CYBER RISK ADDENDUM

VENDOR QUESTIONS AND ANSWERS

Village staff received the following questions from Vendors. Staff answered these questions to the best of their ability.

1. How many users do you have in Entra/AD?
   178 ENTRA / 197 ACTIVE DIRECTORY

2. Will all the sites be accessible from one location for the scan?
   YES

3. Will we be granted admin access to AD/Entra, or is the check expected to be performed during working sessions with your employees?
   GRANTED ADMIN ACCESS

4. How many policies and procedures are there currently in place covering the items under 2E (Risk evaluation areas)?
   NONE

5. Page 7 mentions payment schedule. They do not seem to apply to the scope of this project, i.e. users and data migration. Could you give us more information?
   ADDENDUM CREATED – 100% payment upon completion

6. Are there any existing security frameworks (e.g., NIST, CIS) currently in use by the Village that the evaluation should align with?
   PCI?, NOT CURRENTLY

7. Will prior assessments, security policies, or reports be provided as a reference for the gap analysis?
   THIS THE FIRST OFFICAL ASSESSMENT.
   ALL MATERIALS TO ASSIST WILL BE PROVIDED

8. Are there any known restrictions or configurations on the network that may impact the vulnerability scan (e.g., segmented VLANs or restricted access)?
   VLAN, SEGMENTATION

9. What tools or platforms are preferred for performing the vulnerability scan, if any (e.g., Nessus, Qualys)?
   UP TO VENDOR

10. Are there additional compliance requirements (e.g., CJIS, federal or state-level mandates) beyond those stated in the RFP?
    CJIS

CYBER RISK ADDENDUM

11. Will the assessment include testing compliance with specific standards or regulations?
    VILLAGE STAFF WELCOMES VENDOR RECOMMENDATION

12. Should the cybersecurity risk assessment be aligned with a specific framework (e.g., NIST CSF, NIST SP 800-53, CIS Controls, etc.)?
    Purpose of RFP

13. Does the Village have a formal, documented set of IT security policies and procedures? When were the policies last updated?
    Formal NO – Policies and procedures YES, 5 years since last review

14. How many IT staff members does the Village have?
    2

15. What is the budget for this project?
    PLEASE PRESNET YOUR BEST SOLUTION WHICH MEETS THE REQUIREMENTS

16. Does the Village want the vendor to attempt to exploit vulnerabilities discovered during the network security assessment?
    NO
17. Does the Village want a full CJIS compliance assessment, or should vendors just assess the Village's compliance when/where applicable?
    VILLAGE STAFF IS NOT SURE WHAT IS MENT BY A SELECTIVE CJIS ASSESSMENT PLEASE PROVIDE CLAIFICATION

18. Can vendors provide a sample report for the Village in an appendix?
    YES

19. Is the Village currently aligned with a security framework, such as the NIST CSF or the CIS Controls?
    NO

20. Quantity of active External IP addresses in scope for this effort.
    25

21. Quantity of Domains / Forests.
    1

22. Quantity of accounts.
    178

CYBER RISK ADDENDUM

23. Quantity of Domain Controllers. **2**

24. Is there a particular framework (i.e., CISA, CIS, NIST…) that the Village of North Aurora prefers to align with? **No**

25. How deeply would the Village of North Aurora like to dive into Entra ID? We can go as light as checking Entra ID Connect Sync or as heavy as checking that hybrid device join (including BYOD) are working as intended and get into conditional access polices and privileged accounts assessment. A good blanket way to ask this is "what would you like for us to focus as applicable to Entra ID?".
    THE VILLAGE WANTS TO ENSRUE WE ARE IN THE BEST POSSBILE SHAPE

