Adversarial Assessment RFP – Q&A Responses

	Are you able to share the proposed budget for this engagement?
2.	Is there an incumbent? Are they allowed to propose?
3.	For the scope of the social engineering test, is RISLA requesting only a report on who clicks on the phishing attempt, or is the intended objective for the selected vendor to attempt to obtain user credentials and exploit?

1. There is no proposed budget.
2. There is no incumbent
3. Attempt to get creds and/or exploit.

1. **Assessment Logistics:** Could you please confirm if the assessment will be conducted remotely, on-site, or as a combination of both? If on-site, we would appreciate details regarding the expected logistics and the duration of our team's presence.
2. **Remediation Support:** We would also like to clarify your expectations for remediation support. Are there specific types of remediation you expect us to assist with? Additionally, how would you prefer this service to be structured to best meet your needs?
3. **Report Acceptance Process:** The RFP mentions that the final report must be "accepted" by the CISO before January 1, 2025. Could you provide more details on what the acceptance process entails? Specifically, are there any criteria or specific requirements the CISO will use during the acceptance process?

1. It can be conducted remotely but the team must be in the united states.
2. Really we are just looking for someone we can ask questions to and get a response if we hit a snag. We figure out 99% of the stuff ourselves but just like to have some help if we need to ask how to fix something.
3. I would recommend including a sample report in your rfp submission. I'm pretty loose about the criteria but I don't want like a 1 pager with no actionable recommendations.

1. Can RISLA confirm that it is requesting an adversarial assessment in the form of penetration testing?
2. RISLA lists both internal and external Ips. Can you confirm that both internal and external penetration testing are in scope?

Yes, it's a pentest, but looking for something more substantial than some automated pentest. Not looking for someone to send me a laptop with vpentest and tenable on it and hand me back a rebranded report.

Yes both IP ranges are in scope of the test.

1) When you ask for adversarial testing, are you expecting:

a) Little to no communication with the testing team to emulate real-world attackers and elevated stealth.

b) Lots of communication while testing is ongoing, but using an adversary's Techniques, tactics, and procedures with little to no stealth.

2) Do you have an advisory in mind that you want to emulate?

3) When you say remediation support, do you want:

a) A project manager to aid in remediation

b) A Subject Matter Expert to talk to about remediation efforts

c) Staff augmentation to conduct remediation efforts

d) Re-testing of remediation efforts

4) What is the expectation of automated vs manual testing?

5) What Metrics are you interested in as it relates to the phishing campaign:

a) Phishing for access

b) Phishing to see who click the link

c) Phishing for Credentials

1. I'm looking for something more significant than someone sending me a laptop and running some automated scanner on it and calling it day. You can work as closely as you want with me but I just want someone to put in some actual effort to break into our systems.

2. Not specifically, but a lot of the threats we face are patient and methodical, we'd like something that emulates that but in obviously a shorter timeframe. I'm happy to peel layers of the security onion away to get places quickly, but when you read about most successful hacks these days it's because someone accidentally put a domain password on a batch script that ended up on an open file share. I want that level of detail to the best of someone's ability given the limited timeframe.
3. Really just want the final report to have steps to fix, and if we hit a snag trying to fix it that we can email or call someone to kick some ideas around as to what the issue might be.
4. Can use a mix as you see fit, but definitely not looking for a fully automated test using vpentest and tenable with rebranded reports.
5. Phishing for creds

Reaching out to make sure this is the correct email alias to submit the Q&A and the Proposal to?

Also is there a specific POC name and phone# and email I can add within our internal database to draft the proposal?

Yes, this is the correct alias, per the RFP, that you got this email from. No, we would not like to be added to any databases.