.
    b. The successful contractor will need to comply with all state and local laws and regulations.
19. Number of Buildings that will covered by physical security
    a. Please see section A.1
20. Number of networks
    a. Please see section A.1
21. Number of Firewalls
    a. Please see section A.1
22. Number of External IP's to scan
    a. Please see section A.1
23. Number of Websites to Scan
    a. Please see section A.1
24. Number on Internal IP's to scan.
    a. Please see section A.1
25. Number of cloud based applications.
    a. Please see section A.1
26. Does the vendor have to be located in Kenai or Alaska?
    a. No
27. If not, are there any additional requirements if the vendor is out of state?
    a. No

28. Is there currently an incumbent company or previous incumbent, who completed similar contract performing these services?

    a. There is no incumbent company.

29. If so - can you please provide incumbent contract number, dollar value and period of performance?

    a. N/A

30. Are you satisfied with incumbent performance?

    a. N/A

31. Does this opportunity contain local preference? If yes, please provide the details.

    a. No

32. What is the budget of this opportunity? Is Budget approved?

    a. This project is being funded by a grant from the Department of Homeland Security for $35,000.

33. Can you please provide current number of users and infrastructure details? (VMWare, MAN, # of Servers, # of Workstations)

    a. See section A.1

34. Are any cloud providers used? Do you manage your own datacenter, or do you utilize any 3rd-party/colocation facilities?

    a. We manage our own datacenter, and do no use cloud hosting at this time.

35. Are any vendor products installed for Governance, Risk, and Compliance (GRC) tracking?

    a. No

36. How often are information security policies updated? When it was updated last time?

    a. N/A

37. What is the number of wireless controllers supporting the organization wireless networks?

a. Please see section A.1

38. Are IoT devices included as “assets” on the network?

    a. No

39. Are any vendor products installed for Security Incident & Event Management (SIEM)? If yes, please provide currently used SIEM product name.

    a. No

40. Is external network testing in scope? If yes, how many IP addresses, how many Web application?

    a. Please see section A.1

41. How many systems are on internal network?

    a. Please see section A.1

42. How many Active Directory Domains are in place?

    a. Please see section A.1

43. How many servers, workstations, firewalls and other networking devices? We may use sampling for configuration review based on number and function of the system (Web server, file server, app server, database, firewall (int/ext), VPN, Load Balancer etc).

    a. Please see section A.1

44. Do you want Black/Grey box testing (where we have physical access to the network but no credentials)? Or Whitebox testing, where your team provide necessary documents and credentials for the testing?

    a. The City will defer to the expertise of the proposer.

45. Do you want this as a red team exercise to test the SOC/NOC’s response where they will get to see the results and update their Knowledge Base (KB) afterward or Blue team where we work with the SOC/NOC and share our attacks so they can update their KB during the testing?

a. The City will defer to the expertise of the proposer.

46. How many physical locations?

    a. Please see section A.1

47. Do we get remote access for the internal testing?

    a. Remote access can be arranged.

48. Please provide number of application, External facing (internet accessible) or Internal facing?

    a. Please see section A.1

49. What testing would be required Credential testing or non-credential testing? If credential testing require then how many different roles would be there?

    a. There would be 3-5 roles.

50. Will it be hosted on-premise or on cloud?

    a. The City will defer to the expertise of the proposer.

51. Will it be managed in-house or outsourced?

    a. Management of this project will be conducted by City employees

52. Due to the current pandemic, it might be necessary for all staff to work from home. To accommodate this, is it possible for bidders to submit proposals via email rather than hard copy?

    a. Please see section A.2

53. Is the cybersecurity assessment limited to items listed in the RFP, or would the City want a full review of all cybersecurity/IT general controls?

    a. The City will defer to the expertise of the proposer.

54. Is the City looking for detailed configuration of the listed devices (routers, switches, cameras, wireless equipment, printers, copiers)? If so, could the City please provide the quantities of each device type to be assessed?

a. Please see section A.1

55. What operating systems are to be included in the testing?

    a. Please see section A.1

56. Are external/internal network vulnerability assessments included?

    a. The City will defer to the expertise of the proposer.

57. Is a network architecture review included?

    a. The City will defer to the expertise of the proposer.

58. How many firewalls need to be reviewed? Are any paired/in HA mode?

    a. We have 1 firewall

59. Is the City looking for a full wireless network security assessment/penetration test or just a wireless architecture review?

    a. The City will defer to the expertise of the proposer.

60. Assuming that the wireless network is controller-based, how many controllers are in scope?

    a. Please see section A.1

61. Is the City looking for a detailed review of the Disaster Recovery plan?

    a. Yes

62. Could the City please provide the number of locations for physical security review?

    a. Please see section A.1

63. Could the City share the budget for this project?

    a. This project is being funded by a grant from the Department of Homeland Security for $35,000.

64. Is there an incumbent, or is this a new requirement?

    a. There is no incumbent

65. If there is an incumbent, can the City please provide the incumbent firm's name and the contract value?

    a. N/A

66. Is the City currently aligned with a security/best practices framework, such as the NIST Cybersecurity Framework, NIST Special Publication 800-53, ISO 27001/27002, or the CIS 20 Critical Security Controls? If so, could the City please specify which framework?

    a. The City has selected CIS Control version 7.1 for the framework.

67. Approximately how many IT security policies and procedures does the City have formally documented?

    a. Very few that are actually formalized. For the purposes of this response, assume that no policies currently exist.

Section A

A.1 This is a list of facilities, devices, addresses

- Servers
    - Physical – 7
        - vmHosts – 3
        - Backup
        - Phone Server
        - Wowza
        - CCTV
    - Virtual – 49
- Workstations – 150
- SAN – 1
- Routers – 2
- Switches – 45
- Firewall – 1
- WiFi
    - Controller – 1
    - Access Points – 14
    - SSID – 3
- Voice Gateway – 8
- Active Directory Domains – 3
- External IP addresses – 16

- Cloud applications – 5
- Websites – 5
- Internal IP addresses – 500
- Cameras – 80
- Operating Systems
    - Windows 10 Enterprise
    - Debian Linux
- Sites
    - Major Sites – 10
        - City Hall
        - Public Safety
        - Library
        - Senior Center
        - Airport
        - Airport Operations
        - Parks & Rec
        - City Shop
        - Waste Water Treatment Plant
        - Water Treatment Facility
    - Minor Sites - 11
        - Well house
        - Reservoir

- Dipnet locations – 4
- Cameras – 5

A.2 Section 2.6 is amended to the following:

2.6 Proposal Submission

Four (4) copies of the Technical Proposal are to be submitted to the City of Kenai Public Works Department at 210 Fidalgo Avenue, Kenai, AK 99611, along with one (1) copy of the Fee Schedule in a separate sealed envelope. These five (5) documents shall be submitted in a sealed envelope clearly marked with the proposer's and RFP name.

At the discretion of the proposer, proposals may be submitted via email. Please email proposals to publicworks@kenai.city. The subject of the message must be "Cybersecurity Audit RFP Submission." Submissions must be provided in a PDF file format. As email is not a secure communication method, confidentiality of emailed submissions cannot be guaranteed.

{Deleted text is bracketed}. New text is underlined.