ADDENDUM #2
Cybersecurity Vulnerability Assessment and Penetration Testing
Q&A Posted: 11/14/2024 RFP Open: 11/21/2024
QUESTIONS AND ANSWERS

QUESTIONS SUBMITTED: 76

QUESTION 1: Can the proposal be submitted via email?

CCFC ANSWER TO QUESTION 1:
No. Submissions must be mailed or dropped off to Campbell County Finance, 1098 Monmouth St. Ste 322, Newport, KY 41071 at any time prior to the RFP opening at 10:00 AM Eastern on November 21, 2024.

QUESTION 2: Can business licenses be sent alongside the submission.

CCFC ANSWER TO QUESTION 2:
Yes.

QUESTION 3: When are you looking to begin this project?

CCFC ANSWER TO QUESTION 3:
Potentially beginning the first quarter of 2025 if approved by the Fiscal Court and contracts signed.

QUESTION 4: How many servers are in scope?

CCFC ANSWER TO QUESTION 4:
40+ servers.

QUESTION 5: How many workstations are in scope?

CCFC ANSWER TO QUESTION 5:
300+ workstations.

QUESTION 6: How many of the total IP addresses are expected to be responding to active probes (live IP)?

CCFC ANSWER TO QUESTION 6:
We have listed up to 1,300 IP's with the idea some won't be online or we give priority to only 1,300 devices.

QUESTION 7: Are there web applications or web sites in scope?

CCFC ANSWER TO QUESTION 7:
There are about 10 – 15 sites that are currently websites, portals, or hardware device interfaces. The list was for up to 30 to cover our current list and any growth during this contract.

QUESTION 8: Are any of the IP addresses in scope hosted in a cloud provider (e.g. AWS, Azure, Google, others)?

CCFC ANSWER TO QUESTION 8:
Currently none are hosted in AWS, Azure, or Google. Our website and a few portals are hosted by them and we are unaware of their exact host location.

QUESTION 9: Is there currently an incumbent company or previous incumbent, who completed a similar contract performing these services?

CCFC ANSWER TO QUESTION 9:
There is no incumbent. This will be the first vendor to complete the requested work.

QUESTION 10: Specify the VLAN details – how many are included in the scope.

CCFC ANSWER TO QUESTION 10:
4 VLANs

QUESTION 11: Can you please provide the current number of infrastructure details (Physical Server, Virtual Server, Network Devices, etc.)?

CCFC ANSWER TO QUESTION 11:
Up to 1,300 total devices. (300+ Windows workstations, 30 printers, 15 standalone systems, 40+ servers, 300 Ip phones, 50+ access points. Additional network devices and mobiles up to the 1,300 total.)

QUESTION 12: How much (%) of the infrastructure is in the cloud?

CCFC ANSWER TO QUESTION 12:
None.

QUESTION 13: In the IT department/environment, how many employees?

CCFC ANSWER TO QUESTION 13:
Four employees.

QUESTION 14: Do you manage your own data center, or do you utilize any 3rd party/colocation facilities?

CCFC ANSWER TO QUESTION 14:
Manage our datacenters and none are in 3rd party/colocation facilities.

QUESTION 15: Is there a funding/financial/budget range estimated?

CCFC ANSWER TO QUESTION 15:
CCFC is not currently advertising the budget for this project.

QUESTION 16: According to Section D. Pricing Point 4 on RFP page 2, "Quotations must be submitted on the bid price sheet indicating unit price, total extension of each item, and grand total of bid." We were unable to locate any bid price sheets.

CCFC ANSWER TO QUESTION 16:
Vendors are strongly encouraged to submit attachments with their proposals providing a fully detailed quote or build-out with separate line items.

QUESTION 17: Is a bid bond or performance bond needed?

CCFC ANSWER TO QUESTION 17:
At this time, bid bond is required for 5% of the grand total of any proposal exceeding $99,999 and performance bond for 100% of the grand total of any proposal exceeding $99,999 as CCFC will be utilizing federal funds for the project.

QUESTION 18: Are foreign/non-US companies permitted to submit a proposal?

CCFC ANSWER TO QUESTION 18:
Yes. If there is a cost difference between US testers and testers based elsewhere, please list them on the bid sheet.

QUESTION 19: Do you use Cloudflare or something similar?

CCFC ANSWER TO QUESTION 19:
No.

QUESTION 20: Can we scan web apps in a test environment or can we poke a hole to scan your web apps?

