ADDENDUM #1
Cybersecurity Vulnerability Assessment and Penetration Testing
Q&A Posted: 11/08/2024 RFP Open: 11/21/2024
QUESTIONS AND ANSWERS

QUESTIONS SUBMITTED: 64

QUESTION 1: Breakdown of servers vs workstations within the internal scope.

CCFC ANSWER TO QUESTION 1:
40-50 servers and 300+ workstations as well as APs, routers, etc.

QUESTION 2: Total number of web applications being tested.

CCFC ANSWER TO QUESTION 2:
10+ county internal sites. Up to 30 were included in the list for future growth and potentially checking sec.

QUESTION 3: What is the start time for the test for the winning company?

CCFC ANSWER TO QUESTION 3:
Dependent on the approval process we would like to start scans in the 1st quarter of 2025.

QUESTION 4: Does "one pentest per year" mean that we are expected to test all 30 web applications within a single annual engagement, or should we prioritize certain high-risk applications each year?

CCFC ANSWER TO QUESTION 4:
Currently there are only 10+ sites that would need to be scanned. I have included up to 30 to include any new sites or changes in the future.

QUESTION 5: If testing all 30 applications is required for the same annual window can they be spaced out by quarter instead of all at once?

CCFC ANSWER TO QUESTION 5:
With only one pentest per year and quarterly vulnerability scans it is acceptable that the pentest and vulnerability scan can be on one window and the web application pentest could be included with the one of the other vulnerability scans as long as the schedule is done the same each year.

QUESTION 6: Are all 30 websites equally critical, or are there certain applications that are more sensitive or publicly accessible than others? (This can help in prioritizing or allocating more effort to higher-risk sites.)

CCFC ANSWER TO QUESTION 6:
Not all of the sites are critical, there are several included to ensure we are looking at all access.

QUESTION 7: How many dynamic and static pages for each web application?

CCFC ANSWER TO QUESTION 7:
All the sites are dynamic, the data is controlled by the site's admins. The number of pages is a tough call as we do not control the full development of the sites.

QUESTION 8: Do the web applications include APIs, and if so, should the APIs be included in the scope of testing? How many API's per web application?

CCFC ANSWER TO QUESTION 8:
The only external information our sites use is Google analytics

QUESTION 9: Are there specific compliance requirements (e.g., PCI-DSS, HIPAA, CJIS) or guidelines (e.g., OWASP) that need to be followed?

CCFC ANSWER TO QUESTION 9:
We try to maintain ADA compliance; however, we host no data on our website that requires PCI, HIPPA, or CJIS requirements.

QUESTION 10: Is testing to be performed on production environments, or is there a staging environment for each application? (This impacts risk management and access.)

CCFC ANSWER TO QUESTION 10:
We do not have test sites.

QUESTION 11: Will we have access to test accounts with different roles (e.g., admin, user) to evaluate role-based access controls within the applications?

CCFC ANSWER TO QUESTION 11:
Logins can be provided if needed.

QUESTION 12: How should we handle any discovered vulnerabilities in production if testing in live environments? Is there an emergency protocol in place?

CCFC ANSWER TO QUESTION 12:
Contacting our CCFC IT department so that we may determine a plan per our currently available remediation policies.

QUESTION 13: What level of reporting is required for each website: a single consolidated report for all applications or individual reports per application?

CCFC ANSWER TO QUESTION 13:
Individual reports preferred.

QUESTION 14: Do these IPs represent different types of systems or services (e.g., web servers, email servers, public-facing applications, network devices)?

CCFC ANSWER TO QUESTION 14:
Yes.

QUESTION 15: Is the primary objective to identify and document vulnerabilities, or should we also attempt to exploit vulnerabilities to demonstrate potential impacts?

CCFC ANSWER TO QUESTION 15:
Identify and document.

QUESTION 16: Does the county prefer a focus on specific threat vectors, such as known exploits for public-facing servers, misconfigurations, or denial-of-service vulnerabilities?

CCFC ANSWER TO QUESTION 16:
No specific vector.

QUESTION 17: Will the testing be conducted from our external systems, or should specific whitelisted IP addresses be provided to avoid interference with security controls?

CCFC ANSWER TO QUESTION 17:
Testing should be conducted from your own external systems.

QUESTION 18: Are there any network-based defenses in place, such as firewalls, intrusion prevention systems, or web application firewalls, that we should coordinate with to avoid false positives or service interruptions?

CCFC ANSWER TO QUESTION 18:
Yes.

QUESTION 19: Is multi-factor authentication (MFA) or other security control testing part of the assessment, especially for public-facing login portals?

CCFC ANSWER TO QUESTION 19:
Yes, where it is available.

QUESTION 20: Can you provide a breakdown of the types of systems within the 1300 IPs (e.g., workstations, servers, printers, IoT devices)?

