Questions & Answers II FOR 25-84

	Question	GUC Response
1	Will GUC provide written authorization (Letter of Authorization / Rules of Engagement) explicitly permitting penetration testing across corporate and SCADA-adjacent networks?	Testing will be conducted under an approved scope with formal authorization and documented exclusions.
2	Are there defined approved testing windows (days/times) for a) Corporate network testing and b) SCADA network access attempts (non-production HMI only)?	Testing windows will be coordinated and approved in advance. SCADA-adjacent testing is restricted to non-production systems only.
3	What is the escalation and stop-test procedure if unexpected instability or operational risk is observed during testing?	Testing must immediately cease if instability or risk is observed. GUC must be notified immediately.
4	Does “attempt to exploit and gain access” mean a) validation of segmentation weaknesses only, or b) authentication/authorization bypass on SCADA-adjacent assets (excluding PLCs/devices)?	Testing is limited to validation of segmentation and access controls. Exploitation of PLCs or production control components is not permitted.
5	Should internal testing be performed as a) fully non-credentialed or b) hybrid (limited standard-user credentials on selected endpoints)?	Limited credentials may be provided on approved systems.
6	Are AD, LDAP, or identity services considered in scope for security testing (non-disruptive techniques only)?	Active Directory may be included using non-disruptive techniques only.
7	Is active testing (authentication testing, rogue AP detection, segmentation validation) permitted on a) Corporate Wi-Fi and b) Guest Wi-Fi?	There are 2 wireless networks that can be accessed for testing: corporate and guest.
8	Can GUC confirm a) specific data classifications of interest and b) any data explicitly excluded from inspection?	Sensitive production data and customer data are excluded from inspection.

9	Is OSINT limited strictly to a) Public internet sources, breached credential repositories, and exposed metadata and b) confirmation that no direct contact, impersonation, or supplier interaction is permitted?	OSINT is limited to publicly available information only.
10	Does GUC require pre-approval of exploit categories or tools prior to execution?	All testing tools and techniques must be approved prior to execution.
11	Are authenticated or intrusive vulnerability scans explicitly a) Allowed or b) restricted to specific asset classes?	Authenticated scans are permitted only on approved asset classes.
12	Does GUC require use of a specific severity model (e.g., CVSS v3.1), or may industry-standard risk ratings be applied?	Industry standard severity scoring may be used.
13	Are findings expected to be mapped to any specific standards (e.g., NIST CSF, NERC CIP, ISA/IEC 62443), or only "industry best practices" at a high level?	Findings may be mapped to industry standards such as NIST or equivalent best practices.
14	Will GUC provide logical network diagrams or written descriptions defining a) corporate ↔ SCADA trust boundaries b) access paths allowed to the four SCADA networks?	Details of this nature will be discussed during the development of the Statement of Work (SOW) with the selected vendor and provided as appropriate.
15	For each SCADA network a) will exactly one non-production HMI / workstation per network be provided? Also, what operating systems and access levels will be available on these HMIs?	There will be 1 device per SCADA network that an IP address will be provided for. Additional details will be discussed during the development of the Statement of Work (SOW) with the selected vendor and provided as appropriate.
16	Will GUC provide a final allowlist confirming: a) The 22 external IPs and b) the internal ranges covering 510 endpoints and 195 servers?	yes

17	Are any internally routable systems explicitly excluded beyond PLCs, sensors, valves, and production control components?	Testing is limited to validation of segmentation and access controls. Exploitation of PLCs or production control components is not permitted.
18	Given the engagement is 100% remote, will GUC provide a) remote access to wireless controllers/logs or b) a pre-positioned on-site testing mechanism?	A pre-positioned on-site testing mechanism that is provided by the selected vendor.
19	Are there specific evidence handling, redaction, or retention requirements for screenshots, file metadata, or proofs-of-access?	While this is partially covered within the RFP, further information will be discussed during the creation of the SOW with the selected vendor.
20	Should the proposal price a) only year-1 execution ($45K) or also include b) optional, not-to-exceed pricing for Years 2–3?	The maximum budget $45K, one year engagement only.
21	Is validation / limited retesting of critical findings expected within the approximately 104-day timeline (Feb 11 to Jun 30), or treated as a future-year activity?	All testing and final reporting must be completed by June 30, 2026, remediation is the responsibility of GUC, and any validation or retesting is only permitted if included by the vendor at no additional cost.