CCFC ANSWER TO QUESTION 20:
Currently the web application testing will be mostly websites that are informational, portals, or hardware devices that face external.

QUESTION 21: Can CCFC elaborate on the request for "User profiling and reputational threats" as part of the external network vulnerability assessment and penetration testing?

CCFC ANSWER TO QUESTION 21:
These external tests include VPN and other login access devices.

QUESTION 22: Regarding web application penetration testing of 30 sites, are these sites custom home-grown web applications or commercial off-the-shelf solutions?

CCFC ANSWER TO QUESTION 22:
The sites are a combination of our county website, portals for access to software, or hardware.

QUESTION 23: Regarding web application penetration testing of 30 sites, is CCFC seeking black-box web application testing (i.e., testing from the perspective of a completely unauthenticated attacker), or is CCFC seeking more in-depth authenticated greybox or whitebox web application testing?

CCFC ANSWER TO QUESTION 23:
Testing from the perspective of an unauthenticated attacker. With most of these not-our-own developed or hosted sites, we are looking to ensure the access is secure and if any vulnerabilities are found.

QUESTION 24: Regarding web application penetration testing of 30 sites, will each of the 30 sites receive 1 round of penetration testing and 4 rounds of vulnerability scanning per year, or are they only to receive 1 round of penetration tester per year?

CCFC ANSWER TO QUESTION 24:
The idea is that each of the sites would receive 1 round of testing per year as well as optional remediation scan.

QUESTION 25: Do the ~30 IP addresses that will be in scope for external penetration testing correlate to the 30 sites that will be in scope for web application penetration testing? i.e., is there overlap in targets between those two phases (and if so, do these completely overlap, or only partially? If partial, how much overlap is there)?

CCFC ANSWER TO QUESTION 25:
The 30 IPs are a combination of external IPs the county owns/uses. The up to 30 web applications are websites, portals, or other external facing sites the county users use.

QUESTION 26: Are each of the 30 sites to receive 1 penetration test per year AND 4 vulnerability scan per year?

CCFC ANSWER TO QUESTION 26:
The 30 web applications are to receive a single test and optional remediation scan to follow.

QUESTION 27: The RFP states that work is to be performed consecutively until project completion and that no breaks in service other than weekends and/or recognized holidays should occur; however, the services being requested may be insufficient to allocate personnel every business day for 4 years unless in-depth web application penetration testing of all 30 web applications is desired. IE, after completing one discrete penetration test or vulnerability scan and delivering the report, there may be a significant gap in time in which there is no work to perform until the time for the next vulnerability scan arrives) - can CCFC clarify the desired meaning of the RFP's mention of no breaks in service other than weekends and/or holidays? Does CCFC wish for a continuous testing model where there is work being performed on every business day of the year?

CCFC ANSWER TO QUESTION 27:
The intended wording is per scan or test and is to ensure everything is completed all at one time rather than be stretched out over multiple weeks. Example: If the project requires 7 days of work and it begins on a Monday that it should be completed the following Tuesday with the assumption of no holidays and the only days off would be the 2 day weekend.

QUESTION 28: Regarding vulnerability scanning, is CCFC looking for raw vulnerability scan results, or is CCFC looking for curated vulnerability scan results that are manually tested and validated and have false positives ruled out?

CCFC ANSWER TO QUESTION 28:
Ideally false positives are ruled out to reduce the process for our staff.

QUESTION 29: What is the deadline to have the RFP response to CCFC?

CCFC ANSWER TO QUESTION 29:
November 21, 2024 at 10:00 AM Eastern Time.

QUESTION 30: Is a cashier's check acceptable in place of a bond?

CCFC ANSWER TO QUESTION 30:
No.

QUESTION 31: Is CCFC available for a private call to discuss the project?

CCFC ANSWER TO QUESTION 31:
No. We cannot have private calls with any vendor prior to opening the proposals, as this would grant an advantage not available to all vendors.

QUESTION 32: How can businesses from out of state, which are not part of the Commonwealth, qualify to bid on local contracts, or are there any special exceptions available for out-of-state bidders?

CCFC ANSWER TO QUESTION 32:
Out of state vendors are encouraged to submit proposals and CCFC regularly does business with out of state vendors. If all work is done remotely, Campbell County business license is not required. Active SAM.gov registration is required as federal funding will be used for the project.

