DATE: May 2, 2018

Joliet Junior College
1215 Houbolt Road
Joliet, IL 60431

TO:	Prospective Respondents
SUBJECT:	Addendum No. 1
PROJECT NAME:	Information Security Penetration Testing & Operational Framework Assessment
JJC PROJECT NO.:	R18008

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. For External:
    a. Based on public DNS records we noticed there are a number of cloud based service providers used by JJC. Based on this information and understanding this exercise to be a black box exercise, will the institution provide a range of IP's in scope upon award?
    Yes

2. For Internal:
    a. Can this exercise be done remotely?
    Yes, but we strongly prefer that the chosen vendor is onsite at the prescribed agreed upon times. We don't want it to be a 100% remote engagement.

    b. Can the testing of all environments be done from one central location?
    Yes, on Main Campus

3. For Wireless:
    a. How many locations are in scope for wireless? ***One location, Main Campus***
    b. How many SSID's are at each location? ***Per the RFP, 3 SSID's will be tested***
    c. How many Access Points are there? ***For security reasons, more detailed information will be provided if selected as a finalist.***
    d. Should rouge AP's be identified? ***Yes***
    e. Are client attacks in scope? ***Yes***
    f. How many clients use the wireless network? ***For security reasons, more detailed information will be provided if selected as a finalist.***

4. General:

a. Can the formal presentation be facilitation via WebEx? ***Yes, onsite is preferred.***
b. Can we use social engineering to obtain credentials or to breach the network? ***Yes***
c. For the operational framework finds would it be acceptable to use the NIST 800-171 instead of NIST 800-53? ***Knowing NIST 800-171 is a streamlined version for non-federal entities, baseline pricing should be done on 800-171 and alternate pricing for 800-53.***

5. External Penetration
    a. What is the total number of IP Addresses/hosts (Internet Accessible) that will be in scope for the assessment? (For example: 15 hosts, 3 class C network segments) ***50.***
    b. How many of these services are web sites (HTTP and HTTPS)? ***The college would like to treat this as a black box engagement and ask the vendor to scan and assess.***
    c. Are any of the web services hosted at a third party? If yes, how many and who is hosting? ***Yes. The college would like to treat this as a black box engagement and ask the vendor to scan and assess.***
    d. How many interactive web applications are in scope for the assessment? ***For security reasons, more detailed information will be provided if selected as a finalist.***
    e. Is both authenticated and un-authenticated (anonymous) web application testing requested? If authenticated testing is required, how many applications will be tested? ***For this engagement, we would like to conduct anonymous testing to identity issues from an attacker's perspective.***
        i. Authenticated testing will allow us to determine if a user who has valid credentials can access restricted areas of the application or other user data.
        ii. Anonymous testing will only allow us to identify issues from an attacker's perspective without credentials.

6. Internal Penetration
    a. How many total servers (physical & virtual) are within the environment? ***For security reasons, more detailed information will be provided if selected as a finalist.***
    b. How many workstations are used within the company? ***The scope will be for 10 class C subnets***
    c. How many internal network segments are located outside of the U.S.? Are these segments reachable from a U.S.-based location in which we would be working? ***None, zero***

7. Wireless Penetration
    a. How many SSIDs will be tested as part of this wireless penetration testing? ***Three***
    b. How many locations will be visited in order to conduct the wireless penetration testing? ***One location, Main Campus***

8. Information Security Organization
    a. Can you provide a brief description of the current information security team? ***For security reasons, more detailed information will be provided if selected as a finalist.***
    b. Approximately how many employees manage a control in NIST 800-53 r4?

For security reasons, more detailed information will be provided if selected as a finalist.

9. We are SBA certified Woman Owned Small Business (EDWOSB). Do we qualify for this bid?
   Yes.

10. We are a certified DBE firm for DC & NY states. Do we qualify for this bid?
    Yes.

11. If yes, Is this Firm Fix Price contract.
    Yes.
12. According to the RFP, there are no more than 50 publicly available services. Can JJC provide an exact number of external live IPs to be tested or should it be priced based on 50 IP's?
    Price based on 50 IP's, provide the cost for additional IP to test.

13. Even though JJC will not provide specific network information prior to starting the initial discovery phase, will Joliet Junior College confirm the IP addresses that the tester discovers prior to us performing the vulnerability scanning?
    Yes.

