JOLIET JUNIOR COLLEGE 1901

Addendum No. 1

DATE: March 20, 2023

Joliet Junior College
1215 Houbolt Road
Joliet, IL 60431

TO:	Prospective Respondents
SUBJECT:	Addendum No. 1
PROJECT NAME:	Annual Security Assessment
JJC PROJECT NO.:	R23011

This Addendum forms a part of the Bidding and Contract Documents and modifies the original bidding document as posted on the JJC website. Acknowledge receipt of this addendum in the space provided on the Bid Form. FAILURE TO DO SO MAY SUBJECT BIDDER TO DISQUALIFICATION.

Questions Received:

1. You are asking to list "top five current and prior two year clients" PLUS and additional (3) references for third-part firms. Can our single partner provide all of the above? ***Yes.***

2. What is the total count of External IPs? ***50 Public IP Addresses***

3. What is the total count of internal IP addresses to be tested (if providing an IP range, please indicate the estimated number of live IPs)?
    - ***Internal Penetration Test***
        - ***i. 2,500 Devices (Workstations, Servers, Switchers, Routers, IoT's, etc.***
        - ***ii. Additional pricing can be provided/itemized in menu form the vendor believes this to be of benefit to the college (such as an additional 2,500 devices, etc)***
    - o How many Desktops/Laptops? ***See above***
    - o How Many Servers (both virtual and physical)? ***See above***
    - o How many firewalls are in place at the college? ***See above***
    - o How many routers/switches/access points are in the environment? ***See above***
    - o How many printers and scanners are in the environment? ***See above***
    - o How many surveillance cameras does the college have in scope? ***See above***
    - o How many VOIP devices are in scope? ***See above***

4. Are there any web applications in scope for this project? ***No***

- o If so, how many are publicly available?
- o Are there any web applications that will require code review? (i.e., custom applications built and owned solely by the college)

5. How many locations/branches would be part of the scope? ***One***

6. Are all internal target systems and subnets accessible from a single location or will travel to other facilities be necessary for the internal testing? ***This answer will be shared confidentially with the awarded vendor.***

7. Is there a specific type of testing being requested by the college? (white/gray/black box). o If not, will it be the Consultant or the decision of the College to decide? ***Previously assessments were mostly black hat, some information is provided to the consultant in advance.***

8. Does the College use endpoint detection (EDR/XDR) software? ***Yes***

9. Does your organization have a resource dedicated to enforcing and maintaining security policies, such as a Chief Information Security Officer (CISO)? ***Yes, this question is not relevant to this SOW/assessment.***

10. What security products do you already have (e.g., firewall, intrusion detection, encryption)? ***This answer will be shared confidentially with the awarded vendor.***

11. Do you have a development environment for testing, or will this all be in the production environment? ***This answer will be shared confidentially with the awarded vendor.***

12. Where are your servers located? ***This can be discussed in discretion with the awarded vendor.***

- Are they on-prem, in the cloud, etc.? ***This can be discussed in discretion with the awarded vendor.***

13. Do you allow offshore resources to work on this project (outside of the United States)? ***No, vendor and personnel are restricted to the United States.***

14. Will the project team be expected to implement the suggested remediation as a part of this scope? ***No***

15. Thank you for specifying that the eternal scope is "up to 50 publicly accessible services".

- Approximately how many public facing active IP addresses are these services spread across? ***This answer will be shared confidentially with the awarded vendor.***

16. Of the 10 Class C networks, approximately how many internal active IP addresses (live hosts) are there?

- How many in the 5 optional Class C's? We'd like to understand if the networks are fully or sparsely populated. ***This answer will be shared confidentially with the awarded vendor.***

17. Approximately how many of these IP addresses are: ***This answer will be shared confidentially with the awarded vendor.***

18. Can all network segments that require testing, be accessed from a single network location? ***This answer will be shared confidentially with the awarded vendor.***

