NETWORK PENTETRATION TEST Q&A

Q&A 1

1. Section 4.7: What time(s) of day is permitted for the Web Application Penetration Testing? Any time as long as we are aware of ongoing testing.
2. Section 4.9:
    - a. What time(s) of day is permitted for the Physical Security Assessment? Office hours of 8:30 a.m. – 4:30 p.m.
    - b. Would it be preferred to perform the Physical Security Assessment with the onsite Network Security Assessment/Internal Network Testing? No preference.
3. Section 4.10: What time(s) of day is permitted for Social Engineering Campaigns? Business hours of 8:30 a.m. – 4:30 p.m.

Q&A 2

1. Is this the first time you will be contracting for this work? If not, please provide the name of the incumbent contractor and a copy of the contract. Yes
2. Is there any budget and/or a not-to-exceed budget figure that you can share? None are publicly available.
3. Would you consider offering the option of electronic submission of the proposal response?
4. For the external network penetration test, of the 30 IP addresses you mention, approximately how many will be live? All
5. For the internal network penetration test, of the 500 IP addresses you mention, approximately how many will be live? All
6. For the physical security assessment, please provide the number of locations in scope. Also, how far are these locations from each other? 8 locations total. 4 locations need escort due to armed guards. The furthest distance between locations is approximately 20 minutes.
7. Can you provide more details about the functionalities of the 15 web applications in scope? Also, would they all have login functionality? Would we be provided with test accounts? Upon review, 3 static web applications with some dynamic content.
8. Would the retest after 120 days include the full scope covering external network penetration testing, web application penetration testing, network security assessment, physical security assessment, and social engineering? If not, then which of these and what scopes would be part of the retest? The retest would include network security, web app retesting, and external network testing.

Q&A 3

1. Will the Madison County Government Security Operations Center (SOC) or Security Operation Center provider (SOCaaS) be notified prior to Penetration Testing? Yes, managers will be notified.

Q&A 4

1. Can we submit the proposal online?
2. Is there currently an incumbent company or previous incumbent, who completed a similar contract performing these services? If so – are they eligible to bid on this project and can you please provide the incumbent contract number, dollar value, and period of performance? No.
3. Specify the VLAN details how many are included in the scope? 4
4. Can you please provide the current number of infrastructure details (Physical Server, Virtual Server, Network Devices, etc.)? All are live, additional details provided once a vendor is selected.
5. How much (%) of the infrastructure is in the cloud? None
6. In the IT department environment, how many employees work? 15
7. Do you manage your own data Center, or do you utilize any 3rd-party/colocation facilities? We manage our data center.
8. Is there a funding/financial/budget range estimated that can help us to provide a quotation for this project? No.
9. Do we need to submit questions online on Bid Net or as per RFP it states "The point of contact for all questions or requests for additional information is: supportservices@madisoncountyil.gov?
10. Can you please clarify the proposal deadline time as per RFP deadline time is 9:30 a.m., Wednesday, March 27, 2024, and on Bid Net it is showing 3/27/2024 at 10:30 a.m. EST?
11. As per RFP it seems hardcopy submission but on bid net, it seems online submission, can you please clarify the mode of submission?

Q&A 5

1. Should the proposal cost only cover the initial test or the desired retest after 120 days? Both
2. Do you believe the work can be done remotely? For internal testing, we often provide a hardware appliance or use a VM on one of your servers. For physical, we can, for example, provide USBs for your staff to place. Both
3. Can you provide more detail on the web applications? The number and type determine the hours and thus the bid price. 3 web applications, static-dynamic hybrid.
4. Our testers have been CJIS checked by the State of Florida. Will certification of this meet your requirements? No. Must be the State of Illinois.
5. You mention no more than 500 IPV4 addresses. Can you provide more information on device types, OS, and why type of application? Windows Server 2019 and up, domain controllers, SQL servers, Linux servers, and vendor software servers.

Q&A 6

1. Do we need to submit questions online on Bid Net or as per RFP it states "The point of contact for all questions or requests for additional information is: supportservices@madisoncountyil.gov?
2. Can you please clarify the proposal deadline time as per RFP deadline time is 9:30 a.m., Wednesday, March 27, 2024, and on Bid Net it is showing 3/27/2024 at 10:30 a.m. EST?
3. As per RFP it seems hardcopy submission but on bid net, it seems online submission, can you please clarify the mode of submission?

