Village of Oak Park Cyber Security Assessment RFP

Addendum 1 – Questions and Answers

Issued 2-17-2023

Q1. Is this a single-award or multiple-award contract?
A1. Single.

Q2. What is the anticipated date of award and contract execution?
A2. The date will be determined after vendor is selected, final cost of the project determined and funds appropriated.

Q3. What is the duration of the project?
A3. Not to extend past 3 months.

Q4. What is the total number of man-hours required for this project?
A4. We leave this is up to vendor to decide based on our requested scope of work.

Q5. What is the anticipated timeline for this project?
A5. We leave up to vendor to work out project timeline.

Q6. Do we need to provide resumes for the proposed labor categories?
A6. Yes.

Q7. If resumes are required, do these resumes need to be live or sample?
A7. Resumes should reflect up-to-date qualifications of the personnel assigned to the project.

Q8. If resumes are not required, do we need to only provide the pay rates for the proposed labor categories?
A8. Please provide labor rates for categories involved in the project.

Q9. Will there be interviews post-evaluation?
A9. Only if originally assigned personnel is not available and are being substituted.

Q10. If interviews are scheduled, will it be for the resource personnel only or for a team from the company including a company representative?
A10. Resources and assigned project manager(s).

Q11. Will vendor selection interviews be conducted in person or remotely?
A11. Either.

Q12. If in-person interviews are scheduled, can the client allow us to participate virtually?
A12. Yes.

Q13. Considering the current COVID-19 pandemic situation, if the proposed candidates are not available at the time of award, will the agency allow us to provide replacement personnel with similar or more skill sets?
A13. Yes, but provide resumes and list of engagements first. Village reserves the right to interview replacements.

Q14. If we are shortlisted for the interview and if our proposed personnel are not available at that time, can we propose alternate resources for the interview?
A14. Interviews would be held with personnel directly assigned to the project.

Q15. Could you please clarify the budget for this opportunity?
A15. Budget is flexible. Initial budgeted amount is $35,000 with additional funding under consideration.

Q16. Does Oak Park want an assessment specifically against the NIST Cybersecurity Framework AND the CIS Critical Security Controls frameworks?
A16. At this time Village does not adhere to a particular standard and is looking for recommendations all things considered.

Q17. Can all internal target systems and subnets be accessible from a single location or will travel to other facilities be necessary for the internal vulnerability assessment and penetration testing?
A17. Can be accessed from one location but to note that all Village sites are 5-15 min away from each other.

Q18. Is traffic from all four SSIDs accessible from a single location or will travel to other facilities be necessary for the wireless network vulnerability assessment and penetration testing?
A18. Can be accessed from one location but to note that all Village sites are 5-15 min away from each other.

Q19. Under Deliverables IV.3, does Oak Park want the consultant to assess the IT environment and controls against all control statements/requirements under PCI DSS (232 approx. controls), HIPAA (60 approx. requirements under the Security Rule), and CJIS? Doing so will add considerable effort, time, and fees to the engagement.
A19. As noted in RFP, deliverables should be listed each as line item costs. This will allow Village to evaluate, prioritize and seek additional funding as needed. Note: Village does not store credit card data.

Q20. For the Social Engineering component, does Oak Park have a preference as to the type of social engineering desired? This could be email-based phishing attacks, phone-based impersonation/vishing attacks, and/or physical site penetration testing.
A20. One campaign of each.

Q21. What is the number of email campaigns desired if phishing attack testing was to be included in scope? (One campaign equals one targeted email blast to a group of email accounts.)
A21. One.

Q22. What is the number of vishing campaigns desired if vishing attack testing was to be included in scope? (One campaign equals a single script developed for a group of target individuals.)
A22. One.

Q23. What is the number of facilities that would be in scope if physical site penetration testing is desired?
A23. One.

Q24. For IV.9 Advanced Persistent Threat, “Assess the current environment for indications of an existing breach.” Is there a specific time period that Oak Park wants us to review? And are there system logs during that time frame that would need to be reviewed to identify an existing breach?
A24. This item is contingent upon working findings. If during assessment possible previous breach is found or suspected then those findings should be evaluated further.

Q25. For IV.10-IV.12, development of separate policy documents is seen as a separate engagement requiring additional effort, time, and fees beyond the initial assessment. Does Oak Park want these documents developed as part of remediation activities following the assessment?
A25. Please scope cost of development of these documents as line items in the proposal.

Q26.What is Oak Park's budget for this engagement? We want to make sure it is right sized given all that is being requested.
A26. Please see answer A15.

Q27. Exact External IP Count:
A27. 28

Q28. Exact Internal IP Count:
A28. Can't provide exact number as it is dynamic. Best estimate is about 650

Q29. Total Forest count?
A29. One.

