Department of the Navy SBIR/STTR Transition Program

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

NAVSEA #2020-0364

Topic # N132-140

Cognitive Autonomous Artificial System Intelligence (CAASI)

La Jolla Logic, Inc.

WHO

SYSCOM: NAVSEA

Sponsoring Program: NAVSEA (SEA-O3) - Cyber Engineering and Digital Transformation Directorate

Transition Target: U.S. Fleet Cyber Command (FCC)/U.S. TENTH Fleet (C10F)

TPOC:
(202)781-3623

Other transition opportunities: Within the Defense sector, CAASI would benefit the cybersecurity detection capabilities within NAVAIR and NAVFAC platforms and industrial control systems. As CAASI evolves it is broadly applicable to any computer network system for the detection of unknown anomalous activity including potential security threats and indications of deteriorating mechanical system performance.

Notes: Cognitive Autonomous Artificial System Intelligence (CAASI) augments existing malware detection tools through its ability to detect previously unknown threats. By continuously monitoring and analyzing network connections, CAASI learns the normal patterns and characteristics of a network. Using its learned knowledge base, CAASI is able to detect and isolate suspect activity for further analysis.

WHAT

Operational Need and Improvement: The global cyber threat is continuously evolving. The emergence of state-sponsored malicious actors in the cyber domain magnifies the threat to Department of Defense networks, weapons systems, and platforms which are increasingly connected to take advantage of synergies in netcentric operations. Cyber defense must evolve with the the threat and be capable to detecting and countering hostile actions before they can cause damage. New capabilities are needed to protect the confidentiality, integrity, and availability of defense systems in the contested cyber environment.

Specifications Required: Use of inference engine technology to adapt to new threats, increase cyber security situational awareness, and reduce analyst response times.

Technology Developed: La Jolla Logic has developed a high-velocity data ingestion engine, unsupervised machine learning techniques, and abnormal network behavior detection algorithms to identify potentially malicious activity, whether from direct hack attempts, viruses, bots, or even insider threats. CAASI also models system interactions and interconnectivity which has many benefits in addition to attack detection. Understanding the orchestration of communication between systems on a network can provide survivability on which other systems would be affected if one particular system were to be compromised or to fail.

Warfighter Value: CAASI adds a new capability to existing cyber security tools through its anomalous behavior detection. Unlike existing cyber security detection tools, CAASI does not rely on libraries of known malicious code like traditional antivirus libraries. Instead, CAASI learns and understands normal system behaviors enabling it to seek out previously unknown threats. Simply stated, CAASI has the ability to detect zero-day attacks on a network, drastically limiting the ability of malware to propagate and compromise complex Industrial Control System (ICS) networks.

WHEN

Contract Number: N68335-19-C-0204 **Ending on:** September 8, 2020

Milestone	Risk Level	Measure of Success	Ending TRL	Date
Baseline Integrated CAASI System	N/A	Established laboratory environment and developed prototype into integrated system with baseline visualization functionality to enable testing in relevant environment.	TRL 5	September 2019
Data Ingestion and Analysis	N/A	CAASI successfully ingested 5 TB of recorded network traffic and established learned database.	TRL 5	April 2020
Attack Detection Test & Analysis	N/A	Validated algorithms achieve very high attack detection with very low false positive rate in realistic laboratory environment.	TRL 6	July 2020
If Phase II Extension exercised, Navy Test Event	Low	Integration with NAVSEA cyber security tool suite and realistic test event within a Navy environment.	TRL 7	March 2021

HOW

Projected Business Model: Leverage DoD SBIR funding to address technology risk in development for direct sell to the government which is acting as lead integrator for primary target program. Provide ongoing support to integration into cyber security tool set for application aboard all afloat platforms. Long term, business model includes IP protection and tailored development for application in the commercial market through use of company-funded internal research and development (IR&D).

Company Objectives: Seek additional DoD programs that will benefit from CAASI's cyber security intrusion detection capability to extend adoption across multiple defense networks. Identify potential programs developing condition-based maintenance applications that may benefit from CAASI's identification of anomalous network activity on industrial control networks. Develop a Commercial off the Shelf (COTS) product for application in cyber defense of Critical Infrastructure networks such as Energy Sector/Utilities and in the Financial Sector.

Potential Commercial Applications: CAASI technology is directly applicable to cyber security of any network as a compliment to existing threat detection systems. It can also be adapted with little effort to specific use within Critical Infrastructure systems such as public water distribution and energy sector utilities to analyze detected anomalies and score indicators that a system was acting abnormally and may be about to fail. CAASI's ability to detect abnormal behaviors on industrial control systems can be applied to inform condition-based maintenance models to improve accuracy and reliability of predicted failures.

Contact: Karina Arushanyan, Vice President
karina.arushanyan@lajollalogic.com (619) 517-5783