19. The RFP states "The selected vendor can perform some remote work as part of this engagement, but we strongly prefer that the chosen vendor is onsite at agreed upon times." Can you elaborate?
    - Does JCC want the penetration tester(s) to perform the bulk of the internal pen testing on site, and what is the reasoning behind this? ***We have been please with remote versions of this phase before, it is not a requirement***
    - Would JCC be open to all work being performed remotely? ***Yes.***
    - Our team has developed a drop box that can be shipped to customers, plugged into the network, and be controlled by our testers remotely (with very, very little assistance needed from JCC). This approach tends to save quite a bit of money since travel and living costs are eliminated for the duration of the penetration test. ***This type of scenario has worked for us in the past as well.***

20. When do you intend for the pen test to be performed?
    As soon as possible. Once the award has been approved by the Board of Trustees. We prefer that the project is complete, no later than the end of this Fiscal year June 30th, 2023.

21. Is testing during normal business hours acceptable? (8AM – 5PM CST)
    Yes

22. Are any web applications in scope? ***NO*** If yes: How many custom-developed or customized off-the-shelf Internet-facing web applications are living on your IPs and in scope for testing? How many roles does each web application have and what type(s) of roles would you like testing to be performed from in each application (e.g., admin, user)? Please provide a brief description of each of application to be tested: What languages/frameworks are the applications written in? Are any of the applications multiple instances of the same codebase? If so, please explain. Do any of these applications also have a mobile version in scope for testing? • If so, are they iOS or Android, or just mobile-responsive? Do any of these applications also have an application programming interface (API)? ***N/A***

23. External Penetration Testing How many public active IPs are in scope? How many inactive IPs are in scope? ***See response to question #3.***

24. Internal penetration testing Does the College prefer either of the following testing methods? Physical small form-factor system, Virtual machine (VM) How many internal network segments (VLANs) do you have? o How many will be tested? How many active internal hosts (private IP addresses) are on the segments to be tested? o How many physical servers? o How many virtual servers? o How many workstations? How many total user accounts do you have? o How many levels of user accounts do you have?

25. Wireless testing – is this in scope? Please select your preference in testing: ☐ Perform testing of the internal network FROM a wireless connection OR ☐ Perform testing of the wireless network itself How many locations are included in wireless testing? o Where are these locations in relation to each other? o How many SSIDs at each location? o How many wireless access points at each location? ***Out of scope***

26. The RFP asks for the following: Provide a list of the vendor's top five current and prior two-year clients indicating the type of services the organization has performed for each client. Can you clarify this? Will the top five customer for this year and the top five customers for last year suffice? We do MANY projects for MANY customers and the request implies a list of all clients for the prior two years.
    One list of your top 5 clients (current and prior clients)

27. The Term of Contract states: "Any contract, which results from this RFP, shall be only for the duration of the 2023 annual security assessment period." What is the 2023 annual security assessment period?
    See response to question #20 above.

28. Pricing: Does JJC desire a separate pricing document or can pricing be included in the technical proposal? Including the price in the technical proposal is implied in Section IV Format for Response.
    Please include pricing in your technical proposal.

29. Is there a budget for this project? Are you able to provide the budget estimate?
    The budget will not be shared at this time.

30. Pricing: Is JJC open to T&M pricing or does JJC want to see fixed pricing? ***Fixed pricing..***

31. For the wireless test: ***Out of scope; please see the SOW***
    - How many ESSIDs are to be tested?
    - How many different locations/buildings need to be tested from?
    - Are any networks mixed-use between students and staff/IT?
    - Would we be performing a configuration review of the access points and other equipment?

32. Does the JJC currently conduct penetration testing? If so, what is the typical frequency and type (internal, external, web, etc)? ***This information is not required to fulfil the proposal***

33. againFor the wireless test: ***Out of Scope. Please see the SOW***
    - How many ESSIDs are to be tested?
    - How many different locations/buildings need to be tested from?
    - Are any networks mixed-use between students and staff/IT?
    - Would we be performing a configuration review of the access points and other equipment?

34. Is there an incumbent who is currently providing these services? If so, is there a reason for considering replacement of the incumbent?
    JJC simply issues this RFP on an annual basis.