Q30. Total number of users?
A30. About 375

Q31. Has the organization ever had a cybersecurity assessment or audit completed in the past?
A31. No.

Q32. Is the start date of March/April of 2023 found on page 2 of the RFP a hard start requirement?
A32. Village recognizes broad scope of the project and is flexible with timing.

Q33. Page 2 under section "Award Of Contract" states "The contract period commences on the date the Professional Services Agreement in substantially the form attached is fully executed and will end when the services are completed."
a. Does the Village have an anticipated completion date for all assessments?
b. Does the Village have an anticipated completion date for reporting?
A33. We do not have set dates but whole project should not take more than 3 months to complete.

Q34. For the Social Engineering Tests: which tests would the Village like to be conducted? (phishing, vishing, etc.)
A34. One campaign of each type phishing and vishing.

Q34a. How many staff would the Village like to be tested?
A34a. 10% for phishing campaign, 3% for vishing.

Q35. Regarding Scope item IV.3: Please clarify the expectations for this scope item:
Are assessments for PCI, HIPAA, and CJIS all in scope and to be priced?
A35. Yes, each as separate line item.

Q36. Does the City want separate reporting deliverables for each regulatory compliance assessment, or will a single report be acceptable?
A36. As we asking each compliance assessment priced separately, reports should be separate appropriately.

Q37. How many sites are in scope for the HIPAA compliance assessment, and is this for both privacy and security rule?
A37. One site. Security rule only.

Q38. How many credit card transactions does your organization processes each year?
A38. PCI Level 3

Q38a. If under 6 million, is the City requiring a QSA to perform the PCI compliance?
A38a. Village wants to set baseline and for best practices perform internal scans.

Q39. Regarding scope items IV.8 and IV.5: Please elaborate on the difference between these two scope items.
A39. IV.5 implies remote users, contractors and vendors access on as-needed basis. IV.8 Implies always-on site-to-site VPN's, data transfers between self-hosted and cloud applications These two scope items can be combined.

Q40. Regarding scope item IV.7: Please confirm the requested social engineering is intended to be email phishing.
A40. Phishing is one of the desired social engineering tests.

Q40a. How many targets will be in scope?
A40a. 10% of the users.

Q40b. What kind of social engineering would the City consider to be in scope and how many targets?
A40b. Other type of social engineering would be vishing (3% of the users) and one site for physical access test.

Q40. Regarding scope item IV.4: How many sites are in scope?
A40. One.

Q41. Regarding scope item IV: Please provide clarification: How many such DMZs are in scope for the vulnerability assessment?
A41. One.

Q42. Regarding scope items IV.13.1 – IV.13.14: Please confirm if a single cumulative findings report is desired, covering all tasks, or if separate reports are desired?
A42. No preference.

Q43. Would the City consider an extension of the deadline to allow responders to accommodate answers to questions in our responses?
A43. Not at this time.

Q44. Are there any web applications in scope for this project, perhaps as a component of scope item IV.1a?
A44. Web applications or code review is not part of this project.

Q45. How many people are on the IT team? Is there a dedicated cybersecurity team or individual?
A45. Department consists of 6 and no.

Q46. Does the Village have existing Cyber Security Policies and procedures?
A46. No – it is part of this RFP to develop those.

Q47. Has the Village previously had a cyber security assessment performed?
A47. No.

Q48. Is there a budget or not to exceed dollar amount for this assessment?
A48. Final amount will be appropriated once Village selects vendor.

Q49. Are the cloud SaaS applications in scope for this engagement?
A49. No.

Q50. If so, what cloud environments do you currently utilize? (select all that apply)
A50. Not applicable.

a. Amazon Web Services ☐
b. Microsoft Azure ☐

c. Google Cloud Platform ☐
d. Other (please specify):

Q51. Please confirm the total number of internal network IP addresses to be tested (if providing an IP ranges, please indicate the estimated number of live Ips).
A51. About 650

Q52. We perform many internal network penetration tests remotely. Is remote testing of the Village's internal networks acceptable?
A52. This can be discussed.

Q53. For internal network testing, how many locations are the systems to be tested located over?
A53. Question not clear. We have 10 main interconnected sites.

Q54. For internal network testing, is access to all sites possible from a single location?
A54. Yes.

Q55. How many physical locations are included in scope for the Physical Assessment activities?
A55. One.

Q56. How many physical locations are included in scope for the Wireless Assessment?
A56. SSID distribution is uniform. All can be tested from any one site.

Q57. How many WAPs and SSIDs are at each location?
A57. Depends on the size of the site. From 1 to 10.

