Procurement Services
Lucas Administrative Center, 617
1 Nunn Drive
Highland Heights, KY 41099
859.572.6605
FAX 859.572.6995

ADDENDUM NO:	**1**
IFB/RFP No:	NKU-41-18
Commodity:	IT Security Audit
Date:	4/27/2018
Due Date:	5/4/2018

BIDDER/RESPONDER SHALL CONFORM TO THE FOLLOWING CHANGES AS SAME SHALL BECOME BINDING UPON THE CONTRACT TO BE ISSUED IN RESPONSE TO THIS INVITATION FOR BID.

The following questions were raised:

1. Does NKU have an internal IT department or is the IT department at NKU outsourced? If NKU's IT department is outsourced, could you please provide the vendor it is outsourced to? If NKU's IT department is supported internally at NKU, has a previous security assessment ever been completed on NKU's network?
   We have an internal IT department. And yes, we have had this audit done a couple of years ago.

2. Are there any required or specific certifications for the Auditor which will be required by NKU?
   The RFP states, "Please include short bios of key personnel as well as qualifications / credentials of employees performing the test". While we do not specifically list a certification we will review the certifications of the people identified as working on the audit for evaluation criteria.

3. Must the Auditor remain onsite throughout the project? If so, what are the normal hours expected (EX: Mon-Fri, 8a.m-5p.m.?) Can the Auditor work remotely?
   We understand that part of the audit will be conducted on site and part of the audit will be conducted remotely.

4. Has the University conducted a third party attack and pen assessment previously, pertaining to any of the described areas (internal, wireless, Internet/web application, vulnerability)? If so, when was the assessment performed?
   Yes, 2008, 2012, 2015

5. Does the University have any outsourced IT functions?
   Yes, SAAS platforms like O365, etc

6. Are there any documented security policies, procedures, standards, and network diagrams?
   Yes

7. What testing procedures does the University expect to comply with compliance and regulatory requirements? Aside from specific guidance in NIST does other University regulations have outlined Pen testing guidance that is required? Eg. PCI compliance?
   Yes, we have compliance regulations but no documented procedures for testing.

8. What is the approximate number/breakdown of internal and external (Internet) devices owned/maintained by the University?
   Internet facing, expect two class C address space.

9. How many firewalls, databases, VPNs, and network segments owned/maintained by the University?
   1 Primary Firewall
   1 Primary VPN cluster.
   Do not have a count of databases.

10. Approximately how many physical locations are in scope for on-site visits/walkthroughs?
    One physical site, This is a University Campus

11. Is the University interested in social engineering physical impersonation to attempt to gain unauthorized physical access to a restricted or secure area?
    Data Center Yes.

12. What is the break down/number of internal wireless networks and public (Internet only) wireless networks?
    1 Public
    3 Primary
    Other SSIDs

13. Under the Wireless Assessment, the University asks for recommendations on 3 tools or reporting systems. We are vendor independent. Does that impact the likelihood of being awarded the contract?
    Looking for recommendations to better manage wireless.

14. If so, how many employees would be targeted for the phishing campaign?
    Today we do not use PhishMe type e-mails. Would be interested in options.

15. For each web application considered in scope, please indicate:
    Number of user forms (data entry forms)
    Modifiable code by University?
    Source code owned by University?
    For vendor software, is University authorized to test the application?
    Number of web servers for each application
    Number of database servers for each application
    Number of application servers, if any
    Testing of both Production and Staging or just one environment?
    Perform authenticated, or Unauthenticated testing?
    For authenticated based testing, please indicate by application the number of user types the University requires to be tested. (e.g. Admin, Power User, User, etc.)
    Do not have this information at this time.