QUESTION 33: Section H.2 states "CCFC reserves the right of renewal for any service and maintenance contracts that may be needed for a minimum of two (2) one (1) year periods." As these renewal dates would be for years 5 and 6 of the agreement, do you need pricing on these renewals up front or is this simply stating if we win the RFP and you are happy with the service in the first 4 years, you have the right to renew years 5 and 6 without going to RFP, but by coordinating directly with the provider?

CCFC ANSWER TO QUESTION 33:
This language provides a mutual option of renewal between CCFC and vendor without going back to RFP. A contractor's agreement for the stated four-year agreement will be available to review after the award.

QUESTION 34: In section III. Proposal Specifications under subsection B.a.ii, the county lists roughly 1,300 internal IP's. Does the county want a full vulnerability test **and** penetration test against all systems or can the vendor work with the county to sample a representative set of systems for penetration testing to reduce testing hours and costs? Also, are all 1,300 IPs expected to have live systems/devices or is the actual set of live systems/devices lower than the number of specified IPs?

CCFC ANSWER TO QUESTION 34:
The total number may not include all live systems but the expectation will include all IPs. Public IPs and web applications are listed higher than current counts.

QUESTION 35: In section III. Proposal Specifications under subsection B.a.iii, the county states that there are 30 applications to be scanned. Is the expectation to perform authenticated scans and manual testing against all applications, or is the expectation to perform unauthenticated testing? Can the county specify how many of the 30 applications are commercial-off-the-shelf (COTS) applications versus applications designed by or specifically for the county?

CCFC ANSWER TO QUESTION 35:
To perform unauthenticated testing. The current county web applications is less than 30 but we are including as changes and new sites come on board. These sites are not all hosted by the county and may include our websites or web applications used for purposes with county data. We are unsure of whether these are commercial or customized applications.

QUESTION 36: Web Application Penetration scanning (Up to 30 sites) - **is this web application vulnerability scanning only?**

CCFC ANSWER TO QUESTION 36:
Yes.

QUESTION 37: Testing should include 1 Penetration test per year. **- 1-External network penetration test, 1-Internal network penetration test, and 1-Web application penetration test. Please confirm**

CCFC ANSWER TO QUESTION 37:
The penetration testing should include external network, internal network and web applications hosted/owned by the Campbell County. Web Application vulnerability scans may include additional sites used by and storing county data but not owned by the county.

QUESTION 38: What's the scope of the 4 vulnerability scans? Does the scope include external network, internal network, and all 30 web applications?

CCFC ANSWER TO QUESTION 38:
The vulnerability scans will be external/internal networks. Web application vulnerability scanning will be once a year.

QUESTION 39: Out of 30 sites, only 1 web application will have a penetration test. Please confirm.

CCFC ANSWER TO QUESTION 39:
The penetration scanning covers IPs given for external and may or may not include some of the web application ports. The web application scan is separate and to also be done once per year. If approved and coordinated with the IT Director for Campbell County Fiscal Court these can be scheduled in different quarterly windows.

QUESTION 40: Are you looking for only organizations that are in Kentucky?

CCFC ANSWER TO QUESTION 40:
No. Companies outside of the State of Kentucky are strongly encouraged to submit proposals.

QUESTION 41: Should we fill out the Resident Bidder Status form?

CCFC ANSWER TO QUESTION 41:
You only need to fill out the form if your company is claiming resident bidder status in the state of Kentucky – this is standard language in CCFC RFP's. Not meeting the requirements for resident bidder status does not preclude you from submitting a proposal or being awarded the project – **CCFC will award the project to any company (inside or outside of Kentucky) that offers the best value for the County**.

QUESTION 42: Are we allowed to sub-contract this opportunity that benefits the Campbell county in achieving its objectives of this RFP?

CCFC ANSWER TO QUESTION 42:
Campbell County Fiscal Court is not imposing any restrictions on proposals but all sub-contractors should be listed with outlined roles in the bid. Evaluations of the proposals will be made during the review process.

QUESTION 43: Can we factor the scope of this RFP with offshore resources? We have observed that onshore is preferred but are we allowed to use the offshore resources for this scope of work?

CCFC ANSWER TO QUESTION 43:
Campbell County Fiscal Court are not imposing any restrictions on proposals but all off-shore should be listed with outlined roles in the bid. Evaluations of the proposals will be made during the review process.

