RISLA Adversarial Assessment RFP – Q&A **08/12/2025**

- Are there guidelines around estimated timing for the duration of this project?

A: Anytime during Q4, preferably we would have a rough draft of the report first week of December, with the final draft no later than January 1st, 2026

- Has RISLA undergone a penetration assessment before?
  - If yes, can these results be shared?

A: Yes, we have had penetration tests done, but the results cannot be shared publicly

- Will internal testing require on-site presence, or can it be conducted remotely via VPN or jump box?

A: The testing can be done remotely as long as the team conducting the testing is located within the United States.

- Is physical security testing desired for this engagement?

A: No

- What IDS/IPS protection systems are in place, if any?

A: Several, we will let you know what protections are in place if you win the award.

- Can you provide a network diagram or asset inventory?

A: If you win the award, yes

- All IT infrastructure is stated to be in scope. What systems, if any, are out of scope?

A: No systems out of scope

- A stated assessment goal is "test training and security policies". What training is conducted and what policies are in place?

A: We do several trainings a year on general cybersecurity practices, phishing, smishing, etc. Lots of policies in place, your job to figure out what they are and work around them, a hacker wouldn't know.

- Are there time of day restrictions in place?

A: Prefer during the work day, and not on a Monday, but we're flexible

- Can a high level overview of technologies in use be provided?

A: If you win the award

- Are there known vulnerabilities in the environment?

A: Win the award and find out.

- What, if any, budgetary guidelines can you provide?

A: There are none, award will go to the lowest qualified bidder.