NAWCAD- FAA GPS Antenna Request for Information (RFI) on GNSS Multi-Element Antenna for Civil Applications

The following dates apply to the Request for Information (RFI)

- 60 calendar days after the RFI release: RFI Q&A closes to new questions
- 90 calendar days after the RFI release: Final responses due

Background:

The Federal Aviation Administration (FAA) issued a Safety Alert for Operations (SAFO) (# 24002) on January 1, 2024, that provided information and guidance to operators and manufacturers regarding operations in a Global Positioning System (GPS) / Global Navigation Satellite System (GNSS) disrupted environment. This SAFO highlights ongoing jamming and spoofing incidents that can increase safety of flight risks due to possible loss of situational awareness and increased pilot and Air Traffic Control workload.

The FAA has requested support from the Naval Air Warfare Center Aircraft Division (NAWCAD) to investigate the feasibility and expected performance of applying anti-jam (AJ)/anti-spoofing (AS) GPS/GNSS technology for use in civilian aircraft applications with an initial focus on Transport and Business Jet aircraft. NAWCAD is releasing this RFI on AJ/AS GPS/GNSS technologies for eventual use in civilian aircraft applications. This RFI is a study identifying and discussing the characteristics and performance of the vendors' AJ and AS antenna technologies that are currently available or being developed. The information learned from this RFI may be used to identify potential systems for evaluation testing at NAWCAD. Results from the RFI data and future evaluation testing will be used to develop updated GPS/GNSS AJ/AS antenna Minimum Operational Performance Standards (MOPS) and cockpit displays/annunciation MOPS for the FAA.

NAWCAD is performing the study, hosting the industry day(s), and establishing Cooperative Research and Development Agreements (CRADAs) or technology agreements for test hardware, lab test, chamber test, and future flight test for the FAA.

Purpose

Baseline Jam and Spoof Resistant Adaptive Antenna: The FAA urgently needs to facilitate, certify, and approve adaptive antenna systems for installation on civil aircraft with focus on commercial and business jet aircraft (domestic and international) to enable operations in civil corridors adjacent to areas with active jamming and spoofing. The AJ/AS GPS navigation systems must support GPS L1 Coarse Acquisition (L1C/A) and L1 Satellite-Based Augmentation System (SBAS) for GPS, SBAS, and GBAS operations.

NAWCAD is evaluating the civil aviation industry's current and near-term technology capabilities and performance taking into consideration size, weight, power, and cost (SWAP-C) as well as non-recurring and recurring aircraft integration and installation costs and operating expenses. Results of this research are intended to steer the development of GPS/GNSS Jam and Spoof resistant antenna MOPS in accordance with dual-use technology Commerce Export Administration Regulations (EAR) Export Control Classification Numbers (ECCN) 7A005 and ECCN 7A105. The focus is primarily on higher power spoofing detection and mitigation.

Advanced Jam and Spoof Resistant Adaptive Antenna System: The advanced aircraft adaptive antenna and antenna signal processing electronics suitable for commercial aircraft applications

will increase aircraft resilience and robustness to interference and spoofing of aircraft user equipment and corresponding aircraft applications. Focus is primarily on lower power spoofing detection and mitigation. Offerors should consider practical SWAP-C and long-term threat evolution.

These studies will steer the development of the FAA/EASA Technical Standard Order (TSO)/European Technical Standard Order (ETSO) GPS/GNSS receiver Final MOPS (RTCA DO-401() /EUROCAE ED-259() and corresponding FAA TSO/EASA ETSO, and aircraft installation guidance.

The AJ/AS GPS navigation systems must support GPS L1 Coarse Acquisition (L1C/A) and L1 Satellite-Based Augmentation System (SBAS) for GPS, SBAS and GBAS operations, L5, Galileo E1, and E5a. The antenna needs to have growth capability for accommodation of the more robust L1C signal and its data message structure when that signal is adopted for civil aviation use.

NAWCAD will evaluate non-CRPA/AE GPS protection systems demonstrating similar or better jam resistance characteristics performance and spoofing detection alerting.

Through this RFI, NAWCAD seeks to collect opinions on the civil applications that could benefit from existing and new capabilities, technology, and techniques and industry interest in developing or integrating this technology. This RFI will also seek to understand the challenges associated with implementing these capabilities and techniques for civil applications, particularly in the airborne market. The FAA seeks to understand the impact of potential solutions integrated on existing and future aircraft. Information for this RFI should include size, weight, power and unit cost (SWAP-C) non-binding estimates. Additionally, the FAA seeks to understand industries support for standards development and promote its usage in the airborne sector.

Relevant threat scenarios include targeted spoofing by non-state actors, non-selective jamming and spoofing in large areas, and unintentional interference.

The technologies identified as suitable for civil aircraft applications, will increase aircraft navigation resilience and robustness by significantly reducing or precluding the passing of erroneous signals and data into the aircraft GPS-based navigation solution and provide enhanced detection and alerting for the aircrew.