26. Quantity of active Internal devices / IP addresses in scope for this effort.
    230 (ESTIMATE)

27. How many group policies are currently in place
    42

28. Regarding the Risk Evaluation section, can additional information be provided regarding expectations for the policies and procedures reviews?
    VILLAGE STAFF WANTS TO ENSURE WE HAVE THE REQUIRED AND NECESSARY POLICIES IN PLACE
29. Is the setup hybrid (integrated with on-prem AD) or fully cloud-based?
    HYBRID SYSTEM
30. Does Azure AD integrate with other systems
    YES
31. Have the AD and Azure AD setups been regularly audited in the past, or would this be a first-time review?
    FIRST REVIEW
32. Are there specific expectations regarding auditing tools to be used?
    UP TO VENDOR

33. Should built-in Microsoft tools (e.g., PowerShell, Azure AD Portal) be utilized, or would the Village prefer third-party tools like Quest, Netwrix, or ADAudit Plus?
    UP TO VENDOR
34. What is the approximate size of the directory structure, including details such as domains and organizational units?
    51 Organization Units
35. Does North Aurora require internal penetration testing, or jus vulnerability scanning
    BOTH

CYBER RISK ADDENDUM

36. Does North Aurora want Microsoft 365 configuration included in the assessment effort?
    YES
37. With the Thanksgiving Holiday next week, would North Aurora consider a 1-week extension to the due date?
    NO
38. How many employees does your company employ?
    76
39. How many Security staff members does the company employ?
    0
40. Does the organization undergo any third-party security attestations (i.e., SOC 2, PCI-DSS, etc.)?
    PCI
41. Does the organization have an existing written information security policy?
    NOT FORMAL
42. What are the types of hosts being scanned (Windows, Linux, Mac)?
    WINDOWS, LINUX
43. Are there any trusts setup between forests?
    NO
44. How many server endpoints will be considered in scope?
    9 WINDOW SERVERS, 1 CCTV, 1 DOOR ACCESS

45. Are there any Certificate Authorities in the environment?
    UNKNOWN
46. Does the security audit consist of on-prem resources only or does this extend in to Entra ID?
    BOTH
47. Can you confirm the number of internal VLANs, public IP addresses, and virtual machines expected to be included in the vulnerability assessment?
    230 IP estimate
    12 VLAN
    25 PUBLIC IP (6 actively being used)

48. What is the expected frequency of project status meetings?
    WEEKLY EMAIL IS SUFFICENT, BENCHMARK MEETINGS WHEN NEEDED

CYBER RISK ADDENDUM

49. Can this engagement be conducted entirely remotely?
    YES, AS LONG AS REMOTE CONNEDCTION IS FROM WITHIN CONTINENTAL UNITED STATES AND PERSON HAS SECRUITY BACKGROUND CHECK/CJIS COMPLANCE

50. How does the Village define "sufficient knowledge transfer"? Are there specific types of training or documentation that need to be provided?
    PROVIDING A DETAIL REPORT OF FINDING, NEXT STEPS, RECOMMENDATIONS AND REVIEW OF REPORT

51. Will there be a working session with all submitters to clarify answers to questions verbally, inclusive of the Aurora teams that we'll be interfacing with?
    ALL SUBMITTER PROPOSALS – NO (proposals not meeting the requirements, reference checks, etc., will be eliminated

52. What evidence of CJIS compliance do you require?
    I am not sure what options are available.

53. What evidence of CJIS compliance do you require? I am not sure what options are available.
    NO
54. Should the cost for the tools used be added to the cost section for the hardware and software costs to be incurred during this project?
    YES
55. Would we be given access to modify ACL's or would it be a change request from us to the IT team to make this happen? This will help with our time estimation.
    ADMIN ACCESS
56. We see one vcenter host, the question is there any other additional should we consider?
    NO
57. Is there a preferred format or template for the proposal submission beyond the sections outlined?
    NO
58. Do we have exception process for VM scanning?
    vulnerability identified during a virtual machine (VM) scan will not be immediately remediated
59. Are there any critical assets or sensitive data that need prioritized protection?
    NO
60. Are pre-scan and post scan notifications to be sent to support teams (Server / Application owners)?
    YES - POSSIBLE EXCEPTION IS NON-INTRUSIVE SCAN EXECUTED ACCORDING TO PREDETERMINED SCHEDULE