QUESTION 44: III.B.b.iii, it is stated that there are up to 30 sites (in III.B.a.iii), but then the ask is for 1 web application per year. I want to confirm that the 1 Web application penetration test per year is for all of the sites (up to 30) and not just 1 web application of the possible 30 per year.

CCFC ANSWER TO QUESTION 44:
This is for 1 Web Application penetration and vulnerability scan per year for up to 30 sites.

QUESTION 45: Will the amount of IPs to be tested subject to change during the contract period?

CCFC ANSWER TO QUESTION 45:
The agreement will be up to the included numbers. If any devices are above the numbers then Campbell County Fiscal Court will determine per scan/test if only certain ranges or segments are included.

QUESTION 46: In regards to pentesting, If there are remediation findings, will the Campbell county team expect a retest after remediation is resolved? And what would be the expected timeline for a retest post remediation.

CCFC ANSWER TO QUESTION 46:
Yes, for the pentesting we would like remediation test to confirm any remediated steps were completed successfully and should be run within 45 days.

QUESTION 47: What is permissible for penetration testing conducted by contracted companies, both for national and international testers?

CCFC ANSWER TO QUESTION 47:
Vendors should describe the solution or method recommended as part of the proposal and it will be evaluated. The county does not have a response for guidance related to this item.

QUESTION 48: Will our IP be whitelisted?

CCFC ANSWER TO QUESTION 48:
Yes, it can be added during testing.

QUESTION 49: Regarding internal network penetration/vulnerability testing, do you require credentialed scanning?

CCFC ANSWER TO QUESTION 49:
No, unauthenticated.

QUESTION 50: Regarding internal network penetration/vulnerability testing, how are the assets separated - broadcast domains? By VPNs? By VLANS?

CCFC ANSWER TO QUESTION 50:
Vendors should describe the solution or method recommended as part of the proposal and it will be evaluated. The county does not have a response for guidance related to this item.

QUESTION 51: Regarding internal network penetration/vulnerability testing, what are the subnet sizes?

CCFC ANSWER TO QUESTION 51:
Most locations are /24, a couple /22.

QUESTION 52: Do you utilize Microsoft Intune?

CCFC ANSWER TO QUESTION 52:
No

QUESTION 53: Do you utilize site-to-site VPNs?

CCFC ANSWER TO QUESTION 53:
Remote users use VPNs but not site to site VPNs.

QUESTION 54: Regarding Application Security Penetration Testing, how many applications are in-scope?

CCFC ANSWER TO QUESTION 54:
Vendors should describe the solution or method recommended as part of the proposal and it will be evaluated. The county does not have a response for guidance related to this item.

QUESTION 55: Will application testing take place in a Production or Quality Assurance (QA) environment?

CCFC ANSWER TO QUESTION 55:
Production

QUESTION 56: Will login credentials be provided for testing each of the roles supported by the application?

CCFC ANSWER TO QUESTION 56:
No, unauthenticated testing only.

QUESTION 57: Approximately how many pages comprise each application?

CCFC ANSWER TO QUESTION 57:
Vendors should describe the solution or method recommended as part of the proposal and it will be evaluated. The county does not have a response for guidance related to this item.

QUESTION 58: Do you require an assessment of your Information Security (IS) Policies and Procedures?

CCFC ANSWER TO QUESTION 58:
No.

QUESTION 59: Might you be interested in a NIST CSF 2.0 Framework Assessment?

CCFC ANSWER TO QUESTION 59:
Vendors should describe the solution or method recommended as part of the proposal and it will be evaluated. The county does not have a response for guidance related to this item.

QUESTION 60: Might you need any security awareness training?

CCFC ANSWER TO QUESTION 60:
No.

QUESTION 61: Is Social Engineering testing in-scope?

CCFC ANSWER TO QUESTION 61:
No.

QUESTION 62: Might any of the following assessments also be in-scope:

- Server Evaluation Assessment (Physical and Virtual)
- Data Store Review and Security Assessment
- Microsoft AD, Azure AD and O365 Configuration Assessment
- Mobile Device Management Assessment
- Firewall Assessment
- Network Architecture Evaluation
- Email Security Assessment

CCFC ANSWER TO QUESTION 62:
Vendors should describe the solution or method recommended as part of the proposal and it will be evaluated. The county does not have a response for guidance related to this item.

QUESTION 63: Can you be more specific as to the application for the Business license issued by the Occupational License Department of Campbell County? The county website shows many different application forms.

