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-31-20
Commodity:	IT External Control Testing
Date:	4/22/2020
Due Date:	4/28/2020 @ 2PM

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.

1. **We will be extending the proposal deadline to 4/28/2020 at 2 PM.**
2. Questions and answers are attached.

END OF ADDENDUM

RS-4/22/2020

NKU-31-20 IT Security Controls Annual Assessment and Reporting

Begin Vantage Questions

1. Given recommendations from the CDC regarding travel and the Coronavirus Disease 2019 (COVID-19), to what extent are the dates outlined in the project schedule negotiable? We are curious as to the degree of flexibility you wish to have to deal with current health concerns for the fiscal year 1 assessment to be conducted on campus in May-June 2020.

NKU: Due to the unforeseen restrictions COVID-19 has placed on businesses, NKU can be flexible and conduct the assessment remotely, or with some hybrid of video, screenshot or photo recordings used to validate information to ensure assessment necessarily retains data integrity.

2. Is NKU willing to accept electronic (e.g., email, cloud storage dropbox, or secure file transfer) instead of mailed, physical RFP responses given COVID-19 business disruptions (RFP p. 7, §3.6)?

NKU: InfoSec is okay with this if NKU Procurement is.

3. here are only 7 days between the question submittal date and proposal submission date. What date can bidders expect answers to the submitted questions?

NKU: Due to the COVID-19 outbreak, new date as follows:

- Answers to questions: Friday 4/24
- Bidder submissions due: Friday 5/8
- NKU Selection made: Between Friday 5/15 – Friday 5/22

4. Are there internal deadlines, major milestones, or events driving the timeframe for the project described in the RFP so we can be sure to provide you the information required at the time you need it?

NKU: Yes. Fiscal year ends June 30, 2020 – Selected bidder should be prepared to try to complete assessment by that date, if possible. There may be flexibility due to impact of COVID-19.

5. Vantage appreciates our clients' generosity in providing references for our firm and we do not wish to overwhelm our clients with reference requests. We are glad to provide a detailed list of customer references for similar projects (RFP p. 12, §5.0) upon being named a finalist for the project. Is this acceptable?

NKU: Yes, this is acceptable.

6. Do you have a budget in mind for this project and can you share that with us? By understanding your budget expectations, bidders can maximize their scope of work within your financial constraints and recommend ways to meet your requirements with your budget.

NKU: There are budgetary numbers affixed to this project, but NKU would rather bidders not limit the project scope to meet budgets. Instead, NKU prefers if you have different assessment sizing please provide line item or ala-carte style pricing or bidders may provide a small/medium/large approach to pricing.

7. In our experience, cybersecurity assessments of the type outlined in the RFP typically involve a single onsite visit, spanning several days, to conduct the assessment, with final results presented to the project team in a video conference. Is this acceptable?

NKU: This is acceptable, also with considerations from questions #1 about travel restrictions due to COVID-19.

8. Would you be willing to consider video conferencing for project meetings with the winning bidder, wherever practical, to minimize travel expenses?

NKU: Yes

9. Has any type of assessment similar to that described in the RFP been done in the past, and if so, will the results of that assessment be made available to the winning bidder during the engagement?

NKU: A risk assessment was performed in 2018. Results may be made available to the bidder, once the context is understood. Prefer bidders approach this as a new engagement with no previous assessments performed.

10. Are you willing to share a list of all bidders who have expressed an interest in this project?

NKU: Ryan? Not sure about this one

11. Is there an incumbent and are they eligible to bid on this project? If so, who was the incumbent?

NKU: A company was used for the single 2018 assessment, but wouldn't consider them the incumbent.
Ryan: would we name BKD in this situation? I don't see why they need to know this…

12. Will all potential bidders receive copies of all submitted questions and answers issued as an addendum to the RFP?

NKU: Yes

13. Please list the executive sponsor for this project and describe the working relationship between stakeholders that the winning bidder needs to support in the project.