International Traffic in Arms Regulations (ITAR)/United States Munitions List (USML) restrictions are not applicable to this RFI and all considerations for a solution will be considered when technologies are being evaluated. The FAA will investigate removal of ITAR restrictions as applicable.

The research goal after completion of lab test, chamber test, and future flight test, is to provide recommendations for system performance capabilities and requirements for the aviation industry's development of standards:

- FAA Technical Standard Order (TSO)
- FAA Advisory Circular (AC) for aircraft installation guidance
- System MOPS

Market RFI Participants' Actions:

Provide the following information:

- Applicable data/capabilities in the attached MS Excel spreadsheet named: Civilian GPS Advanced Antenna Matrix Template_R1.xls
- Technology data sheets
- User guides
- Interface documents
- Technology maturation roadmap

All information provided will be protected in compliance with DoD policy and proprietary markings. Data shared with the FAA will be protected in accordance with FAA Order 1600.75.

Evaluation Criteria:

The following criteria will be used to evaluate the antenna systems:

Baseline Jam and Spoof Resistant Adaptive Antenna

Threshold capabilities:

- Technology Readiness Level (TRL) 7
- Simultaneous L1 C/A, L1 SBAS
- Nulling anti-jam
- Analog Radio Frequency output, control/status interface, jamming detection and alerting information via commercial interface to commercial cockpit avionics
- Basic "Interference Protection/Suppression" antenna
- Technologies identified will be evaluated to determine if ITAR restrictions apply. The FAA will review all submissions and is responsible to clear ITAR restrictions if required.
- Antenna technology must be scalable to meet the objective capabilities in the longer term
- Nulling
    - # 4+
    - Null depth 20+ dB
    - 20 dB+ increased receiver protection over a fixed reception pattern reception antenna
    - General direction of jamming
    - Minimize sympathetic nulls
    - Indicate that jammer power (dBm) at the antenna has reached 90% of the system or antenna electronics (AE) unit jammer nulling performance specification
    - Indicate the presence of additive signal power above the thermal noise floor

Objective

- Antenna is optimized to consider both performance and operating cost. Goal: Antenna is as conformal as practical to minimize drag coefficient.

Advanced Jam and Spoof Resistant Adaptive Antenna System

Threshold

- TRL4+
- Capability to simultaneous tracking L1 C/A, L5, L1 SBAS, Galileo E1, E5a
- Nulling anti-jam, spoofing detection and alerting function
- Provide analog Radio Frequency output, control/status interface data, jamming and spoofing situational awareness data
- Basic "Interference Protection/Suppression" antenna
- Exportable for commercial aircraft operations and sales in accordance with licensing provisions under Commerce EAR ECCL (pending ITAR/USML regulatory change/removal)
- Threshold antenna is scalable to meet objective requirements
- Nulling
    - # 4+
    - Null depth 20+ dB
    - 20 dB+ increased receiver protection over a FRPA
    - General direction of jamming
    - Minimize sympathetic nulls
    - Indication of the presence of additive signal power above the thermal noise floor

- Spoofing detection and alerting reporting
    - Spoofing indications and spoofing detection and alerting information via commercial interface to commercial cockpit avionics
    - Substantial positioning, navigation and time errors
    - Identify data as invalid
    - Detect spoofers

- Spoofing hazardous signals that avionics recognize as valid L1 C/A, L1C, WAAS/SBAS, GBAS, GPS L5 and long-term Galileo E1, E5a satellite signals

    - Manipulated signals used by the L1 C/A, GPS L1C, GPS L2C, WAAS/SBAS, GBAS, GPS L5 and long-term Galileo E1, E5a receiver
    - Detecting hazardously misleading data within the antenna or aircraft avionics
    - Wide-area interference could include jamming, repeater, or SBAS correction manipulation. Non-targeted interference is not expected to match live sky signal strength closely and should not track the aircraft's movement. It may or may not match live sky ephemeris/almanac data and signal timing. Received power will vary widely, but a reasonable benchmark might be -85 dBm.
    - Unintentional interference could include misconfigured GPS repeaters, personal privacy devices, and stationary transmitters using GPS-adjacent frequencies. Indicators and effects of interference, as well as mitigation, will likely be similar to wide-area interference.
    - The targeted spoofing interferer may be a passenger with a software-defined radio (SDR). The spoofing would likely be close in power to live sky, although the spoofing signals for all satellites would originate from the same source inside the aircraft; combined power would exceed any single satellite's power by 10-20 dB, although

the total spoofing power would still be similar in magnitude to thermal noise (-110 dBm at 2 MHz and 290K).
    - Aviation capabilities to conduct collateral operations in the presence of interference from
        - U.S. government testing
        - Inadvertent emissions
        - Adjacent to/in jamming in areas of conflict and counter UAV, missile systems emitting active jamming and/or spoofing emissions.
        - Enroute and approach/landing operations at airports near interference, jamming and spoofing sources

Objective capabilities:

- Antenna is optimized to consider both performance and operating cost. Goal: Antenna is as conformal as practical to minimize drag coefficient.