CCFC ANSWER TO QUESTION 63:
Occupational License is required if work is to be done on-site within Campbell County. Form can be found at https://campbellcountyky.gov/division/blocks.php?structureid=49 > Business License Application

QUESTION 64: Will the internal penetration assessment include physical security awareness testing? If so, please list out the number of locations to be tested.

CCFC ANSWER TO QUESTION 64:
No, this RFP does not include physical security awareness testing.

QUESTION 65: Out of the total number of 30 IP Addresses / host, how many total services are available from the Internet?

CCFC ANSWER TO QUESTION 65:
Vendors should describe the solution or method recommended as part of the proposal and it will be evaluated. The county does not have a response for guidance related to this item.

QUESTION 66: Will the external penetration assessment include authenticated web application testing?

CCFC ANSWER TO QUESTION 66:
No, this will be unauthenticated testing.

QUESTION 67: Please clarify if number of websites to be tested, either authenticated or unauthenticated, for the web application assessment.

CCFC ANSWER TO QUESTION 67:
This will be unauthenticated testing for up to 30 sites tested once per year.

QUESTION 68: Will the external penetration assessment include email and/or phone social (phishing attacks)?

CCFC ANSWER TO QUESTION 68:
No.

QUESTION 69: Can scanning occur from one network location or will multiple scanning agents / appliances be deployed?

CCFC ANSWER TO QUESTION 69:
This is not defined and will be evaluated as part of the proposals.

QUESTION 70: Section III a.c.i and a.c.ii indicate that we are to provide one annual penetration test and four vulnerability scans per year, over a 4-year contract period. This seems to be slightly contradicted by Section III b.a.ii which states that Internal Network Vulnerability Assessment and Penetration Testing (up to 1300 Internal IPs) is required. Can you please confirm if internal penetration testing is required or if it is just vulnerability scanning that is required?

CCFC ANSWER TO QUESTION 70:
Correct this is 1 penetration test per year, 1 web application scan per year and 4 quarterly vulnerability scans per year.

QUESTION 71: If an internal infrastructure penetration test is required, are any 911 systems included in the 1300 IP address scope?

CCFC ANSWER TO QUESTION 71:
911 dispatch center is not affiliated with Campbell County Fiscal Court

QUESTION 72: Question and Answer number 15 of Addendum 1 seems to indicate that the goal of the web app penetration testing is to identify and document vulnerabilities, but not exploit them. This seems more like a robust vulnerability scan than a full penetration test. Can you confirm if a full penetration test with exploitation is required for the web apps?

CCFC ANSWER TO QUESTION 72:

The answer was that the primary objective is to identify and document vulnerabilities. This does not state that vulnerabilities should not be exploited. Vendors should describe the solution or method recommended as part of the proposal and it will be evaluated.

QUESTION 73: Question 17 of Addendum 1 indicates that testing should be performed from our own external IPs/systems. Penetration testing can be done from multiple different contexts, can you confirm that you want us to test from the context of an adversary without whitelisted/network connectivity? Allowing our known IPs to connect to the webapps on all ports would allow for a more thorough penetration test of the application itself, whereas testing without whitelisting will test your current network based protections more.

CCFC ANSWER TO QUESTION 73:

The interpretation of this question was from a vendor asking about the External Network Pentest and whether the testing should be from the vendor's network or if the county would provide a whitelisted IP address to avoid interference with controls. The County will not provide a whitelisted county system on the network to perform all testing but will whitelist an approved IP from the vendor to complete necessary internal testing. If a system is necessary for thorough testing, the vendors should describe the solution or method recommended as part of the proposal and it will be evaluated.

QUESTION 74: Does CCFC have Git accounts/code repositories with GitHub, BitBucket or GitLab that should be scanned for potential sensitive data leakage?

CCFC ANSWER TO QUESTION 74:

No.

QUESTION 75: Does CCFC have infrastructure in Amazon Web Services (AWS)? If yes, do you want a posture assessment performed of your AWS environment?

CCFC ANSWER TO QUESTION 75:

No.

QUESTION 76: Is OSHA program a mandate or optional as part of the submission? If this program is not part of the bidder organization will that impact the decision of the proposal?

CCFC ANSWER TO QUESTION 76:

On page 3 of 10 of the RFP document, the county would not anticipate OSHA hazardous communication program to apply to this project, but cannot dictate your company's worker safety programs.