4. Is there currently an incumbent company or previous incumbent, who completed a similar contract performing these services? If so – are they eligible to bid on this project and can you please provide the incumbent contract number, dollar value, and period of performance? No.
5. Specify the VLAN details how many are included in the scope? 4
6. Can you please provide the current number of infrastructure details (Physical Server, Virtual Server, Network Devices, etc.)? All are live, additional details provided once a vendor is selected.
7. How much (%) of the infrastructure is in the cloud? None
8. In the IT department environment, how many employees work? 15
9. Do you manage your own data Center, or do you utilize any 3rd-party/colocation facilities? We manage our data center.
10. Is there a funding/financial/budget range estimated that can help us to provide a quotation for this project? No.

Q&A 7

1. Would it suffice if the penetration testers already hold a Public Trust clearance, issued by the US Office of Personnel Management, or will they still be required to travel to Madison County Sherriff's Office for fingerprinting? No, they will be required to receive background check at Madison County Sheriff's office
2. If the Public Trust clearance will not suffice, how long does the CJIS background process take? For example, will testers be required to travel to Madison County to get fingerprinted and complete background check paperwork, wait for 2-4 weeks to get cleared, then travel back to Madison County to perform testing? 2-4 weeks for clearance, travel back may be necessary
3. Is Madison County flexible on completing all testing within 10 days? If not, what is driving this requirement? Yes, we are flexible and will finalize a timetable when a vendor is selected.
4. Will the pen testing be performed to meet certain compliance requirements (i.e. PCI, GLBA, HIPAA, etc?) If so, which one(s)? Certain servers contain HIPAA information
5. Will **re-testing** of physical security controls be required (on site), or only **re-testing** of network/system/application vulnerabilities identified (where re-testing can be performed remotely)? We would like to ensure that we are including the appropriate travel considerations in the bid. No, physical security assessment will not require retesting.
6. Regarding the Web Application Penetration Testing:
    - Are the web applications Commercial Off the Shelf (COTS), or custom coded by a 3rd party, or custom coded in house? Custom
    - What software or coding languages are used? ASP.net
    - How many unique dynamic pages (pages that change based on user inputs)? (e.g., an e-commerce site that sells products may have hundreds of dynamic pages, but each dynamic page is the same underlying code) For scoping purposes, only provide the number of unique pages with dynamic content. Upon further review, we are limiting the scope of this section. 3 static pages with some dynamic content will be in scope for this section of the project.
    - Will credentials for authentication be provided? In scope sites do not have authentication
    - If authenticated web application testing is being requested, how many and what types of user roles would you like tested? NA
7. Regarding the Physical Security Assessment/Penetration Test:
    - How many physical locations are in scope? 8

- Are there armed guards? For 4 locations, there are no armed guards
- Will physical security assessment/on-site social engineering be conducted during or after business hours, or both? During business hours
- In the event that the testers are "caught" do you wish for us to continue testing physical security controls, either by escort or in-the-open? Yes
- What physical security controls have been implemented? Cameras, prox cards, cypher locks
- Are there particular areas or techniques that are off limits for this assessment? 4 buildings will require escorted access due to armed guards, the other 4 will be unescorted.

8. Regarding Social Engineering:
    - Will Madison County provide the emails, phone numbers, etc of individuals to target, or will this be up to the vendor to discover? Yes, relevant information will be provided

Q&A 8

1. Five (5) independent stand-alone tasks creates significant breakage in planning a project. Do you actually want 5 standalone tasks, or will one planning exercise and one project report suffice? One exercise and project report will suffice, this structure was just laid out for logical purposes.
2. In what section of the proposal do you want the Bid Form?

Q&A 9

1. For the webapps, is the County looking for grey-box testing or black-box testing? IE, will the County provide test accounts for the various user roles present on the applications so the vendor can do an in-depth analysis of them or will the vendor be operating as an unauthenticated, untrusted attacker? Also, are these custom home-grown webapps or pre-canned/COTS software? Lastly, if the vendor is operating as an unauthenticated/untrusted attacker (black box), are these webapps already part of the intended scope for external network penetration testing? Any information that can be provided about these webapps would be helpful to better scope this.
2. No test accounts will be necessary, no user authentication is available on the 3 in scope pages. Pages are static with some dynamic content.
3. These webpages were built by Madison County Government
4. These websites are externally facing.
5. For physical security testing, what specific locations does the County want tested? Can the building names/addresses be provided? Does the County want each location to be tested, or is the County simply providing a list of in-scope locations seeing if the vendor can physically breach into any of them to gain access to the internal network?
    - 4 buildings will require escorted access due to armed guards, the other 4 will be unescorted.