NKU: The executive sponsor for this project is the Chief Information Security Officer within the Office of Information Technology. The CISO and select stakeholders from the project office, compliance, and operations will support the winning bidder to perform and complete the controls assessment. The CISO will review and approve the scope of the assessment, support the assessment activities, and approve the final report.

14. Please describe how information technology operations are provided at NKU?

NKU: Central IT operations are insourced and on-premise mostly. Some colleges and departments use cloud services, that are generally reviewed by IT for approval during the procurement process. NKU

Central IT leverages cloud offerings of Office 365 for communications, and Canvas for LMS. No IT operations are currently outsourced.

a. Are services centralized or decentralized? NKU: NKU IT is a centralized operation, but departments and colleges have some autonomy for computer and server operations for academic use.
b. If services are decentralized, please clarify NKU: See answer directly above. An example is the College of Informatics maintains a separate set of VMs for use in their cybersecurity classes. NKU IT assists and supports "light" – but the college oversees their server patching, operations, and maintenance. They are setup on a separate network.
c. Which decentralized IT units are included within the RFP scope. NKU: None at present or foreseeable. The assessment may identify issues with controls between central IT and departmental IT operations for remediation.
d. RFP p. 12, §4.4, "Supplementary Information," references a College of Nursing, the University of Kentucky College of Medicine, and NKU's College of Informatics cybersecurity program. Are the IT systems and units supporting these departments included within the RFP scope of work? NKU: No – these departments may designate faculty or students who act as ad-hoc system or application administrators. This information is for awareness for conducting the assessment, in case controls may be found to be inadequately controlling sensitive data from those colleges or on-campus entities.
e. Please provide an organizational chart for your information technology unit(s). NKU: That is proprietary information and may only be shared with the winning bidder after approval of the CIO is provided.

15. Do you have a current IT asset inventory, cataloging your IT assets, services, and data?
NKU: NKU does not current use a CMDB, but could produce a rough list of hardware and software assets through SCCM and Active Directory. Any specific lists would have to be created manually.

16. Do you have a current service catalog, outlining the services provided by NKU information technology units?
NKU: Yes, you can find this on the NKU IT website: https://inside.nku.edu/it/service-catalog.html

17. Can you provide information size of the overall NKU technology environment?
a) Number of employees? Roughly, 2,500 faculty and staff FTE
b) Number of Servers? Roughly 300, mixture of physical and virtual, 99.9% hosted onsite with ESX
c) Number of laptops & desktops (workstations)? Managed end points: Roughly 2,500 - 3,000, including all on-campus computer labs. There are several unmanaged devices that students and faculty bring to campus and are allowed to use the network (but not join AD). It is estimated to be between 3,000 to 5,000 average daily unmanaged devices on the network, including laptops, cell phones, tablets, and other IoT devices
d) Number of switches: 800 physical, 230 in stacks, routers: 17, firewalls: 2 e) Number of internet connections? 2

18. Do you have any proprietary IT systems (built specifically for you)?
NKU: Limited to interfaces between COTS systems, however select COTS systems are very old and unsupported (Ex. Infra ticking system)

19. Do NKU information technology units support any classified research? If so, are the IT systems that support that research in scope for the project.

NKU: Currently, NKU IT is not aware of any classified research projects occurring in any college.
END Vantage Questions

BEGIN CLA Questions

1. Have you had an IT security controls assessment completed before?

NKU: (Answered in Vantage, Q9) A risk assessment was performed in 2018. Results may be made available to the bidder, once the context is understood. Prefer bidders approach this as a new engagement with no previous assessments performed.

2. Have you had a GDPR Data Protection Impact Assessment (DPIA) completed?

NKU: No

3. Is the IT infrastructure centrally managed?

NKU: (Answered in Vantage, Q14a-d) Yes

4. Will you be looking for more than one report (different departments)?

NKU: No, only a single, comprehensive report

5. How many applications are in scope? How many contain, process, or transmit ePHI data?

NKU: At minimum, seven (7) applications with one (1) of the seven potentially storing, processing or transmitting PHI data. In addition to the seven applications 2-3 core, shared infrastructure applications will be included (Office/Exchange 365, Active Directory at minimum). More may be identified as necessary dependencies during initial project meetings.