16. Total Number of Servers:
    350 to 400

17. Total Number of Firewall:
    1 Primary

18. Total Number of Virtualisation Hypervisor:
    23

19. Total Number of Desktop:
    Approx. 5000

20. Total Number of Router:
    Approx. 20

21. Total Number of Switches:
    700+

22. Assessment to be done remotely or onsite:
    Expect both from internal and from external.

23. Vulnerability Assessment to be done OR Penetration Testing?
    Both

24. Operating System Details (IOS/Android
    Windows/Linux/AIX

25. In which tab should we describe the services that we are proposing?
    In tab 3

26. Are any distributed IT systems managed directly by the academic colleges and departments? If so, may we assume that they adhere to the same information security policies and procedures established for the University as a whole?
    No, there are systems managed by departments specific to their areas. We are not auditing those,.

27. For Section VI (Risk Assessment), does NKU have a preference for a given cybersecurity framework (e.g. NIST CSF, ISO 27001, CIS)?
    There is not a formal framework but are reviewing NIST due to Federal Regulations.

28. In Section VI, there is a request to create a summary of reviewed policies with recommendations for changes, additions or deletions. Please identify which policies will need to be reviewed (e.g. HIPAA Security policy, Acceptable Use policy, Data Classification policy, Information Security policy, Incident Response Plan, Security Program document, Business Impact Assessment/Business Continuity Plan/Disaster Recovery Plan, GLBA).
    Published NKU policy and Internal IT Policies. We are looking for Gaps and improvements.

29. Has NKU created an inventory of PII/ePHI/PCI cardholder data types, applications and infrastructure components on which they reside?
    No formal inventory

30. Has an inventory been created for those third-party providers that safeguard NKU PII/ePHI/PCI cardholder data?
    No formal inventory

31. Has NKU segmented its network? Please describe.
    NKU does use logical separation of the network.

32. Would we be able to get a current organization chart for IT and for the University as a whole?
    Management level org chart is available to the public.

33. Has NKU recently completed a Cybersecurity Risk Assessment, network penetration test, etc. Would the chosen service provider have access to this information?
    3 years ago. Access to information would need to be discussed.

34. As part of the Internal Network Penetration Test, it is requested that the tester review and assess the Intrusion detection response, including logs. What logging tools are in place? Will the tester be given direct access to the logging tools or will a copy of the logs be provided?
    Current engine is qradar. No access was planned but that can be discussed.

35. NKU has requested that there will be no disruption to network or systems as a result of network testing. While disruption is a rare event, it remains a potential occurrence for anyone performing this service. Would NKU require service providers to accept liability for any or all incidental and/or consequential damages arising from such disruption?
    If tool has been known to cause disruption then the scan would need to be scheduled during the maintenance windows in case of outage.

36. The following question may be unique to BKD, as NKU's financial auditor: AICPA specifies that the indemnification of a client, where any fault may be attributable to client's own actions, would impair the auditor's independence under ET Section 1 .228.020, Indemnification of an Attest Client. This interpretation applies to all CPA firms. BKD currently performs the financial statement audit for the University which requires the auditor to maintain independence. We believe the indemnification requirements stated in Section 23 of the General Terms and Conditions may pose a potential conflict with professional standards. Therefore, if engaged, we would propose to limit indemnification only to the extent the claims, damages, liabilities, loss, etc., result from the services performed and caused by our own negligence or intentional misconduct, so as to not indemnify and hold harmless the University for its own negligence and actions. Would NKU be willing to discuss such revisions with BKD, if selected?
    All things can be discussed.

37. Whether the application contains any content management module (CMS) or any 3rd party package (e.g. Joomla, Drupal, WordPress, Liferay etc).
    Adobe Experience Manager (AEM)

38. Would you need our support for implementing the findings?
    Recommendations for resolution

39. Also please clarify the number of locations in scope
    primary campus

40. if NKU has IT Security policies
    some

41. IT Incident response
    some

42. Business Continuity
    some

43. Disaster recovery
    Some

44. The objectives reference NIST 800-53 as the compliance standard. Is this in addition to the GLBA referenced in Section V?
    800-53 because of Federal Regulation need. In theory if we have 800-53 then most of 800-171 would be in place. This year we are being audited for GLBA.

45. Will offline databases be provided for assessing existence of PII?
    a. Does NKU currently store PHI? No known storage

46. Is scope limited to just internal hosts / devices on the trusted network? Yes
    a. If no, approximately number of hosts / devices to be tested on the external, public-facing network? External is two class C addresses. Not all populated.

