QUESTIONS & ANSWERS FOR 25-83

Question #	Document Section	Question	GUC Response
1		Our firm's reconnaissance phase is cyclical in nature and is interwoven with other phases based on the systems and services discovered during enumeration. With this in mind, can GUC expand on what is meant by 'Time allowed for reconnaissance and OSINT: 10 hours'?	Reconnissance searching time is limited to 10 hours for budgetary purposes.
2		For wireless access devices, should testing be limited to configuration and firmware review, or must it also include wireless authentication strength testing (for example, WPA2/WPA3 handshake capture and analysis)?	testing is limited to configuration and firmware review and access control
3		If wireless testing requires an on-site presence, what is the estimated distance between access points and how many sites will require on-site testing?	There are 2 wireless networks that can be accessed all from one physical location
4		If wireless testing can be conducted remotely, via a shipped device, will it be possible to access both corporate and guest networks from a single location?	There are 2 wireless networks that can be accessed all from one physical location
5		How many web applications or portals hosted on in-scope servers are included in this engagement? If present, will they require in-depth web application testing, or only a limited, high-level assessment of exposed functionality?	there are 5-10 web application or portal hosted on in-scope servers. Only a limited high level asssessment of exposed functionality. Further refinement will be discussed within the SOW.
6		Our firm offers ongoing support and continuous testing. If that option is not selected, will a remediation window be provided and will retesting of discovered issues be required after that window	Retesting is not required as part of this engagement, and no formal remediation window is included. Any remediation activities will be handled internally at GUC's discretion. That said, vendors are welcome to propose optional retesting or follow-up services as a no-cost value-add, clearly identified as outside the scope of this engagement and not required for consideration.
7		Are there any restrictions on testing hours (business hours versus after-hours) that will affect scheduling or effort?	Testing should be done from 7 a.m. to 5:30 p.m. Monday-Friday Eastern Standard Time. These are the times that any work that may have negative impact should be conducted since we will have staff working to address any issues.
8		Are there any blackout dates, high-availability windows, or other operational constraints we must avoid during testing?	Testing should be done from 7 a.m. to 5:30 p.m. Monday-Friday Eastern Standard Time, excluding Federal and State holidays.
9		Will test accounts/credentials be provided for either external or internal portions of the assessment, or is all testing to be performed from an unauthenticated perspective?	The selected vendor will be provided with a generic user account with basic privileges along with access to a device on the corporate network to attempt lateral movement and escalation from.
10	Exhibit A – Budget, Timeline, Access and Scope	Regarding the statement "Any work that has any potential of negative impact should be performed from 6 a.m. to 6 p.m." Is this requirement designed to ensure that staff are available to respond in the event of a negative impact?	Your understanding is correct. Further, the times listed in Exhibit A should have been "7 a.m. to 5:30 p.m. Monday-Friday Eastern Standard Time". These are the times that any work that may have negative impact should be conducted since we will have staff working to address any issues.
11	Internal Scope	Approximately how many Wi-Fi access points are deployed?	This will be discussed further with the selected vendor when developing the Statement of Work (SOW) with the selected vendor.
12	Internal Scope	Will authorization be granted to attempt to access sensitive data as proof of compromise?	The selected vendor will be provided with a generic user account with basic privileges along with access to a device on the corporate network to attempt lateral movement and escalation from.
13	Internal Scope	Will GUC provide a list critical systems/servers that should NOT be tested (production databases, etc.)	This will be discussed further with the selected vendor when developing the Statement of Work (SOW) with the selected vendor.
14	Internal Scope	Within Active Directory are there multiple domains or forests?	No
15	Internal Scope	Beyond the provided generic user account, should we plan to test from multiple privilege levels? (power user, admin)	The selected vendor will be provided with a generic user account with basic privileges along with access to a device on the corporate network to attempt lateral movement and escalation from.
16	Internal Scope	Are there service accounts that should be tested?	This is possible, however further clarification will be discussed further with the selected vendor when developing the Statement of Work (SOW) with the selected vendor.
17	Internal Scope	Is Active Directory enumeration and attack testing authorized?	Yes, as long as no users are services are impacted.
18	Internal Scope	Are password attacks (spraying, cracking) against AD permitted?	No
19	Internal Scope	Is lateral movement between systems authorized?	Yes
20	Internal Scope	Is testing of backup systems and management interfaces permitted?	This will be discussed further with the selected vendor when developing the Statement of Work (SOW) with the selected vendor.
21	Internal Scope	Are denial of service tests permitted in any capacity?	No
22	External Scope	Are any IP ranges shared with other organizations (co-located, shared hosting)?	No
23	External Scope	What external-facing services are in scope? (Web servers, email, VPN, FTP, etc.)	Yes
24	External Scope	Are there any DDoS protection services in place?	This will be discussed further with the selected vendor when developing the Statement of Work (SOW) with the selected vendor.