14. Is a social engineering/phishing exercise in scope for the external penetration test?
    Yes.

15. How many locations are required for the internal penetration assessment? Can we see the entire network from one central location, or are we required to go to one of Joliet Junior College's five extension campuses?
    For the internal penetration assessment, per the RFP Scope of Work 'Penetration Testing Phase' item number two, the assessment will include at least 10 class C IP ranges. The vendor is to provide a cost for any additional class C IP range. The college and vendor will agree upon any additional subnets to be tested dependent on the results from the initial assessment.

    Testing will be conducted from one location, Main Campus.

16. Will credentials be provided to the tester for the internal penetration assessment if we were not able to harvest any during the initial attack?
    Yes.

17. For the internal assessment, how many servers, both physical and virtual, are in the environment?
    For security reasons, more detailed information will be provided if selected as a finalist.

18. For the internal assessment, how many work stations are in the environment?
    For the internal penetration assessment, per the RFP Scope of Work 'Penetration Testing Phase' item number two, the assessment will include at least 10 class C IP ranges.

19. Does the formal presentation of findings and recommendations need to take place onsite, or can this be done remotely through a skype/conference call session?
    On-site preferred.

20. If the results of the penetration testing phase are mapped to NIST SP 800-53 standards, would this encompass the operational framework review phase as well? Or is that required to be a separate engagement?
    It's ok to be addressed in the penetration testing; as long as all requirements from NIST are covered in the engagement.

21. Are all controls (families) of the NIST SP 800-53 required to be in scope for the Operational Framework Review phase?
    Yes. Per question 4c above, please provide baseline pricing on 800-171 and alternate pricing for 800-53.

22. For the wireless assessment, are the three wireless networks in scope visible from the main campus location? Or would we need to go to one or more of the extension campuses?
    Yes. One location, Main Campus.

23. Are bidders permitted to work with subcontractors to perform the testing/assessments?
    No.

24. Should travel expenses be included in the proposed expenses as a line item?
    Yes.

25. What budget does JJC have allocated for the entirety of this project?
    JJC has a budget line item for this project.

26. When does JJC plan to begin formal planning with the chosen vendor after awarding that vendor?
    Formal planning would begin after board approval in June and the project completed by July 31st.

27. When does JJC need these services completed by?
    By July 31st, 2018.

28. We would like clarification as noted below:
    For security reasons, more detailed information will be provided if selected as a finalist. The awarded vendor for this RFP will schedule a one-time engagement.

Joliet/ TRS	Approx. No. / URL / Applications	E.g.	Frequency	Our Standard
No of Ips - External	?	Public IP's	Monthly	Quarterly
No of Ips - Internal	?	Internal IP's / Live IP's in Class A/B/C	Monthly	Quarterly
No. of External Network Pen. Test	?	Public IP's	Monthly	Annual
No. of Inernal Network Pen. Test	?	Internal IP's / Live IP's in Class A/B/C	Quarterly	Annual
No. of External App Pen. Test	?	www.companylogistics.com	Annual	Annual
No. of Internal App Pen. Test	?	Fast Track Application	Annual	Annual

29. Phase 1, External Penetration Test - Confirm that "50 publicly available services" refers to instances of HTTP/HTTPS, SMTP, Telnet, etc. exposed to the internet.
    Yes.

30. Phase 1, External Penetration Test - Will JJC provide the networks that are in-scope and owned by the college?
    Yes.

31. Phase 1, Internal Penetration Test - Approximately how many hosts are present on the 10 /24 networks in the base scope, and the 5 /24 networks in the extended scope?
    For security reasons, more detailed information will be provided if selected as a finalist.

32. Phase 2 - What is the size of the security team and the size of the overall IT organization at JJC?
    For security reasons, more detailed information will be provided if selected as a finalist.

33. Phase 2 - Are all technology and information assets under the management of a central IT organization within JJC? If not, how many groups within JJC are responsible for their own technology and information assets?
    Yes.

34. How many controllers are in scope for the wireless network assessment?
    For security reasons, more detailed information will be provided if selected as a finalist.

35. Is the IT organization centralized or decentralized?
    Centralized.

36. Are there documented policies, procedures, standards, and guidelines in place? If so, how many?
    There are documented policies and procedures in place.

37. What are the College's key drivers for seeking external assistance with these services?
    To identify vulnerabilities and risks with the current state of the college and create a security program based on the NIST framework.

38. How many locations (offices/data centers) are in scope?
    One physical location, Main Campus (On-premise and cloud).

