GUC RFP 21-65

Q&A Response to Vendors

We appreciate the questions that many vendors have provided. In response we are providing the following Addendum to the RFP, followed by answers to the specific questions asked. Similar questions asked by multiple vendors but with wording variations have been consolidated into one response.

RFP Addendum

The first goal of this pen test is to determine if an outsider can penetrate our network firewalls. For this external portion of the project, we will provide you with our external IP range that has a total of 40 IP addresses. You will then conduct reconnaissance and OSINT for up to 10 hours and then provide a preliminary report of findings for GUC to review.

Next, we will assume you have been able to gain access to our network and want to know if you can move laterally and escalate within our network. We will provide you with a generic AD user account with general user privileges for you to use to attempt to exploit and gain access to workstations, servers or systems in a non-obtrusive and non-destructive manner. Our goal is for you to find and identify weaknesses in our AD environment that would allow gaining root access, access to PII or other high value documents, etc. If you wish to provide a VM or appliance that has needed tools for doing such reconnaissance, we will install it and provide you with secure remote access to it for this phase of the project.

Finally, from that same foothold in our network, you are to attempt to access our SCADA production networks with the goal of finding any weaknesses in the internal firewalls that separate the general network from our SCADA networks. Further, we will provide you with the IP address of 1 device (workstation, switch, or server) in each of the 4 SCADA networks for you to scan and try to gain control of. Since you will be in a SCADA production environment, you are NOT to do a general scan of the network or attempt any action on any other device except the 1 device of the IP address provided. Access to the PLC networks is not in scope for this project.

It is our further expectation that a detailed statement of work will be created with the selected vendor. That document will clearly lay out all details for the engagement.

Answers to specific questions asked, grouped by type:

BUDGET

1. Is there a preliminary budget for this project and can it be shared? Yes. The budget for this project is $45,000.00

REMOTE ACCESS

2. Would GUC prefer the work associated with this project to be completed remotely, on-site, or a combination of both? GUC prefers an all-remote engagement to reduce costs.

3. Should travel costs for any onsite testing be incorporated in the firm fixed price for hours to complete the pen test? Yes. If a vendor prefers that a portion of the work take place on site, that is acceptable. In that case, all travel costs of the on-site portion should be included in the total cost of the project.

4. Do you have any restrictions for 100% on-site, remote or offshore? See answer to # 2 and # 3 above; also note that all remote workers and scans should originate from sites in the USA. If the red team is not based in North America, please indicate to us the country of origin.

5. We plan to execute this project with our experts from US and offshore, are there any restrictions on staffing resources from our offshore team? See answer # 4 above.

6. Can the project plan of operations include a majority of remote solution to complete the pen test? Assuming this question is asking if most of the work can be done remotely, the answer is Yes.

7. Can testing be conducted remotely via a VM or on-premise system? (Note that remote access would need to be confirmed.) Yes.

8. Can all in scope systems be reached from a central network point or would testing require access to be seated in multiple networks? YES. If multiple, please indicate the number of separate environments. NA

9. In case of on-site execution of penetration test, is there a central location where all the networks are reachable from? Yes

SCADA SYSTEMS

10. Can you clarify the intent of testing as it relates to SCADA systems? Is testing limited to leveraging systems/users as a means to gain access to the SCADA network(s) (no scanning/testing of SCADA systems)? The intent is to determine if remote access into SCADA network is possible and if so, can the 1 device that an IP addresses is provided for be compromised. No scanning/test of SCADA systems is allowed, except for the single IP address that will be provided for each of the 4 SCADA networks.

11. Does the scope go deeper than the SCADA systems on the OT side, i.e., PLCs, valves, sensors? No. Scope will be to attempt to access 1 designated SCADA device behind each of the SCADA firewalls, nothing more. PLC's, valves and sensors are not in scope.

12. Is the testing against the production environment or a staging environment? Testing is against production environments for both IT and SCADA networks. For SCADA/OT, only 1 IP address will be provided per network that is in scope. Any exploit that might be disruptive to our networks is out of scope.

13. How many SCADA devices will be in the scope for the four different SCADA networks (Electric, Water, Wastewater, and Natural Gas)? Only 1 per SCADA network

14. Scope of Services: What is the ratio of IT SCADA workstations/servers versus OT embedded devices like drive controllers, logic/safety controllers, relays, load balance/sync, mass flow, GCs, etc.? Only 1 specified device per network is in scope.

15. Will you provide a list of SCADA systems and identify what is explicitly out of scope? Yes, a single IP address within each SCADA network will be provided as in scope. Anything else is out of scope.

16. If access cannot be obtained to the four SCADA networks, will GUC want those networks to be pen tested with white card access provided? No

17. Please confirm the scope of the SCADA assessment is to only attempt to gain access to the networks. Yes, that is the primary scope, and to further see if the one specified device in each network can be compromised.

18. Do you have an estimate of the number of IT related hosts in each of the SCADA networks? No. The precise number is 1 per SCADA network as noted in prior answers.

SCOPE

19. Will GUC provide the external IP address ranges to conduct external penetration test? OR Does the Reconnaissance and OSINT for 10 hours also include the assessment team discovering external IP address. The external IP address range will be provided.