Q58. Does the Village use any endpoint detection (EDR/XDR) software?
A58. No

Q59. Approximately how many external partners does the Village connect to?
A59. 6

Q60. For the Active Directory assessment:

Q60a. How many forests/domains require review?
A60a. One.

Q60b. Approximately how many active users are on the domain?
Q60b. 450 (includes all accounts)

Q60c. How many Groups?
A60c. 569

Q61. Which locations have wireless networks?
A61. SSID distribution is uniform. All can be tested from any one site.

Q62. For Physical access review, how many locations are in scope?
A63. One.

Q63. Does the City want the assessment to include 100% of the devices or is a sampling methodology acceptable?
A63. For workstations sampling is sufficient.

Q64. For remote access review, is the village expecting to review the configuration file for the VPN applicance?
A64. Expectation is to review configuration of different platforms that construct whole process.

Q65. For Internet access review, is the Village expecting to review the configuration of the email/web filtering platform?
A65. Expectation is to review configuration of multiple elements that comprise email/web filtering flow.

Q66. Can you list what platform/tool is used for the same?
A66. Multiple. Detailed information will be provided to selected vendor.

Q67. What types of Social Engineering assessments are acceptable? Phishing, Phone calls (Vishing), Branch impersonation (physical infiltration), road apple?
A66. Phishing, vishing, physical.

Q68. For Phishing – How many scenarios are to be considered and what would be the number of email addresses to target
A68. One scenario. 10% of the users.

Q69. For Vishing, we use a sampling methodology to call no more than 10 employees. Is this acceptable or should the sample size be larger?
A69. Acceptable.

Q70. For Physical impersonation, how many locations/branches would be in scope?
A70. One.

Q71. Can you elaborate on what is expected out of “Connections to External Partners”. Is it to review the Village’s WAN and VPN configuration?
A71. Configuration and protocols used.

Q72. For endpoint protection report, can you list which Anti-Virus or EDR platform is currently being used?
A72. Sophos.

Q73. Are there any Web Applications to be tested in scope? If so, are there any applications needing authenticated testing?
A73. Please see answer A44.

Q74. For Advance Persistent threats, can you list they type of SIEM platform being used and if the Village will provide us with Logs and other reports to assess indicators of compromise?
Q74. Village will use best effort to provide logs and any pertaining information if such need arises.

Q75. Kindly confirm if we can provide our NMSDC certification in reference to the vendor’s minority proof.
A75. All forms required for submittal are included as part of RFP.

Q76. Please explain what the village expects in response to “Annotated listing of publications reports, etc. of prior research work or needs assessments”. Are we expected to provide the sample reports of the previously conducted assessments and pen tests?
A76. Provide list of similar deliverables your company provided from previous engagements to comparable municipalities/agencies.

Q77. Is there any local preference given to the IL vendors?
A77. Please refer to RFP part VI.A.2

Q78. How many vendors Village intend to award?
A78. One.

Q79. What is the budget of the contract?
A79. Please see answer A15.

Q80. Is this a new contract? If not, what was the previous spending of the same, enlist the name of incumbents.
A80. New.

Q81. “evaluate Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA) and Criminal Justice Information Services (CJIS) compliance.”
Reference to above, Do you expect VAPT assessment to include PCI ASV (Approved Scanning Vendor) scanning. If so, could you please provide external IPs to perform ASV scan.
A81. Yes. Detailed information will be provided to selected vendor.

Q82. “Wireless systems to include access points from all Service. Set Identifiers (SSID’s) and their encryption levels;”
Reference to above, we assume that 21 wireless access points, 4 wireless SSID’s from single location/building. If not, kindly let us know if these areas are dispersed among facilities
A82. SSID distribution is uniform. All can be tested from any one site.

Q83. “Review and testing of physical access controls to IT infrastructure.”
Reference to above, which physical access control aspects must be addressed in full? The assessment for physical access is included in the data centre. In such case, co-hosted or internal DC?
A83. Internal

Q84. “An architecture report identifying flaws with the current overall security architecture and provide mitigation plan”
Reference to the above, will a complete network diagram/map be provided or will this report be based purely based on the flaws identified during the assessment?
A84. Combination of both.

Q85. IV.2 -> AD User Access Review -> How many Users, OU's, and if they have any more details regarding their goals and expectations?
A85. Please see answer to Q60.

Q86. IV.3 -> The only one we can consider is the HIPAA Compliance Assessment. Would that take us out of the running if we weren’t able to perform the other standards?
A86. Village will consider all submitted proposals.

Q87. IV.10 -> -> What type of policies would you want to be included so we can determine how many and what standards would they want the policies based on so we can accurately determine the Level of Effort for pricing. ISO, NIST, etc.?
A87. Please see answer to Q16.