- Nulling anti-jam
    - # 5+
    - Null depth 30+ dB
    - Bearing/direction of each jammer
    - Geolocation of each jammer
- Beam steering L1 C/A, L1C, WAAS/SBAS, GBAS, L5 and long-term Galileo E1, E5a, E6
    - Minimum # of beams- L1 C/A 6+, L5 6+
    - Provide a digital multi-beam output
- Support anti-spoof capabilities
    - Inhibit interference
    - Inhibit the use of spoofing signals inside the navigation solution
    - GNSS L1 C/A, L1C, L2C, WAAS/SBAS, GBAS, L5 and long-term Galileo E1, E5a RF signal with spoofing signals removed
    - GNSS L1 C/A, L1C, L2C, WAAS/SBAS, GBAS, L5 and long-term Galileo E1, E5a RF signal with spoofing signals not removed
    - Signal Manipulation Protection
    - Spoofing information
        - # of spoofers
        - Type of each spoofer
        - Bearing/direction of each spoofer
    - Identify as invalid data and remove from final Navigation solution
    - Detect spoofers and remove from final navigation solution
    - Geolocation of each spoofer
    - Authenticate almanac and ephemeris data messages
    - Spoofing Avionics hardware and software for identifying hazardous signals that avionics (and pilot) may recognize as valid GPS and WAAS/SBAS satellite signals
        - Inhibit and preclude pilot and aircraft automation use of United States Government-recognized spoofing threats that manipulate or simulate false GPS/SBAS signals and data messages
- Simultaneous L1 C/A, L1C, WAAS/SBAS, GBAS, L5 and long-term Galileo E1, E5a protection

- Continuous L1 C/A, L1C, WAAS/SBAS, L5 and long-term Galileo E1, E5a services

Additional Considerations

Technologies to consider including in the antenna/AE:

- Resilient integrated SDR GPS receiver
- Ephemeris integrity checks
- Almanac integrity checks
- Direction of arrival
- WAAS message authentication
- Time of arrival techniques
- Multipath resilience
- Inertial Measurement Unit aiding into antenna
- Barometric altitude
- Receiver autonomous integrity monitoring (RAIM), Advanced Receiver Autonomous Integrity Monitoring (ARAIM)
- Independent, complementary position, navigation, and timing sources, including legacy and/or modernized navigational aids (NAVAIDs, e.g. Distance Measuring Equipment (DME), IMU)
- Probability of detection

Technical approaches for non-antenna solutions will be reviewed for potential further investigation and understand. If methods present are viable to meet the intent of the FAA requirements, they may be selected for follow on testing to assist in the development of the end-products.

Questions to Market RFI Participants

1. What capabilities does the offeror recommend adding to the DO-401 draft MOPS to complement the offers' antenna and antenna electronics?
2. Does your company have advanced GPS integrity or antenna development efforts for civil applications?
3. If applicable, does your company develop GPS/GNSS related certified product(s) according to FAA TSO and/or European Union Aviation Safety Agency's European Technical Standard Order?
4. Are you currently involved in or planning research and development activities for GPS/GNSS secure radio frequency interference/spoofing (RFIS) systems to include antenna technologies, signal processing techniques, or other technologies and do you see a market opportunity for such development?

   If NO:

   a. If consideration to conducting research and development of GPS/GNSS RFIS systems were evaluated but not targeted, were there any technologies that may aid in a solution set for this capability?

b. Please describe the difficulties/barriers faced, if any, or the factors preventing you from developing a multi-element antenna for the civil market (other than ITAR/USML).
c. Please describe how much time is expected to be required to complete development and when an actual flight test could be achieved.
d. What level of investment do you estimate is needed to develop a multi-element antenna with marketable capabilities for the civil market?
e. Identify assessment/assumptions of current and projected global RFI environments for the purposes of responding to the next two questions.
f. Based upon the RFI environment assessment/assumptions, what are the multi-element antenna and antenna electronics capabilities, characteristics and performance foreseen as marketable for aircraft retaining legacy GPS, GPS/SBAS, or GPS/GBAS receivers.
g. Same question as above except for aircraft equipped with TSO/ETSO avionics consistent with expectations for the future RTCA DO-401() /EUROCAE ED-259().

If YES:

a. Please specify the maturity level of the technology developed.
b. Please describe the timeframe you foresee completing the development and when you believe in achieving actual implementation.
c. Please describe the difficulties/barriers, if any, being faced in the development of the multi-element antennas for the civil aviation market
d. What is the level of investment being used to develop a CRPA antenna for the civil aviation market?

5. Does your company have any advanced GPS/GNSS RFIS on civil aircraft?
If YES:

a. What are your company's product design layers (CRPA antenna, antenna electronics, GPS receiver software)?
b. What protections would be in each layer?

6. Would your company be interested in participating in the development of minimum operational standards for technologies for GPS/GNSS protection for civil aviation applications?

POC

Point of Contact	Email
William Reinking	william.a.reinking.civ@us.navy.mil