Q&A 10

1. What is the County's budget? No budget has been publicly disclosed
2. Does the assessment include configuration reviews of network assets, and if so, how many:
    - A total of 500 live IPs will be in scope

- A total of 30 external live IPs will be in scope

3. How many locations will the contractor need to visit for the physical security assessment?
    - 4 buildings will require escorted access due to armed guards, the other 4 will be unescorted.
4. How many copies of the proposal does the County require?
    - 1 'original' copy and 4 additional copies
5. Does the County require a full post-remediation report, or would a memo be sufficient?
    - A full post remediation report is desired
6. Is it possible that the County would consider fingerprinting be done at a US Post Office or local police department with the results sent directly to the County?
    - Fingerprinting must be performed at Madison County Sheriff's Office
7. There are some requirements (e.g. pending litigation, proof of insurance, bid form) that do not fall under the required five tabs. Does the County want an appendix for outlying requirements?
    - Yes, that will be acceptable
8. For the purpose of the timeline, when does the County expect work to begin? We are hopeful to begin work in May/June, but that may be adjusted due to unforeseen delays.

Q&A 9

1. Physical Security – how many individual facilities, how many offices, rough square footage, and number of jacks are in scope?
    - 4 buildings will require escorted access due to armed guards, the other 4 will be unescorted.
2. Social Engineering – how many users/what percentage of the 900 users are in scope for the social engineering assessment?
    - Up to 100 users will be subject to social engineering

Q&A 10

1. What is the total number of external IPs in-scope for External Penetration Testing ? 30
2. Regarding Internal Network Vulnerability Testing:
    - Do you require credentialed scanning ? Yes, this may be included
    - How are the assets separated - broadcast domains? By VPNs? By VLANS? By both broadcast domains and VLANS
    - What are the subnet sizes ? /24
    - Do you utilize Microsoft Intune ? No
    - Do you utilize site-to-site VPNs ? Yes
3. How many applications are in-scope for the Web Application Security Testing in-scope ? 3 static pages with some dynamic content
4. Is Wireless Penetration Testing in-scope ? If so, how many sites ? Not in scope
5. For Physical Penetration Testing, how many facilities will be in-scope ? 4 buildings will require escorted access due to armed guards, the other 4 will be unescorted.
6. Do you require an assessment of your Information Security (IS) Policies ? No
    - If so, how many are presently defined and implemented, and are there any that need to be developed from scratch ?
7. Is any framework testing in-scope (NIST CSF, etc.) ? Madison County strives for NIST compliance
8. Are any of the following assessments also in-scope ?
    - Network Architecture Evaluation No
    - Firewall Configuration Assessment (VPN, DMZ, VLAN)No
    - Server Evaluation Assessment (Physical and Virtual)No

- Data Store Review and Security Assessment No
- Microsoft AD, Azure AD and O365 Configuration Assessment No
- Mobile Device Management Assessment No

9. Do you need any Security Awareness Training ? Madison County currently has a solution.
10. Are you in need of a Managed Detection and Response (XDR, EDR, MDR) solution ? Madison County currently has these solutions in place.

Q&A 11

1. **Internal Security Assessment**
    a. Are you using Active Directory today? Yes
    b. If so, how many Active Directory domains are in scope? 1
    c. Are there specific environments that are segmented within the organization for segmentation validation? There are Vlans segmenting the environments
    d. How many segments are in scope for validation? 500 live internal IPs are in scope
2. **Web Application Pen Test**
    a. What is the purpose of the application(s)? Presenting data or lookup to the public, no authentication
    b. Are these 15 distinct applications or are they sub-applications within one main application? This has been modified to 3 static pages with some dynamic content
    c. Does a user authenticate once and navigate to the rest of the applications/sub-applications or are their distinct authentication mechanisms for each application? There is no authentication
    d. What is the purpose of the application(s)? Presenting data or lookup to the public, no authentication
    e. Are the applications externally accessible? Yes
    f. How many pages are in each application? 3 static pages with some dynamic content
    g. How many roles are to be tested? External user with no authentication
    h. What are the names of the roles to be tested? NA
3. **Physical Security Assessment**
    a. How many locations are in scope? 8 locations
    b. What are the physical addresses of locations in scope? These will be provided at a later date, but all are within Madison County Illinois and all are within 20 minutes of Edwardsville, IL.
    c. Approximately, how far away are the locations from each other if there are multiple? Within 20 minutes of Edwardsville, IL.
    d. Other than physical network access, are there any other specific flags or objectives as part of the assessment? No specific additional guidelines, we are looking for a standard assessment.
4. **Social Engineering**
    a. What are your desired outcomes for the social engineering testing? To determine the response of critical users.
    b. Is there a prioritized list of social engineering engagements that are in scope? Yes, there is a prioritized list of the top 100 users.