DATE: March 9, 2020

Joliet Junior College
1215 Houbolt Road
Joliet, IL 60431

TO:	Prospective Respondents
SUBJECT:	Addendum No. 1
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.

Questions Received:

1. Page 6 of the RFP states: This solicitation contains a goal to include businesses owned and controlled by minorities, females, and persons with disabilities in the College's procurement and contracting processes in accordance with the State of Illinois' Business Enterprise for Minorities, Females, and Persons with Disabilities Act (30 ILCS 575). What is the participation goal for this project?
   Joliet Junior College has an overall aspirational goal of 20%.

2. Is there a list of interested bidders, so that MWBEs can seek partnerships with prime contractors?
   The college does not have a list of interested bidders for this project.

3. In reference to the M/WBE utilization goal indicated in the RFP, could JJC please indicate what the goal is in terms of a certain percentage of the contract value?
   Joliet Junior College has an overall aspirational goal of 20%.

4. On page 7, the RFP requests the vendor's top three current clients. Is JJC asking for the vendor's three largest clients, or just a sample of three clients for which the vendor is doing similar work?
   Top three clients, largest or sample can work as references.

5. On page 8 of the RFP under the Invoicing Procedure section, JJC asks for "documentation identifying all of the vendor's fees." Is this just a statement that our invoices need to include documentation of all fees, or does JJC want to see a sample invoice reflecting all proposed fees for this project? ***Describe your invoicing procedure and line item details of your fees.***

6. We have performed such work on numerous government contracts (local, state, and federal) nationwide. Our personnel have experience performing assessment and testing services to higher educational institutions. QUESTION - - Will you consider waving the requirement for 3 references for projects of similar size and scope for higher education institutions?
   See response to question #4 above.

7. Does JJC plan to release a full list of interested bidders to all contractors?
   The college does not have a list of interested bidders for this project.

8. Does JJC plan to release responses to questions to all interested bidders or to just the individual bidder who posed the question?
   All questions will be addressed through ESM's electronic sourcing module. These questions and JJC's responses will be issued via addendum and available online at: https://www.jjc.edu/community/vendors/current-solicitations

9. Does JJC currently have a NIST-based CSF in place, including controls, policies and procedures?
   Yes

10. What is the projected date for starting the project, and its projected completion?
    This information is not available.

11. Is drafting/developing NIST-based CSF (e.g., controls, gap analysis, P&P, risk assessment, training, etc.) within the scope of the Operational Framework Assessment phase of the project***? Developing is within the scope***. Could this be an itemized cost? ***This can be an itemized cost.***

12. Are certified MWBEs outside Illinois eligible for this project?
    All qualified vendors are eligible to submit proposals for this project; however, certification must be established in Illinois for the project to count toward the college's utilization goals.

13. What are the unique type of services and applications in the client's environment?
    This will be discussed with the awarded vendor upon selection.

14. Penetration testing and Vulnerability scan both part of scope?
    Yes

15. What are the total number of Critical Systems?(A critical system is any additional system outside of the card data environment boundary that could affect card data security. For example, firewalls, IDS, authentication servers - any assets utilized by privileged users to support and manage the card data environment)
    This will be discussed with the awarded vendor upon selection.

16. Is there any testing environment or scan will be performed on live/production environment**? This might be a possibility but it will be discussed with the awarded vendor.**

17. Degree of exploitation?
    This will be discussed with the awarded vendor upon selection.

18. During what time window will testing need to be performed?
    This will be discussed with the awarded vendor upon selection.

19. Are there any legacy systems that have known issues with automated scanning? If so, how should testing be performed against these systems? ***This information will be provided to the awarded vendor***

20. Is there a preferred method of communicating about scope and issues encountered during the engagement?
    This will be discussed with the awarded vendor upon selection.

21. Does client want updates regarding ongoing exploitation of systems during the test? If so, JJC will need to determine whether they will or will not act upon such information or make changes to the environment. JJC may also want to implement its incident response plan in response to an exploit. ***This information will be provided to the awarded vendor***

22. Are there security controls that would detect or prevent testing? Consider whether these should be disabled or configured to not interfere during testing.
    This will be discussed with the awarded vendor upon selection

23. If passwords or other sensitive data are compromised during the testing, does the tester need to disclose a list of all passwords and/or sensitive data accessed?
    Yes

24. If equipment owned by the tester is to be connected to the organization's network, what steps must be taken to ensure the equipment does not pose a threat to the environment (updated to the latest operating system, applied service packs and/or patches, etc.)?***This will be discussed with the awarded vendor upon selection.***

25. Does the tester need to provide all IP addresses from which testing will originate?
    This will be discussed with the awarded vendor upon selection.