20. Does GUC have preference for the type of penetration testing (for e.g., white-box, gray-box, or black-box) for internal scope? We prefer grey box. The selected vendor will be allowed to put a device on the network and a user with basic AD rights to use for investigation.

21. Will the assessment team be provided with high-level network architecture description or diagram of the corporate and SCADA networks? No.

22. Scope of Services: Could you please confirm current standards/practices implemented for each of the 4 sectors (electric, water, wastewater, natural gas)? This is not needed, as it is not in scope to evaluate how the systems rate with such standards, and detailed scanning of the SCADA networks is not in scope.

23. Scope of Services: Are SCADA endpoints included as internal IPs/AD endpoints in the 500 count? No, they are not.

24. Internal Scope: Is success for SCADA defined only as seeing IP addresses on SCADA network, or access to SCADA devices on the network? Success is defined by being able to access and compromise the one device in each network that you will be given an IP address for.

25. Internal Scope: Is "basic Active Directory user rights" provided (white box) or must be extracted (black box)? We will provide you with a generic AD user account with general user privileges for you to use to attempt to exploit and gain access to workstations, servers or systems in a non-obtrusive and non-destructive manner.

26. Scope of Services: Confirm that services focused on penetration testing and not security assessment against standards/practices. Correct. The focus is to be purely on technical aspects. This is not a security assessment against standards, policies and procedures.

27. We assume this testing needs to be designed for no impact on production GUC systems, and that arranging rules of engagement accordingly is expected? That is correct. We expect to negotiate a formal SOW with the selected vendor and rules of engagement will be detailed at that time, including the requirement of no impact on production systems.

28. Please specify which operating systems the 263 non-SCADA servers support? (number of servers provided in the Scope of Services section of the RFP.). Windows and Linux

29. Are there any restrictions around testing windows? We typically perform automated and manual testing utilizing 24x7 windows. Yes, any work that has any potential of negative impact should be performed from 6 a.m. to 6 p.m. Monday-Friday, Eastern Standard Time. Any further details will be specified in the SOW negotiated with the selected vendor. Please indicate if other testing windows are required. (Note that non-standard testing windows may impact the overall duration of the penetration test and could have an impact on overall cost.) Also note that all scans should originate from sites in the USA, as most other countries are blocked.

30. Can you please specify how many enterprise applications are in scope for this engagement? We will identify from 3 to 5 applications that will be in scope, and the specifics of what will be provided about those applications will be negotiated in the SOW with the selected vendor.

31. Are there Web Applications on the External Scope to be tested? Some of the internal servers in scope are application servers. We will provide more specifics for 3 to 5 applications in the statement of work negotiated with the selected vendor. If yes – will the Commission provide user accounts for the applications? No. You will have only the generic AD account to use as a foothold.

32. Does GUC plan to conduct Wireless Penetration Testing for the network? We can perform this on-site or remote, where we send a device to GUC, and they need to switch it on for us to conduct wireless assessment. The wireless controller is in scope, but not the wireless network. The focus of this assessment is AD accounts, not wireless networks.

GENERAL & Miscellaneous

33. We understand that the proposal is limited to 40 pages. Does this include attachments, such as sample reports? No. Attachments with samples can be additional pages beyond the 40 pages.

34. Does the project have a mandatory start date? (We understand the project needs to be completed and paid for by June 30th, 2022). No.

35. Is this funded by a federal grant or under a prime federal grant? No.

36. Do they have a comprehensive Security Program for Corporate (for eg. IEC 62443, ISO 27001, NIST) and SCADA environment (NERC CIP) that GUC would like vendor to assess? Assessment of our security program is not in scope.

37. Is Phishing or social engineering in scope? No.

38. Is GUC responsible for the management and administration of these SCADA equipment (including interconnections throughout the industrial network) or is this management outsourced? GUC is responsible.

39. Should the deliverables be made for each corporate network (water, gas, electricity), by headquarters, location? No. A single report for GUC, including SCADA networks is sufficient. Specific findings per network or device should be delineated within the single report.

40. What does “vendor's response time” in the RFP refer to? One factor in the vendor selection will be the amount of time the vendor states it will take to complete the work. For example, if a vendor stated they could not start the work until May 1 and claims to be able to complete all the work and provide an invoice by the last of June, we would probably conclude that is not a "reasonable response time" to do this job. This item might have been better worded as "vendor's schedule and capacity for accomplishing work in the required time frame."

41. We typically price our engagements based on a fixed fee approach – not hourly rates. Is this acceptable to GUC? Yes.

42. Is this tender going through the State of North Carolina Department of Information Technology contract 918-A for security assessment services such that final terms and conditions (not scope) will align to the already agreed to terms in 918-A? No

43. Due to the confidential nature of our security business as well as existing NDAs, we would like to provide anonymized references at this RFP stage, i.e., we would provide project implementation details, but the client would be described, not named, and specific contact information would be withheld for now. Reference calls would be coordinated upon request at down-select. Would this approach be acceptable to GUC for this RFP response? 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.

44. Letter of Compliance to E-Verify – are questions 1-4 for the prime contractor, and 5-7 for any subcontractor(s)? Please refer to NCGS, E Verify, Article 2 of Chapter 64 of the North Carolina General Statutes.

45. Is the vendor required to be duly licensed in the state of North Carolina prior to award or is upon award acceptable? No. To our knowledge there is no license required at this time for this type of service.