6. Are you looking for an internal vulnerability assessment and external penetration testing as part of the assessment?

NKU: Internal vulnerability: We would like line item pricing to conduct vulnerability scanning as a value-add. External penetration testing: No

7. Are there documented policies/procedures for the core IT processes
    a. Change Management: NKU: Yes, and is currently being updated (April 2020)
    b. Software Development: NKU: SAP: Yes
    c. Incident Management: NKU: Yes
    d. DRP/BCP: NKU: Yes
    e. Logical Access Management: NKU: Yes
    f. Backup/Recovery: NKU: Yes
    g. Other: NKU: Security Policy, Data Classification Policy, Acceptable Use Policy, Data and Web privacy policy, records management policy

8. Given the recent developments with COVID-19 is it still required that we mail the proposal, or are we able to submit via email?

NKU: (Answered in Vantage Q1): Due to the unforeseen restrictions COVID-19 has placed on businesses, NKU can be flexible and conduct the assessment remotely, or with some hybrid of video, screenshot or photo recordings used to validate information to ensure assessment necessarily retains data integrity.

END CLA Questions

BEGIN JANUS Software Questions

1. Page 1, Item 5 states "That the Offeror, and its affiliates, are duly registered with the Kentucky Department of Revenue to collect and remit the sale and use tax imposed…and will remain registered for the duration of any contract award." May we register our company with the Kentucky Department of Revenue post award or do we have to register prior to submitting our proposal?
   NKU: This is a procurement dept question, correct?
2. The RFP states that proposal are due 4/17/20 but NKU's Online Planroom states that proposals are due 4/18/2020. Since 4/18 is a Saturday is it safe to assume that what is posted on the website is incorrect?

NKU: (Answered in Vantage Q3): Due to the COVID-19 outbreak, new date as follows:

- Answers to questions: Friday 4/24
- Bidder submissions due: Friday 5/8
- NKU Selection made: Between Friday 5/15 – Friday 5/22

3. In light of COVID-19 will you consider accepting proposals via email?

NKU: Ryan question

4. Are you still planning to require on-site performance?
   NKU: (Answered in Vantage Q1): Due to the unforeseen restrictions COVID-19 has placed on businesses, NKU can be flexible and conduct the assessment remotely, or with some hybrid of video, screenshot or photo recordings used to validate information to ensure assessment necessarily retains data integrity.

5. Page 12, top of page. Is a separate executive summary document required or will a separate section suffice?
   NKU: A separate section will suffice under a single, comprehensive report document.

6. Scope. Is this a review of policies, functions alone or is there a technical component included to assess the technical risks? NKU: Comprehensive review of policies, functions and select technical components for seven (7) applications and select technical systems
   If so, how many of the following are to be included:
   a. Number of users? NKU: To be discussed and determined. For policy, function, and technical assessment, there will be at least 10 to 15 IT users to work with or interview. Select Non-IT users/business process owners may be included.
   b. Number of IPs in scope?: To be determined, but minimum of 50 IP addresses associated to the seven (7) applications and select technical systems
   c. Number of firewalls: NKU: 2, routers: NKU: 17, switches: NKU: 800, 230 in stacks? Not all may be in scope
7. Number of applications in scope? NKU: seven (7) applications and 2 -3 select technical systems
   a. Number of devices in scope and type?
   b. NKU: approximately 25 systems, mixture of x86 and RISC based physical and virtual (both hard and soft partitioned)

c. What operating environment is in place – Windows, UNIX, etc.?
NKU: AIX, Windows 20XX, select Linux, F5 load balancers

