



## **S<sup>2</sup>MARTS Project: small Unmanned Arial Systems (sUAS) Advanced Technique Development Request For Solutions (RFS) Question & Answer | Date: August 13, 2021**

**1. Question: Must you use Ettus COTS for this or if any COTS are acceptable?**

Answer: Ettus hardware is not mandatory but generated technique must be capable of being implemented on an SDR platform.

**2. Question: Would you accept cyber solutions which would not/could not be implemented on Software Defined Radios for c-UAS applications: hence a solution which could potentially address near-peer adversary drones which are leveraging RF shielding and AI autonomous systems with sophisticated inertial guidance systems that are not GPS dependent?**

Answer: Currently we are not looking at this as an option.

**3. Question: Could you confirm that both program managers and reviewers for this RFS would support funding efforts to expose weaknesses in the firmware of Software Define Radios (SDRs) and in the hardware, (e.g.: FPGA's)? Rationale: to protect US assets, we must clearly evaluate how US drone's SDRs would most likely be compromised and how we can most efficiently mitigates/prevent such exploitations from occurring at the lowest compute/power cost to US' SDRs/US drones?**

Answer: We are not currently looking at evaluating US assets.

**4. Question: Would you support/fund technology which is center focused on FPGA and ARM core Firmware exploitations so as to mitigate group 1-2 drone risks from near-peer adversaries who are developing AI capabilities to conduct low-cost offensive operations against US and/or Ally ships? – so as to conduct EW/cyber operations and/or secret surveillance against near peer adversaries and understand how to defend US assets against similar exploitations.**

Answer: We are specifically looking at EW countermeasure techniques for an identified technology to be implemented on an SDR. We are not looking to evaluate UAS CONOPS against US assets.

**5. Question: Would you consider funding a multitiered approach which uses cyber as one layer for risk mitigation (offensive against adversaries and defensive to protect US drones & ships) against near peer adversaries' drones (with or without AI capabilities) but also, with another layer which would provide a low cost (less then \$2k) drone interceptor demonstration capable of more than twice the speed of existing group 1 threats (120 MPH) and could be integrated with pre-existing ship-board sensors and/or operate with its own sensors' suite for ship-board defense against group 1-2 drones?**

Answer: Currently we are interesting in developing EW countermeasures for a specific UAS communications technology to be implemented into an SDR. We are not currently interested in any other defense capability.

**6. Question: Could you provide us with some insights as to whether or not you are expecting multiple awards to be given to qualified multi-company teams? And... if so, can that award/budget reach the \$3 million mark for enhancing TRL-5 to 7 pre-existing capabilities within a single teaming award?**

Answer: At this time, we are not expecting multiple awards.

**7. Question: Could you provide us with some insights as to whether or not you are expecting multiple awards to be given to qualified multi-company teams? And... if so, can that award/budget reach the \$3 million mark for enhancing TRL-5 to 7 pre-existing capabilities within a single teaming award?**



Answer: Same question as #6

**8. Question: The RFS states that the selected party will be required to procure a novel sUAS communication technology to evaluate. Will the government provide guidance on which technology to procure in terms of a specific system, or potentially a list of systems of interest to the government? Or, will we choose a system to procure?**

Answer: The government will provide guidance on the exact technology to procure.