25	External Scope	Are there any CDN services protecting assets? (Cloudflare, Akamai, etc.)	This will be discussed further with the selected vendor when developing the Statement of Work (SOW) with the selected vendor.
26	External Scope	Are there any WAF (Web Application Firewall) solutions in place?	This will be discussed further with the selected vendor when developing the Statement of Work (SOW) with the selected vendor.
27	External Scope	Should we test from a known/whitelisted IP or perform true black-box testing?	This will be discussed further with the selected vendor when developing the Statement of Work (SOW) with the selected vendor.
28	External Scope	Is exploitation of discovered vulnerabilities authorized?	Yes as long as there are no disruptions
29	External Scope	Should we attempt to pivot to internal networks if possible?	Yes
30	External Scope	Are brute force attacks against authentication systems permitted?	No
31	External Scope	While not in scope as a specific task, is social engineering via external vectors (phishing from external test) permitted?	No
32	External Scope	Would GUC prefer testing be stopped if a critical vulnerability is found, or continue?	We have a security team that any critical findings will need to be reported to during testing. This will be discussed further with the selected vendor when developing the Statement of Work (SOW) with the selected vendor.
33	Exhibit A – Application Testing	For pricing, approximately how many applications are in scope?	Application testing is not in scope and will be removed from the SOW.
34	Exhibit A – Application Testing	What type of application testing to be performed, i.e., Static or Dynamic?	Application testing is not in scope and will be removed from the SOW.
35		Regarding Wireless Testing (as part of Internal): # of SSIDs?	Details of this nature will be discussed during the development of the Statement of Work (SOW) with the selected vendor and provided as appropriate.
36		Regarding SCADA, does the "Number of internal IPs (Endpoints) accounts: 510" include SCADA IPs? If not, how many SCADA IPs are there?	The number provided was for the IT corporate network only. Endpoints in the SCADA environments are not in scope for this project beyond the 1 device per SCADA network that an IP address will be provided for.
37		Will GUC accept contract revisions? If so, how would you like them to be submitted?	We prefer our Terms and Conditions
38		Due to existing NDAs, may we provide anonymized references at this stage? The customers would be described, and project descriptions provided, but clients' names and contact information withheld until down select.	Yes. We will accept anonymized references for this stage if they indicate the size of the company, the industry they are in, and the scope of security work provided to them. After review of all proposals, we will narrow the list to the top 2-4 vendors and will require full contact info for references at that time.
39		Is application testing in scope?	Application testing is not in scope and will be removed from the SOW.
40		Can non-US based engineers perform the work, they are based in EMEA but would be connecting from US infrastructure.	All remote workers and scans should originate from sites in the USA.
41		Can references and contacts be provided on down selection, most customers don't like their information being put out into open bids so we would request to provide those on down select.	We will accept anonymized references for this stage if they indicate the size of the company, the industry they are in, and the scope of security work provided to them. After review of all proposals, we will narrow the list to the top 2-4 vendors and will require full contact info for references at that time.
42		Is the $45,000 budget firm or is there flexibility if we believe we would go over that cost?	The maximum budget is firm.
43		Is the $45,000 budget intended solely for the first-year engagement?	The maximum budget is firm, one year engagement only.
44		Should the proposal be priced as a fixed fee, with the rate table included only for reference/administrative purposes?	While engagements like this are typically a fixed fee project, vendor can choose to submit a time and materials proposal with a maximum "not to exceed" amount. In that case, a schedule of rates would be required.
45		What remote access method (VPN, jump host, bastion, or VM/appliance) will be provided for SCADA network testing?	Details of this nature will be discussed during the development of the Statement of Work (SOW) with the selected vendor and provided as appropriate.
46		Will GUC provide network segmentation diagrams for both corporate and SCADA environments to support rules-of-engagement planning?	Details of this nature will be discussed during the development of the Statement of Work (SOW) with the selected vendor and provided as appropriate.
47		Are there any additional SCADA restrictions (protocol limits, read-only requirements, logging expectations, etc.) beyond those listed in the RFP?	Details of this nature will be discussed during the development of the Statement of Work (SOW) with the selected vendor and provided as appropriate.
48		For the application penetration test, will the scope include authenticated testing, unauthenticated testing, or both?	Application testing is not in scope and will be removed from the SOW.
49		For wireless testing, can all testing be performed remotely via a VM/appliance, with no onsite presence expected?	Yes

50		Are there any blackout periods or maintenance windows beyond the stated 6 a.m.–6 p.m. EST, Monday–Friday restriction for potentially impactful tests?	Further, the times listed in Exhibit A should have been "7 a.m. to 5:30 p.m. Monday-Friday Eastern Standard Time". These are the times that any work that may have negative impact should be conducted since we will have staff working to address any issues.
51		Are there any AWIA (America's Water Infrastructure Act)–related requirements or reporting expectations tied to this engagement?	No.
52		(3) SSIDs in scope or are there more in 2025/26?	There are 2 wireless networks that can be accessed all from one physical location
53		Are all internal systems (endpoints, servers, SCADA & non-SCADA) and wireless still accessible from one location?	Details of this nature will be discussed during the development of the Statement of Work (SOW) with the selected vendor and provided as appropriate.
54		Does GUC want pricing listed as an hourly rate or fixed-fee? Per section "Proposal Requirements" #6 or section Page 19, exhibit A	While engagements like this are typically a fixed fee project, vendor can choose to submit a time and materials proposal with a maximum "not to exceed" amount. In that case, a schedule of rates would be required.
55		Does the 11 pt. font requirement for the response apply to tables?	Responses are limited to a total of 40 pages; however, an attachment of a sample report can be beyond the 40-page limit. The font size shall not be smaller than 11-point.
56		For the web application, with a large unknown size, testing will be conducted via a timebox scenario, averaging 80 hours, is this acceptable or would you prefer more hours allocated? We normally base price on pages, if that number is not available, timeboxing is recommended.	Application testing is not in scope and will be removed from the SOW.
57		Will GUC please provide a weighted evaluation criteria?	Please refer to page 6 of 21 in the RFP, Evaluation Criteria.