Department of the Navy SBIR/STTR Transition Program

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.
NAVAIR 2023-0153

Topic # N211-009
Cyber Protection for Physical Avionics Data Inputs to Navy Platforms
Intellisense Systems, Inc.

WHO

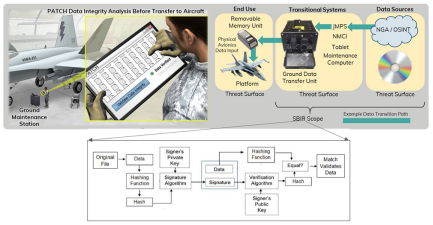
SYSCOM: NAVAIR

Sponsoring Program: NAVAIR- PMA209

Transition Target: T-45, CH-53K

TPOC: (301) 342-2966

Other Transition Opportunities: The Lockheed Martin F-35 Lightning



Notes: Intellisense Systems, Inc.'s Persistent Avionics Threat Chain Hardening Technology (PATCH) is a computer processing platform proposed to augment data security within mission planning environments (MPE). PATCH can be integrated into an existing MPE systems to:
- Minimize threat surface of computers in MPE;
- Ensure data integrity along entire data flow path in MPE;
- Protect against malicious tampering and errant corruption.

WHAT

Operational Need and Improvement: PATCH addresses the Navy's need to ensure the integrity of all physical avionics data input to all Navy aircraft and to identify and overcome threat surfaces and holistically support data integrity prior to its being transferred to the aircraft.

Specifications Required: - Minimize threat surface along the data chain.
- Protect aeronautical data from NGA access to aircraft uploading against both purposely or errantly corruption or manipulation.
- Mitigate all risks, including errant and malicious tampering, that could impact the integrity of the mission-critical aeronautical data at all stages.

Technology Developed: The PATCH system is an innovative end-to-end cyber protection framework on aeronautical data through integration of computer/network security procedures and data protection software to ensure the integrity of the aeronautical data maintained through all the threat surfaces along the data chain, without causing unnecessary burden on the aircrew or mission planning staff.

Warfighter Value: PATCH's unique combination of traditional and non-traditional data integrity analysis provides a comprehensive cyber threat coverage for both errant corruption and targeted data manipulation.

WHEN

Contract Number: N68335-23-C-0210 **Ending on:** Feb 24, 2025

Milestone	Risk Level	Measure of Success	Ending TRL	Date
Gen 1 prototype demonstration in lab	N/A	Integrity protection on aeronautical data	4	2nd QTR FY24
Gen 2 - Enhance the performance	N/A	Data integrity protection with minimal latency	5	4th QTR FY24
Gen 2 prototype lab test	Low	Integrity protection against malicious tampering and errant corruption in controlled environment	5	2nd QTR FY25
Gen 2 prototype field test	Medium	Integrity protection against malicious tampering and errant corruption in field environment	6	2nd QTR FY26

HOW

Projected Business Model: We plan to develop PATCH to TRL-7/8 and then transition to low-rate initial production, selling directly to the Navy/government for platforms such as T-45 and CH-53 K. We anticipate that the first fully productized system will be available in either late 2027 or early 2028.

Company Objectives: Intellisense intends to leverage the PATCH technology into a new family of products for use by all branches of the DoD and other government agencies for different operating environments.

Potential Commercial Applications: PATCH can be applied to protect the integrity and validity of the data that are received by aircraft and ground vehicles from disparate sources. Mission and ground station platform primes can also benefit from this technology.

Contact: Steven Mitts, Director, Business Development
smitts@intellisenseinc.com (424) 319-7824