CYBER RISK ADDENDUM

61. Can the firm start in less than 4 years but each of the members has 15 years of information security experience bid for this project?
    YES
62. Is there any requirement around visa status (Citizens / Green card holders/ H1B visa holders) within US only to be placed for this project
    MUST BE US CITIZEN OR HAVE CJIS SECURITY CLEARANCE, ADDITIONAL SECURITY BACKGROUND CHECK MAY BE PERFORMED BY NORTH AURORA POLICE
63. Does the firm have to be registered in IL? If we are getting the project we will open one in IL but do let us know if that is mandatory or not?
    NO
64. Are there specific criteria for the reference projects that should be included in the proposal?
    NO SPECIFIC CRITERIA (PREVIOUS US GOVERNMENT PROJECTS PREFERRED)
65. Similar Services provided is clear, but does it required to have the same size as well?
    SIMILAR SERVICES YES, SIZE NO
66. What is the process for obtaining consent for subcontracting, and are there any limitations on the types of services that can be subcontracted?
    A WRITTEN STATEMENT PROVIDED TO VILLAGE STAFF, MUST MEET SECURITY REQUIREMENTS
67. How should change orders be documented, and what is the timeline for approval once identified to perform the scans/assessments?
    CHANGE ORDERS WILL BE SUBMITTED IN WRITING AND MUST BE APPROVED BY VILLAGE PROJECT MANAGER. NEXT BUSINESS DAY APPROVAL
68. Will there be additional points of contact within the Village for different aspects of the project, or will all communications go through the designated Project Manager?
    DESIGNATGED PROJECT MANAGER
69. Which format of the reports (CSV, PDF, XLS) are shared?
    VARIOUS
70. How are the reports shared
    MICROSOFT TEAMS/SHAREPOINT PREFERRED
71. Who will be the Stakeholder to receive the reports?
    PROJECT MANAGER
72. Do we maintain a POC tracker for Platform support team for remediations?
    NO
73. How are the remediation activities tracked and reported? Is there any specific tool used for tracking and reporting?
    THIS RFP IS FOR AN ASSESSMENT ONLY, NO REMEDATION
74. Do we have any SLA for Vulnerability Management?
    THIS RFP IS FOR AN ASSESSMENT ONLY, NO REMEDATION
75. What are the customers' main goals for the vulnerability management program?
    THIS RFP IS FOR AN ASSESSMENT ONLY, NO REMEDATION
76. Are there specific outcomes or timelines they are targeting?
    NO

CYBER RISK ADDENDUM

77. Is there a scoring chart on how the vendors are scored?
    NO
78. Is there a not-to-exceed budget for this project that you can share?
    PLEASE PRESNET YOUR BEST SOLUTION WHICH MEETS THE REQUIREMENTS
79. When you say “network scan and vulnerability assessment”, we understand that you are not looking for a full penetration test but rather only a scan. Is that correct?
    CORRECT
80. We understand that apart from the external and internal network vulnerability assessments, no other type is in scope, e.g. no wireless, web application, social engineering, etc. are in scope. Can you please confirm?

WIRELESS POLICY, RULES, SETTINGS AND CONFIGURATION REVIEW

81. Can you confirm how many facilities/locations are in scope? Also, where are they all located (distance from each other)? Can a large part of the project be performed remotely or is on-site performance mandatory?
    FIVE PHYSICAL FACILITIES, ALL WITH IN TWO MILE RADIUS, ALL LOCATIONS CAN BE ACCESSED FROM A SINGLE LOCATION
82. Please provide a high-level description of your overall technical operations and sensitive information/data flow so that we are able to assess the size and complexity of the engagement.
    VILLAGE CURRENLTY DOES NOT IMPLEMENT DATA CONTROL SETTINGS.
83.