26. Will sensitive data shown to be accessible during the test be retained by the tester during and after the penetration test? Only a proof-of-concept test should be performed, any cardholder data obtained must be secured in accordance with PCI DSS.
    No

27. What steps will be taken if the tester detects a previous or active compromise to systems being tested? (For example, activate incident response procedures and stop penetration test until resolution of the compromise situation.)
    Activate incident response procedures and stop penetration test until resolution of the compromise situation. This can be discussed upon selection. This information will be provided to the awarded vendor.

28. Any third party hosted system such as cloud? If so, can we get approval from the third party for Penetration Testing?
    This will be discussed with the awarded vendor upon selection.

29. Can tester get the list of old vulnerabilities in the system?
    A list of old vulnerabilities with not be provided.

30. Are you willing to set aside the contract as a certified SDVOSB or SBA 8(a)?
    The college cannot legally set contracts aside specifically for small or certified business.

31. Are you looking for a fixed price or some type of time and materials contract?
    Fixed Price, with itemized pricing for recommended services that are out of scope.

32. In reference to the contract in paragraph 9, are you looking for our standard terms and conditions?
    Yes, please provide a sample contract with your firm's standard terms and conditions.

33. Is a full financial audit required or will a independent "review" or a "compilation" by an authorized CPA be acceptable?
    An independent review by an authorized CPA is acceptable.

34. For the wireless penetration testing, there is a requirement to have the testing performed onsite. Can you describe the scope and projected level of effort? This could be discussed further upon selection.
    If the bidder somehow has a method to pen test a wireless remotely, they can list that in the bid.

35. Is the scope of the assessment only for infrastructure and publicly accessible services? Are defensive tools, applications, authentication systems, etc, a part of the assessment?
    This will be discussed with the awarded vendor upon selection.

36. Are there web services that utilizes SOAP UIs, WSDLs, etc.? If so, will this information be delivered upon selection?
    This information will be delivered to the awarded vendor upon selection.

37. Are social engineering techniques within scope of the assessment?
    Yes

38. As part of the validation process, are system/application exploitation processes allowed? i.e. web shells, command prompts, powershell, root, etc.
    Yes

39. Should findings during the assessment be delivered as they are found? Should they be delivered at the end of each phase or only at the conclusion?
    Yes, findings should be delivered during the assessment as they are found.

40. For the operational framework assessment, will the organization's security policies, procedures, standards, defensive posture, etc, be delivered?
    This information will be delivered to the awarded vendor upon selection by request.

41. Would you like to know ALL exploitable vulnerabilities on the network, or do you prefer a scenario based approach where we get privileged access**? The vendor can use security best practices to determine this.** ***This information will be provided to the awarded vendor***

42. What is the main purpose of each phase? What are you looking to find? ***This information will be provided to the awarded vendor***

43. For internal penetration testing, how many IPs are in use for each one of the 10 Class C IP ranges? How many for the 5 additional? ***This information will be provided to the awarded vendor***

44. Are all 3 wireless networks at the same location? ***This information will be provided to the awarded vendor***

45. For the internal/external testing, do you also want remediation testing included in our pricing? No

46. How many "live" IPs are in the 10 Class C Subnets? ***This information will be provided to the awarded vendor***

47. How many "live" IPs are in the additional 5 Class C subnets? ***This information will be provided to the awarded vendor***

48. Can you provide an estimated breakdown of the devices that would be included in all Class C subnets? ***This information will be provided to the awarded vendor***

49. How many physical locations need to be assessed? 1

50. How many servers are to be assessed? ***This information will be provided to the awarded vendor***

51. How many workstations are to be assessed? ***This information will be provided to the awarded vendor***

52. How many different CIDRs (i.e IP blocks such as 192.168.10/24) are to be assessed? ***This information will be provided to the awarded vendor***