CCFC ANSWER TO QUESTION 20:
Systems: rough numbers

i. 300+ windows workstations
ii. About 30 printers
iii. About 15 standalone systems
iv. About 40 servers
v. Over 300 IP phones

vi. 50+ Access points
vii. Many mobile devices
viii. The 1300 IPs is the currently leased IPs with static devices. Not all of them are managed by the CCFC IT Department, but are owned by sister agencies

QUESTION 21: Are certain segments or devices within the internal network a higher priority for testing, or should all 1300 IPs be tested equally?

CCFC ANSWER TO QUESTION 21:
There will be some priority given to core servers and equipment and then equally spread to rest of workstations, etc.

QUESTION 22: Will we be able to provide a network device to connect to your network to allow us access to your network? Or do you have a HyperVisor such as VMWARE of HyperV and allow us to setup a virtual device to access?

CCFC ANSWER TO QUESTION 22:
If there is an OVI to import to our VMware environment, then that may be best option. Otherwise, we can setup a system to allow access.

QUESTION 23: Is the internal network segmented, and will we need credentials or permissions for different segments?

CCFC ANSWER TO QUESTION 23:
There is some segmentation to the network.

QUESTION 24: Will we need elevated privileges or domain-level access for parts of the penetration test, particularly if Active Directory or similar domain controllers are in place?

CCFC ANSWER TO QUESTION 24:
We have Active Directory, please detail the kind of access you need to our domain.

QUESTION 25: Are there specific compliance or security standards to follow for internal testing, such as CIS benchmarks, NIST, or specific industry frameworks?

CCFC ANSWER TO QUESTION 25:
We follow CJIS and HIPPA guidelines.

QUESTION 26: What existing security controls are in place (e.g., firewalls, Intrusion Detection/Prevention Systems, Network Access Control)?

CCFC ANSWER TO QUESTION 26:
Firewall, Carbon Black, rights management via AD, and some switch level controls are in place as well.

QUESTION 27: Are endpoint protection solutions (e.g., antivirus, EDR) active across internal systems, and should we coordinate to avoid triggering alerts or conflicts?

CCFC ANSWER TO QUESTION 27:
Carbon Black for majority of systems, Trendnet for some agencies sharing our network. Yes, some coordination with the IT Director should be made so we can evaluate alert notices.

QUESTION 28: Are there specific applications, databases, or services on the internal network that should receive extra focus due to their sensitivity or criticality?

CCFC ANSWER TO QUESTION 28:
Yes, there are a couple of current applications that may be still in use at the time of these scans that will be given higher priority.

QUESTION 29: Are there specific windows during which testing can occur to minimize potential disruptions, or should testing occur only after business hours?

CCFC ANSWER TO QUESTION 29:
No, further discussion about levels of disruption will be needed to confirm this.

QUESTION 30: Will the quarterly scans cover the entire network, including both internal and external IPs, and web applications, or should different scans focus on specific subsets of assets each quarter?

CCFC ANSWER TO QUESTION 30:
All assets each quarter if possible, by user count. If total count exceeds the contract's included amount, then some quarterly scans may focus on different products in a rotation.

QUESTION 31: Should the scans include all devices (e.g., workstations, servers, network devices) and web applications or only selected critical assets or applications?

CCFC ANSWER TO QUESTION 31:
All assets if possible.

QUESTION 32: Are there specific types of scans required (e.g., network vulnerability scanning, application layer scanning, configuration scanning)?

CCFC ANSWER TO QUESTION 32:
Not required, just a comprehensive scan of the network would be preferred.

QUESTION 33: Should we perform scans that also assess for compliance with security standards like CIS, NIST, or any industry-specific requirements?

CCFC ANSWER TO QUESTION 33:
KY CJIS Standards

QUESTION 34: What level of detail is expected in each quarterly scan report (e.g., summary of critical findings, detailed technical report with remediation steps)?

CCFC ANSWER TO QUESTION 34:
If the different reports have different costs, it is advised to include separate quotes within your RFP.

QUESTION 35: Does Campbell County require real-time alerts or immediate reporting of critical vulnerabilities, or is a quarterly report sufficient?

CCFC ANSWER TO QUESTION 35:
Quarterly reports are sufficient as long as reported within the requested timeframe from the scans.

QUESTION 36: Is there an expectation for follow-up scans to verify that vulnerabilities have been remediated, or is remediation verification only expected during the next quarterly scan?

CCFC ANSWER TO QUESTION 36:
If available, a remediation scan would be preferred to verify changes were successful. In some cases, the next scan cycle would be acceptable depending on the solution.

QUESTION 37: Would the county like guidance on implementing patches, or does it prefer high-level recommendations only?

CCFC ANSWER TO QUESTION 37:
This depends on the type of guidance. In general, we are open to guidance on implementing patches, but it may need to be scaled back if we determine the information is not helpful.