47. For internal assessment, approximate number of hosts / devices to be assessed / tested?
    Internal Approximately 350 servers, 5000 PCs, 20 routers, 700 switches, 1 Primary firewall. Sampling method may be needed.

48. Please expand on what is requested re: "operational weaknesses in process…"
    a. Will vendor be reviewing policy, process, procedure and control documentation? Yes
        i. If yes, will vendor be required to validate / test controls, or will attestations in reviewed documentation suffice?

    Attestations in reviewed documentation suffice

49. Is a full log management assessment to be included?
    a. If yes, does NKU have a SIEM system? Yes
    b. If no, will vendor be required to assess log management on individual devices / hosts?

How many devices / hosts are in scope for log management assessment? Not individual logs unless needed.

50. Does NKU have network architectural diagrams and associated documentation?
    High level

51. Will vulnerability and pentesting be conducted as an unauthenticated user, as an authenticated user or both?
    No valid credentials to be provided. Open to discussion.
    Is firewall configuration security assessment to be included? Yes
    a. If so, how many firewalls are in scope? 1 Primary Firewall

52. Is there an active IDS / IPS system in use? No

53. Are wireless devices centrally managed? Yes

54. How many "types" of wireless access does NKU support; i.e. guest, trusted student, trusted staff, etc? ·Public, 3 Primary, Other SSIDs

55. Are BYOD devices to be included in scope? No

56. Are logs currently being collected for wireless access sessions and/or attempted authentication? Yes

57. Does NKU have policy documentation that speaks to wireless usage and access? Yes

58. **Section IV: Internet Assessment & Web Assessment Questions:**

59. How many websites / web applications are in scope; i.e. specific URL's to be tested?
    Email Login, Password Change Page, myNKU and www, listed in the RFP.

60. Is web testing to include unauthenticated testing, authenticated testing or both?
    Unauthenicated

61. Is DDOS testing to be included?
    Yes, but mitigations will needed to be provided is vulnerable.

62. Does NKU have a remote access policy? Yes

63. Is website code analysis to be included?
    a. If so, will source code be provided?
    To be discussed.

64. Has a Gramm Leach Bliley assessment been conducted in the past?
    This is our first year to face GLBA.

65. Regulatory Standards are mentioned in multiple places. Stated below….."Regulations that may be in scope for the University. Examples: HIPAA-HITECH, GLBA, FERPA, State Breach Notification Laws, GDPR."

    Is the vendor to include these baselines / compliance guidelines as part of the risk assessment, or just GLBA? In theory we should not have a control in place or a policy in place with out a corresponding control. Part of the purpoase of the audit is Gap analysis.

66. NIST 800-53 is mentioned in the Overall Objectives portion of Section III. These controls are on our future plate due to Federal Regulations.

67. Is a full Active Directory security assessment in scope? Yes

68. How many internal devices would be in scope? Primary Server segments (approximately 400), sampling of PC endpoints.

69. Are you willing to provide IP addresses for devices in scope? Yes

70. Would remote access be allowed in lieu of on-site access? We would like someone here for the internal assessment.

71. How many locations/ buildings would be in scope? 1 Primary Datacenter, 2 Cores, a sampling of wiring closets.

72. How many locations/ buildings would be in scope? Primary Campus.

73. Approximately how many external devices will be in scope? Two Class "C" address space.

74. Are you willing to provide IP addresses for devices in scope? Yes

75. Would Social Engineering be in scope? Target IT only.

76. For each of the 5 websites, are you expecting uncredentialled testing only, or will there be credentialed testing involved. Uncredential

77. Can you please provide a little more information on what is expected in the Business Area Reviews?
Review of Process and Procedures for a recurring Risk Assessment by the Business units. We are looking for improvements/ gap analysis.

78. For the physical assessment: Is physical access (tailgating) in scope?
Yes

79. Will NKU accept reference letters in lieu of client contact information?
We would like the ability to call and talk to a person.