35. Who will the awardee coordinate with to perform the work? ***This information will be provide directly to the winning bidder***

36. Has JJC experienced any breaches within the last 3 years? If so, can JJC provide information on the nature of the breach and remediation steps taken?***This information is not required to fulfil the RFP.***

37. Depending on the number of questions and timing of the answers, will JJC consider delaying the due date of the proposal? ***No***

38. RFP Page 10 VI. Scope of Work 2. Internal penetration assessment & vulnerability will be performed from inside the organization, mimicking an attacker with internal network access with no credentials. The approach will be the same as in the external penetration assessment and will include at least 10 class C IP ranges. Please provide the cost for 5 additional class C subnets in the event it is deemed necessary by JJC during the testing. Question: For accuracy, can you give us the total number of active IP addresses? If not, we will estimate 200 live addresses per /24, so 2000 total (with 1000 on stand-by). Page 10 VI. Scope of Work 2. "The selected vendor can perform some remote work as part of this engagement, but we strongly prefer that the chosen vendor is onsite at agreed upon times." Question: Our standard operating procedure is remote access via an appliance that we ship. Travel and lodging can be added to the cost, but from an operational standpoint, we strongly prefer remote access. What is the purpose of the onsite presence and is this a negotiable requirement? ***This information is not required to submit a proposal.***

39. RFP Page 10 VI. Scope of Work 2. Internal penetration assessment & vulnerability will be performed from inside the organization, mimicking an attacker with internal network access with no credentials. The approach will be the same as in the external penetration assessment and will include at least 10 class C IP ranges. Please provide the cost for 5 additional class C subnets in the event it is deemed necessary by JJC during the testing. Question: For accuracy, can you give us the total number of active IP addresses? If not, we will estimate 200 live addresses per /24, so 2000 total (with 1000 on stand-by). Page 10 VI. Scope of Work 2. "The selected vendor can perform some remote work as part of this engagement, but we strongly prefer that the chosen vendor is onsite at agreed upon times." Question: Our standard operating procedure is remote access via an appliance that we ship. Travel and lodging can be added to the cost, but from an operational standpoint, we strongly prefer remote access. What is the purpose of the onsite presence and is this a negotiable requirement? ***There is no requirement to be onsite. This information is not required to submit a proposal.***

40. Does any Web/Mobile Application (all Internet-accessible systems) involved in the VAPT? ***This information is not required to submit a proposal.***

41. External VAPT is unauthorized, can we do Authorized scan for better results? ***All scans will be authorized. The details will be discussed with the winner bidder.***

42. Please share with us some approx. IP's for in Class C IP ranges? ***This information is not required to submit a proposal.***

43. Is there a specific time when scans should be performed? ***The nature of this assessment is that the vendor would perform scan within an agreed upon window. In previous cases this has been over the duration of a week.***

44. Are there any specific subnets that has to be excluded from the scan? ***If so, it will be provided to the winning vendor.***

45. Are there any dead zones (systems not reachable from the DC)? ***If so, it will be provided to the winning vendor.***

46. For Cloud Platforms. IaaS - Similar to traditional environment PaaS - Identity & Access Management, DB Security Features SaaS - Accesses alone ***Please note that this appears to be an incomplete question.***

47. What is the business requirement for this penetration test? ***Please refer the SOW in the proposal.***

48. When was the last VA/PT performed? ***Annually***

49. Total number of Internal IP addresses
    See response to question #3 above.

50. Are there any OT devices that need to be scanned? ***This information is not required to submit a proposal.***

End of Addendum #1

JOLIET JUNIOR COLLEGE 1901

Addendum #1

DATE: March 20, 2023

Joliet Junior College
1215 Houbolt Road
Joliet, IL 60431

TO:	Prospective Respondents
SUBJECT:	Addendum No. 1
PROJECT NAME:	Annual Security Assessment
JJC PROJECT NO.:	R23011

Please acknowledge receipt of these addenda by including this page with your proposal. Include your company name, printed name, title, and signature in your acknowledgement below. Failure to do so could result in disqualification of your bid.

Issued by:

Matt Stephenson
Senior Director of Business & Auxiliary Services
Joliet Junior College
815.280.6643

I acknowledge receipt of Addendum #1.

_____
Company Name

_____
Printed Name

_____
Title

_____
Signature