Department of the Navy SBIR/STTR Transition Program

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.

NAVWAR

Topic # N193-A01

Certificate of Robustness and Safety for AI (CORSI)

Quantum Ventura Inc

WHO

SYSCOM: NAVWAR

Sponsoring Program: Naval Information Warfare Systems Command

Transition Target: Program Executive Office for Command, Control, Communications, Computers and Intelligence (PEO C4I)

TPOC:
(619) 553-2861

Other transition opportunities: Unmanned Underwater Systems, Unmanned Aircraft Systems, Safety-critical systems of Autonomy and Automation, Counter Artificial Intelligence, Cyber, Integration of Automatic Identification System (AIS) Data through AI/ML Applications, Integration of Automatic Dependent Surveillance

https://www.dvidshub.net/image/6623716/ford-strike-group-air-defense-exercise

WHAT

Operational Need and Improvement: To make well-informed, accurate and timely decisions, artificial intelligence/machine learning is often used; e.g., automatic target recognition, ship or airplane tracking, cybersecurity, etc. However, AI/ML systems are opaque, and the predictions are unexplainable. They can often be fooled by novel, unexpected or corrupted data. This could have disastrous effects on C4ISR, unmanned systems, cybersecurity, etc. CORSI focuses on evaluating the robustness, safety, validation and verification of AI/ML systems. CORSI evaluates both white box (where the source code and the ML models are available) and black box (where ML application structure and details are unknown) AI/ML models. We have also developed adversarial attacks to AI/ML systems as well as created defenses against those attacks.

Specifications Required: The solution requires primarily requires input and output data pairs used in AI/ML. E.g., AIS track from three previous timesteps for training, and one for prediction; images and labels, text documents and categories, etc. (This data can also be multisensor, multimodal, etc.) If AI/ML models, either as white or black boxes, are available, that is also helpful. Domain knowledge and expected performance criteria are useful but not necessary.

Technology Developed: CORSI produces verification and validation of AI/ML systems. This means testing and certifying AI/ML systems to certain changes in inputs. Furthermore, CORSI also defends against adversarial attack performed on AI/ML systems.

Warfighter Value: CORSI enhances AI/ML systems delivering results that can be trusted and validated. This will lead to quicker and more accurate decisions in variety of fields such as C4ISR, unnamed systems, cybersecurity, etc. As the Navy continues to use more machine learning within and across domains, CORSI's value will also increase.

WHEN

Contract Number: N68335-20-F-0589 **Ending on:** November 8, 2021

Milestone	Risk Level	Measure of Success	Ending TRL	Date
Define detailed technical specs	Low	Design document	3	TBD
Enhanced CORSI-DNN (Deep Neural Network) toolkit	Med	Data Flow Successful	5	TBD
Prototype Demo	Med	Data Flow Successful	6	TBD
If Option exercised Prototype Demo	Med	Technology Integration with C4ISR Program	7	TBD

HOW

Projected Business Model: The business model for the advancement and transition of CORSI is a combination of license and services for both defense and industry application. The platform can be hosted in the Cloud or onsite locally. Implementation includes not only the base technology but add-on applications for specific customer needs. As part of the services provided with the platform, Quantum Ventura will work with customers to ensure secure data integrations to existing legacy systems. We are also exploring "AI in a box", a complete hardware/software implementation of CORSI.

Company Objectives: Along with our strategic partner Lockheed Martin, we will target DOD customers and identify additional partners and customers to both scale the existing offering across defense and industry organizations as well as to identify new opportunities for engagement.

Potential Commercial Applications: CORSI has wide applicability in many different commercial applications where AI/ML technologies are used, e.g., image/video recognition, cybersecurity, natural language processing (NLP), etc. The technology is a system with dual-purpose defense and industry applicability. The verification and validation and defenses against adversarial attack capabilities of this platform will benefit organizations with high value assets and mission critical need to consistently and reliably operate. Beyond Navy use, defense applications include UAVs, UUVs, etc. Private sector applicability includes areas such as aviation, transportation and manufacturing.

Contact: Srini Vasan, President & CEO
srini@quantumventura.com (424) 227-1417