QUESTION 38: Would Campbell County like access to a dashboard or other means of real-time reporting from the scanning tool?

CCFC ANSWER TO QUESTION 38:
Yes

QUESTION 39: What level of detail is expected in the reporting? Should it include a prioritized risk-based analysis of vulnerabilities, or a more technical deep dive?

CCFC ANSWER TO QUESTION 39:
If the different reports have different costs, it is advised to include separate quotes within your RFP.

QUESTION 40: Will the report need to include both an executive summary for management and detailed technical findings for the IT team?

CCFC ANSWER TO QUESTION 40:
Yes

QUESTION 41: Is a final presentation or debrief for key stakeholders required, or is the report submission sufficient?

CCFC ANSWER TO QUESTION 41:
A final presentation or debrief to key stakeholders (ie. Judge Executive and Commissioners) is not required. However, these are required to the IT Director and IT Staff.

QUESTION 42: Are all websites hosted on the same server or across different servers?

CCFC ANSWER TO QUESTION 42:
Different server.

QUESTION 43: Are they hosted in a cloud environment, on-premises, or a hybrid setup?

CCFC ANSWER TO QUESTION 43:
Both, but not hybrid.

QUESTION 44: What web servers (e.g., Apache, Nginx, IIS) and technologies (e.g., PHP, ASP.NET) are being used?

CCFC ANSWER TO QUESTION 44:
Unknown, the hosts do not tell us as these are not internally hosted websites.

QUESTION 45: How are the websites linked? Do they share resources (like databases or APIs)?

CCFC ANSWER TO QUESTION 45:
No

QUESTION 46: Are there subdomains associated with the primary websites that require testing?

CCFC ANSWER TO QUESTION 46:
No

QUESTION 47: Are the sites single-page applications or traditional multi-page applications?

CCFC ANSWER TO QUESTION 47:
Multi-page.

QUESTION 48: Is Single Sign-On (SSO) implemented, or do users have separate logins for each site?

CCFC ANSWER TO QUESTION 48:
Not SSO.

QUESTION 49: What types of user roles exist, and are there access control requirements for each?

CCFC ANSWER TO QUESTION 49:
Admins

QUESTION 50: Are any Content Management Systems (like WordPress, Joomla, or custom CMS) used?

CCFC ANSWER TO QUESTION 50:
Custom

QUESTION 51: If so, are they regularly updated and secured, or are they legacy systems?

CCFC ANSWER TO QUESTION 51:
Regularly updated

QUESTION 52: there any sensitive data stored on these websites (e.g., PII, financial data)?

CCFC ANSWER TO QUESTION 52:
No

QUESTION 53: Are there compliance requirements (e.g., GDPR, HIPAA) affecting the application setup?

CCFC ANSWER TO QUESTION 53:
N/A

QUESTION 54: Are there staging or testing environments available for testing without impacting production?

CCFC ANSWER TO QUESTION 54:
We are not involved in the development.

QUESTION 55: What is the process for deploying code updates or patches?

CCFC ANSWER TO QUESTION 55:
N/A

QUESTION 56: Are there any third-party integrations (like payment processors or social media logins) that require testing?

CCFC ANSWER TO QUESTION 56:
Google Analytics

QUESTION 57: Do the sites use APIs (internal or third-party) that would also require validation?

CCFC ANSWER TO QUESTION 57:
Unknown

QUESTION 58: When are the peak usage times for these websites?

CCFC ANSWER TO QUESTION 58:
Mid-day

QUESTION 59: Are there maintenance windows or low-traffic times ideal for conducting tests?

CCFC ANSWER TO QUESTION 59:
We do not have this schedule.

QUESTION 60: What are the primary user interactions (e.g., form submissions, file uploads, data retrieval) on each site?

CCFC ANSWER TO QUESTION 60:
Data retrieval and form submissions.

QUESTION 61: Are there transactional processes (e.g., e-commerce checkout) that require in-depth testing?

CCFC ANSWER TO QUESTION 61:
No

QUESTION 62: Are error logs and application monitoring available for real-time issue detection during testing?

CCFC ANSWER TO QUESTION 62:
We do not have access to that information.

QUESTION 63: What are the main types of websites in the scope (e.g., informational, transactional, portals, user management systems)? Knowing this can inform the complexity of the testing needed.

CCFC ANSWER TO QUESTION 63:
Our website is informational but we have other internet facing sites that are portals, etc.

QUESTION 64: What types of technologies and frameworks are used in the web applications? (e.g., Java, .NET, PHP, Content Management Systems like WordPress, custom-built applications).

CCFC ANSWER TO QUESTION 64:
Our website is custom built sites, or word press. There will be additional sites that are portals to hardware or websites that are internet facing.