39. How many third-party vendors are providing IT services?
    Not Applicable.

40. Are there any services in the cloud?
    Yes.

41. When was the last vulnerability scan completed? Who completed it?
    For security reasons, more detailed information will be provided if selected as a finalist.

42. Is there a CISO position at JCC? What is their role in this engagement?
    Yes. Primary contact and project lead.

43. What security framework is currently in place?
    We would like to start utilizing the NIST framework and the reason for this engagement.

44. Who is the project sponsor at the College?
    Executive Director of Information Technology and CISO

45. External Vulnerability Scanning Questions:
    a. How many active external IP addresses are in scope? ***The college would like to treat this as a black box engagement. For security reasons, more detailed information will be provided if selected as a finalist.***
    b. How many external web applications are in scope? ***The college would like to treat this as a black box engagement. For security reasons, more detailed information will be provided if selected as a finalist.***
    c. What virtual architecture is in use? ***The college would like to treat this as a black box engagement. For security reasons, more detailed information will be provided if selected as a finalist.***
    d. General architecture orientation: What versions of Unix/Linux are in use? ***The college would like to treat this as a black box engagement. For security reasons, more detailed information will be provided if selected as a finalist.***
    e. General architecture orientation: what versions of Windows server are in use? ***The college would like to treat this as a black box engagement. For security reasons, more detailed information will be provided if selected as a finalist.***
    f. What web programming languages are in use with the web applications? ***The college would like to treat this as a black box engagement. For security reasons, more detailed information will be provided if selected as a finalist.***

g. Are web applications custom off the shelf (COTS) or developed internally? ***For security reasons, more detailed information will be provided if selected as a finalist.***

46. Internal Vulnerability Scanning Questions:
    a. Are internal workstations included***? Yes.***
    b. How many internal web applications are in scope? ***The college would like to treat this as a black box engagement. For security reasons, more detailed information will be provided if selected as a finalist.***
    c. How many of each: servers/databases/firewalls/routers/switches? ***The college would like to treat this as a black box engagement. For security reasons, more detailed information will be provided if selected as a finalist.***
    d. General architecture orientation: What versions of Linux are in use? ***The college would like to treat this as a black box engagement. For security reasons, more detailed information will be provided if selected as a finalist.***
    e. General architecture orientation: What versions of Windows server are in use? ***The college would like to treat this as a black box engagement. For security reasons, more detailed information will be provided if selected as a finalist.***
    f. Is virtual architecture in use? What version, i.e., VMWare, Hypervisor, Zen, etc.? ***The college would like to treat this as a black box engagement. For security reasons, more detailed information will be provided if selected as a finalist.***
    g. How many databases are in scope and what type, i.e., MS SQL, DB2, Oracle, MySQL, etc.? ***The college would like to treat this as a black box engagement. For security reasons, more detailed information will be provided if selected as a finalist.***
    h. What ERP does JCC have implemented and are the database servers in scope? ***Yes, database servers are in scope. The college would like to treat this as a black box engagement. For security reasons, more detailed information will be provided if selected as a finalist.***
47. Wireless Vulnerability Scanning Questions:
    a. How many Access Points in how many locations? ***The college would like to treat this as a black box engagement. For security reasons, more detailed information will be provided if selected as a finalist.***
    b. What is the current wireless architecture? ***The college would like to treat this as a black box engagement. For security reasons, more detailed information will be provided if selected as a finalist.***
    c. How many authorization servers? ***The college would like to treat this as a black box engagement. For security reasons, more detailed information will be provided if selected as a finalist.***
48. Is a firm(s) providing the proposed services to the College, either currently or recently? ***Not currently contracted.***

    If yes:
    a. Who is the vendor(s)?
    b. For how many years has the College worked with this vendor(s)?
    c. When is/was the work conducted and how similar was it to the services requested in the current RFP?
    d. Will the results of the previous project(s) be shared with the selected consultant?
    e. What was the dollar value of the most recent contract(s) for these services?
49. Does the College have a budget for the services requested? If yes, please provide detail. ***Yes, the college does have a budget for services requested.***
50. On the Wireless Pen test and Assessment. Are the three wireless networks centrally managed by the same wireless controller? ***The college would like to treat this as a black box engagement. For security reasons, more detailed information will be provided if selected as a finalist.***

51. TraceSecurity can tailor our information security risk assessment methodology for many different organizations. Our typical Risk Assessment involves the following asset groups:

Asset	Description
Applications	Asset to represent categorical threats and controls that apply to the organization's key applications.
Data Center	The organization's primary data center facility, housing core information technology components.
Network	The organization's data network, including network appliances, security devices, cabling and firewalls.
Organization	Asset for assigning entity-level threats and controls. Identifies broad categories of threats with impact across the organization.
Personnel	Employees represent a key asset to the organization and a potential target for information security breaches.
Physical and Environmental	A general category for those assets that relate to the physical presence of the organization, such as office locations, data centers, and other facilities.
Records	Physical, hard-copy or media records stored on the organization's premises.
Systems	The category of information systems, such as servers and workstations.
Technical Assets	This asset represents a parent category for the organization's technical environment, encompassing network infrastructure, systems, applications, etc.

52. Would additional asset groups need to be included for this assessment?
    If so, which additional asset groups? ***The college would like to reference the NIST framework. See answer to question 4c.***
53. Is the expectation for the Board/Senior Management presentation to be performed onsite or can it be conducted remotely via remote conferencing applications (Zoom, WebEx, GoToMeeting)? ***Onsite preferred.***
54. Operational Framework Review:
    a. When was the last Operational Framework review completed? ***We would like to start utilizing the NIST framework and the reason for this engagement.***
    b. What were the existing policies and procedures that were included in the prior Security Operational Framework review? ***See answer 54a above.***
    c. Have there been any significant changes to your environment since the prior Security Operational Framework review? ***See answer 54a above.***
55. Penetration Test:
    a. How many IPs are considered in scope for the internal penetration testing?
    For the internal penetration assessment, per the RFP Scope of Work 'Penetration Testing Phase' item number two, the assessment will include at least 10 class C IP ranges.
    b. How many external facing IPs are considered in scope for the External penetration test? ***Per the RFP, 50.***
    c. How many wireless networks will require penetration testing? ***Per the RFP, 3.***
    d. What windows of time will be available for penetration testing (e.g. normal business hours, small windows of evening/ night hours, weekend only, etc.)? ***Normal business hours, as long as the testing does not place overhead on the network. If it is known to do so, then the testing should be done after hours or on the weekend.***
    e. In the case that a system is penetrated, how should the testing team proceed?
    Notify JJC CISO, discuss item compromised, and determine next steps.

f. At what point do you consider the pen-test complete?
    i. Are there particular resources that, if compromised, would be a "game-over" scenario? ***Yes.***
    ii. Should we attempt to gain domain admin access, or gain admin rights to a web application? ***Yes.***
    iii. Should we attempt to install benign malware on any systems? ***Would require further information on the software (benign malware) and its origin.***

56. What kind of devices will we be pentesting – production servers, endpoints, web applications, etc.?
    Yes.

57. Is there anything "off limits" for testing?
    No.

58. Is there any social engineering component to this?
    Refer to the answer given in question 4b.

59. Is there any sort of physical security component to this test?
    Yes, based on NIST frameworks.

60. Is there any sort of phishing component to this test?
    Refer to the answer given in question 4b.

61. Will this be a "black box" pentest where we have no knowledge of the network beforehand?
    Yes.

62. Will we be given any sort of initial foothold (VPN access, a valid guest account)?
    Refer back to question 16 and answer.

63. Are there web applications included in the Penetration Test?
    Yes.
64. What are the JCC business objectives intended to be met by the penetration testing? Is this primarily intended for validation of existing security posture (i.e., evaluation of effectiveness of current controls)? Or should it be focused on discovery and enumeration of vulnerabilities?
    Both, evaluation of effectiveness of current controls (finding gaps) and discovery/enumeration of vulnerabilities
65. Does JCC have current information security and privacy policies that will be available for review during the Operational Framework Review? If so, can JCC provide a list or summary of the policies that exist today? ***Yes, Responsible Use of Technology.***
66. To assist with estimating the size of the engagement, can JCC provide the following details regarding the current IT environment:
    a. Current number of IT staff?
    b. Number of major applications supported?
    c. Estimated server count?
    d. Number of data centers?

    The college would like to treat this as a black box engagement. For security reasons, more detailed information will be provided if selected as a finalist.

End of Addendum #1

DATE: May 2, 2018

Joliet Junior College
1215 Houbolt Road
Joliet, IL 60431

TO:	Prospective Respondents
SUBJECT:	Addendum No. 1
PROJECT NAME:	Information Security Penetration Testing & Operational Framework Assessment
JJC PROJECT NO.:	R18008

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