80. What is the budget for this project?
Yes, there is a budget but do not want to limit the possibilities of the audit.

81. Will you accept a separate redacted proposal for public record?
We cannot accept a separate redacted proposal

82. Page 14, Section IV. A. indicates that the RFP Response should be organized as follows: Tab 1 – Signed Authentication of Bid…; Tab 2 – Cover Letter; Tab 3 – Background, Experience, and References; Tab 4 – Pricing Structure. Under which tab are we to present our Methodology and Approach?
You may attach it in tab 3

83. Page 17, Section H. Occupational License – can this license be obtained post award?
Yes, you can obtain it if awarded

84. How many IP addresses or network ranges will be in scope for the internal testing? Unknown
Of the above IP ranges, approximately how many live devices?
What approximate percentages of these live devices are servers (physical and virtual), workstations, network devices and other systems? (for example, 25% servers, 50% user systems, 25% network devices)
Internal Approximately 350 servers, 5000 PCs, 20 routers, 700 switches, 1 Primary firewall. Sampling method may be needed.

85. Will our testers be able to reach all of the devices identified in question 2 from one centralized location? That is, will testers have to physically move locations to reach all the devices?
Varies based on VLan

86. Is remote testing an option?
Note: For remote testing we utilize the RSM Nomad appliances that allow us to perform testing in the same manner as if we were on-site without incurring travel costs. Additional materials can be provided.
Would need to be discussed. Expecting person on site for internal testing.

87. Are any systems handling payment card data in-scope for this assessment and other assessment sections? That is, would the testing have to align with PCI requirements to validate network segmentation and other PCI controls?
We have PCI networks. PCI is one of the reasons for this assessment.

88. How many facilities (network cores, datacenters) are to be evaluated for physical safety and security?
1 Campus, 1 data center, sampling of cores.

89. Approximately how many wireless access points are in scope for this assessment?
800 access poits through a central wireless controller.

90. Are wireless attacks against wireless clients in scope? For example, establish rogue access points or perform DNS spoofing. Yes

91. What are the external IP ranges that are in-scope for the testing? 2 Class C addresses

92. Do you have Intrusion Prevention services (either on-site appliances or a third-party service) in place that may interrupt the testing? Note: We typically leave the defenses in place for the first round of testing to validate they are working correctly, then have our testing systems white-listed for a second round of testing in order to produce accurate results. No

93. For testing of myNKU, are multiple roles desired for testing? For example, student, faculty, administrator. Would need to discuss for authenticated testing

94. Does a current information classification and data inventory already exist? Yes

95. Can the GLBA assessment be executed side-by-side with the Risk Assessment? Yes

96. Is the scope of the assessment the NKU Office of Information Technology or campus-wide?
    NKU Campus

97. Are any specific frameworks or methodologies desired? For example, NIST or ISO.
    No. We are interested in NIST due to Federal Regulations.

98. When was the most recent IT Security Assessment performed? Will this assessment be made available for review prior to submission of proposals?
    2015 , open for discussion. New audit with new eyes. In case something was missed in prior audit.

99. Is the IT Organization Chart available for review prior to submission of proposal? If not, can you please provide a list of key IT sub departments or areas and the number of personnel in each?
    Management level is available to public. Open for discussion for detail.

100. On Page 6 of of the RFP it states that "NKU's information systems infrastructure is composed of 2 Network cores, 11 buildings with a primary router, 350 switches, and 800 wireless access points. Wireless has both public and organization access. Servers include 200 Windows Servers, 50 Linux, and others. 5,000 managed endpoints. 8,000 BYOD undocumented devices a day on the network. IT has 80 employees."
    How many physical locations are to be included in Section II Physical Security Assessment?
    Primary Data Center, and spot check of cores. All on the same campus.

101. Does the University expect 100% testing, or is sampling acceptable? If sampling is acceptable, does NKU have a pre-determined coverage expectation, or will the sampling and related coverage be at the discretion of the consultant?
    Entire Internet facing IP ranges, (Two class Cs) Sampling is acceptable.

Please contact Ryan Straus with any questions.

THE END