



DATE: March 11, 2020

Joliet Junior College
1215 Houbolt Road
Joliet, IL 60431

TO: Prospective Respondents
SUBJECT: Addendum No. 2
PROJECT NAME: Security Penetration Testing & Operational Framework Assessment
JJC PROJECT NO.: R20009

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 as specified at the end of this addendum. FAILURE TO DO SO MAY SUBJECT BIDDER TO DISQUALIFICATION.

Please be advised that a number of questions were left out of Addendum #1. Those questions are addressed below:

1. Page 10, Deliverables. In light of current travel concerns, may the formal presentation to senior management be performed via teleconference or is an in-person presentation needed?
Teleconference will likely suffice. This information will be provided to the awarded vendor.
2. Page 10, Executive Summary Report. Is this to be a completely separate report or may it be a separate section of the technical report?
A separate Executive Summary is required
3. When was the last comprehensive pen testing performed and are the findings and remediation's available
The findings and remediations of previous testing will not be provided.
4. What time restrictions for performing the testing ?
This information will be provided to the awarded vendor.
5. What areas of the college's technology environment are out of scope for testing ?
This information will be provided to the awarded vendor
6. What classes of technology are to be tested ?
This information will be provided to the awarded vendor.

7. Paragraph 2 of phase 1 states that the college prefers that the chosen vendor is onsite at agreed upon times. What does this mean as to when?
If the bidder somehow has a method to pen test a wireless remotely, they can list that in the bid.
8. Paragraph 3 of Phase 1 states that the wireless penetration assessment phase will be performed onsite at the Main Campus Location, but the description of the facility identifies 5 significant locations and a number of satellites. Does this mean that wireless testing in facilities outside the Main Campus Location is out of scope?
One location will likely be selected for testing. This information will be provided to the awarded vendor.
9. Paragraph 3 of Phase 1 states that the scope of wireless test includes three separate wireless networks. Are these three separate networks with each having its own set of Access Points, or is this three logically separated networks using the same physical access points (e.g., three different SSIDs on the same set of access points)?
One location will likely be selected for testing. This information will be provided to the awarded vendor
10. Is the college expecting the tester to demonstrate exploitability of each discovered vulnerabilities?
Yes, within reason; this can be discussed the awarded vendor.
11. Will the testers have access to a technical person employed by the college who can make “test/no test” decisions on assets that may be adversely impacted by the testing?
Yes
12. Will the testers be held harmless and immune from penalty should testing inadvertently disrupt critical assets or cause loss of sensitive or critical data? This presumes that the testers have followed best practices and observed normal procedures in attacking the assets.
This information will be provided to the awarded vendor
13. What protocol does the college want the testers to follow when a discovered asset is determined to be potentially susceptible to serious damage if the testing is allowed to proceed to conclusion (e.g., the asset is found to be deficient in OS or firmware versions or patching levels that may give rise to significant damage if certain tests are conducted)?
This information will be provided to the awarded vendor
14. Phase II is very vague in describing expectations for the Operational Framework Review. Will the college provide necessary documentation to allow the testing company to fully evaluate the current state of the technological environment of the college and understand the future direction for the next 3 to 5 years? This includes the following: College’s strategic plan for the next 3 to 5 years particularly plans for accommodating changes in size of student body and number of faculty and staff and changes in methods for delivering course material and evaluating student performance over the next 3 to 5 years; supporting technology projects budgeted or for which budgets have been requested over the next 24 months; current tactical and strategic plans for the use of technology to support the business goals of the college; current asset inventories; current network configuration and architectural diagrams; access to event logs and any monitoring systems in use; current

cybersecurity policies, procedures and standards; copies of audits and operational reviews and their findings and remediation over the last 12 months.

This information will be provided to the awarded vendor.

15. Phase II references the need to structure an organization-wide program for information security based on the NIST Cybersecurity Framework. Since the NIST framework is a general framework, what expectations does the college have for tying the NIST framework to specific State and Federal compliance requirements that the college must meet?

This information will be provided to the awarded vendor

16. The deliverables call for a formal presentation of findings and recommendations to senior management. Does this require a return to the college for an oral delivery of the findings and response to questions that may arise?

This information will be provided to the awarded vendor

17. Can you explain the relevance of security audit experience as it relates to pen testing?

This information will be provided to the awarded vendor

18. On page 8 under #8 Invoicing Procedure, b. Include documentation identifying all of the vendor's fees, what documentation are you specifically referring to or looking for?

Vendor should provide information regarding their invoicing procedure based on proposed fees

19. On page 7 under Profile of Vendor, it states: b. Submit independently audited financial statements. As a small business, we do not have audited financials. What other information can be provided as an acceptable alternative to audited financials?

An independent review by an authorized CPA is acceptable.

20. We would like to prepare as proposal that is as competitive as possible. Is there any way to get a better idea of the number of IPs as our pricing is calculated by the number of active/live IP's we are testing. Our price breakdowns fall into these categories based the number of IP's:

- a. 1-25
- b. 26-50
- c. 51-100
- d. 101-150
- e. 151-250
- f. 251-500
- g. 501-1000
- h. 1001-1500
- i. 1501-2500
- j. 2500+

Please provide itemized/tiered pricing within your response.

21. Also the Wireless Penetration testing is priced per site. So if there are 3 networks on one site, it is priced at one fee. If there are 3 networks at 3 locations it will be 3x the fee. Do you have any insight into if it is 3 separate locations or all at one site?

We are only going to test from one of our locations.

End of Addendum #2



DATE: March 11, 2020

Joliet Junior College
1215 Houbolt Road
Joliet, IL 60431

TO: Prospective Respondents
SUBJECT: Addendum No. 2
PROJECT NAME: Security Penetration Testing & Operational Framework Assessment
JJC PROJECT NO.: R20009

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:

Janice Reodus
Director of Business & Auxiliary Services
Joliet Junior College
815.280.6643

I acknowledge receipt of Addendum #2.

Company Name

Printed Name

Title

Signature