8. Page 11, Assessment Report Content, 5th bullet. Are 3rd parties to simply be identified or are we to identify their issues? NKU: As much information that can be provided - within reason - about the issue(s) so there is context to investigate and remediate. Example: Microsoft O365 is sending plaintext AD usernames to IP XXX.XXX.XXX.XXX at minimum, not just a simplified response like "Microsoft is sending sensitive data to an internal or external server". should be provided If so,
    a. How does each one in scope interface with the University's technology?
    NKU: The third parties we sanction interface mostly through API calls at the application level, and use our on-site AD for authentication.
    b. How many are in-scope?
    NKU: (Answered in CLA Q5): At minimum, seven (7) applications with one (1) of the seven potentially storing, processing or transmitting PHI data. In addition to the seven applications 2-3 core, shared infrastructure applications will be included (Office/Exchange 365, Active Directory at minimum). More may be identified as necessary dependencies during initial project meetings.
9. Is remote computing in-scope (in the time of COVID-19)?
NKU: Yes, including NKU usage of VPN.

END JANUS Software Questions

NKU IDS/IPS RFP Q&A

Begin Trace3 Questions

1. Do you know the baseline aggregate throughput you would like the IPS/IDS device(s) to be able to achieve in an inline posture day one? (We will add the growth statistics requested for the final solution)

   NKU: NKU prefers not to have an inline posture starting day one – rather NKU would like to use port mirroring/spanning or TAPS to only analyze the traffic for year 1, possibly year 2 in order to remove any possibility for operational disruption.

2. For TAP and/or eventual inline placement, would a single set of redundant appliances with enough 10G interfaces work in your topology, or would you need separate appliances for some applications?

   NKU: Yes, a single set of redundant hardware (minimum of 2) is acceptable. The major technical requirement is that IDS/IPS needs to handle MPLS traffic.

3. If so, how many? Trace3 assumes a set of two interfaces inline per each of the 4 zones you wish to monitor (total of 8 not including management). In TAP mode one interface from each set would be used.
4. NKU: Two interfaces (one interface from each set) with an aggregate capacity of 20Gbps should suffice per zone.

5. When you reference the ability of the IPS to "fail open", do you require fail to wire interfaces.

   NKU: FTW is preferred, but not a hard requirement. Lossless packet transfer is preferred but not required. For the foreseeable two-year operational window, the NIDPS should not have the direct capability to impede or affect network traffic (even if operating outside of the appliance scope) – it should only be analyzing and reporting on network traffic.

Would these interfaces need to be short or long range fiber (LR or SR)?

NKU: We use single mode fibre to connect campus buildings.

Do you have Cisco Identity Services Engine passive identity connector functionality in place today in your ISE deployment? If not, is ISE already integrated with your Active Directory environment?

NKU: ISE is currently integrated with Active Directory Federated Services on campus.

Per the statement "Allow for encrypted and non-encrypted network traffic without special configuration": do you require SSL decryption capabilities on the IPS, or just the ability to pass encrypted traffic?

NKU: We do not want SSL decryption capabilities for the foreseeable (<=2 years) operational window. NIDPS should just pass it.

For the 3 customer references, is it acceptable if the reference customers are using our chosen OEM vendor IPS/IDS solutions, but not necessarily the same size hardware recommended for the RFP, provided that the capabilities are the same?

NKU: Yes, this is acceptable.

END Trace3 Questions

Begin CBTS Questions

On page 15, under the "proposed solution must" section it states we must: provide 24x7 monitoring and response to incidents, activities, and critical events. It then goes on to say, IF the solution will be provided as a managed service on page 16.

Which would you like to see proposed? NKU managed as the prime response and Service Provider MS as a secondary option?

NKU: Both if the vendor can also act as a MS provider – one cost for hardware/software/service with internal NKU team acting as the prime response team and a second, separate cost where the service provider provides the hardware/software/service and also acts as the primary response team. If a bidder only once to bid on one or the other solutions, that is also acceptable.

END CBTS Questions