53. How many websites are to be assessed? ***This information will be provided to the awarded vendor.***

54. How many external IP addresses are to be assessed? ***This information will be provided to the awarded vendor.***

55. For the wireless portion, can one representative WIFI network be assessed - or does every WIFI network need to be assessed? ***This information will be provided to the awarded vendor.***

56. Can all network CIDRs & VLANs be reached from one main location? (i.e. from the Data Center or Admin Vlan). This would be a substantial cost savings. ***This information will be provided to the awarded vendor.***

57. For these assessment services, is there a requirement for MBE/WBE goal for this proposal? ***This information will be provided to the awarded vendor.***

58. Of the 50 publicly accessible services that will be assessed, how many of them are web servers and/or running web services (HTTP and HTTPS)? ***This information will be provided to the awarded vendor.***

59. Is email social (phishing attacks) in scope for the assessment? a. If yes, how many employees would you like to sample for email social engineering? I. We would recommend a sample size of 3%-10% of the company. b. How many users have Internet and/or email access? ***This information will be provided to the awarded vendor.***

60. Is telephone social engineering in scope for the assessment? a. This would involve contacting employees via phone in attempts to provide information, or increase the response rate from email social engineering If yes, how many employees would you like to sample for telephone social engineering? i. We would recommend a sample size of 5-20 employees. ***This information will be provided to the awarded vendor.***

61. How many campuses/facilities will be assessed? (e.g. locations traveled to) o If more than one, do they all abide by the same set of policies and procedures? **One**

62. Roughly how many internal devices exist (including, but not limited to, firewalls, routers, workstations, servers, switches, etc.) within the 10-15 Class C IP ranges? ***This information will be provided to the awarded vendor.***

63. Do you require the NIST assessment to be required onsite or remotely? ***This information will be provided to the awarded vendor.***

64. Is physical security awareness testing in scope for this assessment? b. How many locations would you like to test for physical and on-site social engineering as well as document disposal? c. What is the geographic region of these sites, specifically how many miles apart? ***This information will be provided to the awarded vendor.***

65. Are there expectations for a particular framework? (e.g. NIST, COBIT, ISO) ***This information will be provided to the awarded vendor. We use NIST CSF as our framework.***

66. Does your organization have compliance requirements that should be considered as part of this assessment? If so which one(s)? (PCI, HIPAA, MA 201 CMR, etc.) ***This information will be provided to the awarded vendor.***

67. Number of individuals in your IT department? ***This information will be provided to the awarded vendor.***

68. Number of business SME's that we would need to interview to obtain a representative sample of end-users of IT? ***This information will be provided to the awarded vendor.***

69. Number of servers? ***This information will be provided to the awarded vendor.***

    Number and types of platforms? ***This information will be provided to the awarded vendor.***

70. Number of key applications (and how many of these are custom code)?
    This information will be provided to the awarded vendor.

71. Number and types of encryption solutions? ***This information will be provided to the awarded vendor.***

72. Number of distinct e-Commerce sites? ***This information will be provided to the awarded vendor.***

73. Number of data centers and locations? ***This information will be provided to the awarded vendor***

74. Number of physical locations and their size? ***This information will be provided to the awarded vendor***

75. Number and type outsourced functions within IT?
    This information will be provided to the awarded vendor.

76. For wireless penetration testing: a. Number of physical locations to be assessed? ***This information will be provided to the awarded vendor***
    b. Number of wireless networks deployed? ***1 Wireless network*** c. Types of encryption employed? ***This information will be provided to the awarded vendor.***

77. Page 5, Proprietary Information. Instead of marking specific pages, is it acceptable to submit a redacted copy of the proposal? ***Please indicate what information in your proposal is confidential/proprietary.***

78. Is the incumbent eligible to bid on this? ***This is a competitive solicitation. All vendors are eligible to participate.***

79. 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.***

80. Page 10, Executive Summary Report. Is this to be a completely separate report or may it be a separate section of the technical report? ***Separate Report***

End of Addendum #1

DATE: March 9, 2020

Joliet Junior College
1215 Houbolt Road
Joliet, IL 60431

TO:	Prospective Respondents
SUBJECT:	Addendum No. 1
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 Reedus
Director of Business & Auxiliary Services
Joliet Junior College
815.280.6643

I acknowledge receipt of Addendum #1.

_____
Company Name

_____
Printed Name

_____
Title

_____
Signature