Naval Information Warfare Center (NIWC) Atlantic

Rapid Capabilities Cell (RCC)

Commercial Solutions Opening (CSO)

N65236-26-S-0001

Prototype Title: Multi-Enclave, Wireless 5G, Tactical Fly-Away Kit (FAK)

Area of Interest (AOI) Number: 26-A009

Command Focus Area: 3.1 Battlespace Connectivity

Problem Statement

The Navy requires transformative, self-contained communications systems that provide resilient, high-bandwidth, low-latency connectivity for multiple security enclaves simultaneously. These systems ideally would operate within a secure wireless environment that is survivable against electronic warfare (EW) threats, compliant with shipboard safety standards, and capable of rapid deployment with minimal configuration.

Desired Solution:

Portfolio Acquisition Executive (PAE) Mission Systems seeks vendor solutions from the commercial sector for a Multi-Enclave, 5th Generation (5G) or better Wireless, Tactical Fly-Away Kit that integrates mature (TRL 7+), commercially derived technologies. Compelling solutions must utilize a Modular Open Systems Approach (MOSA) to avoid vendor lock-in and must address the following:

1. Establish a Survivable, Secure Multi-Enclave Wireless Environment
    - The prototype must create a secure, localized wireless communications "bubble." It must securely transport data from multiple security classification levels (Unclassified through TS/SCI) simultaneously. Solutions must align with National Security Agency's Commercial Solutions for Classified (CSfC) capability packages and incorporate Low Probability of Intercept/Low Probability of Detection (LPI/LPD) technologies to minimize the Radio Frequency (RF) signature against adversarial Signals Intelligence (SIGINT).
2. Provide Unified, Zero-Trust Cross-Domain Access
    - The solution must enable users to access multiple security enclaves from a single endpoint device (e.g., laptop, tablet) while maintaining strict data isolation. The architecture must align with DoW Zero Trust principles, ensuring no data spillage between classification levels on the endpoint or in transit.
3. Demonstrate Resilient, Agnostic, and Anti-Jam Connectivity

- The FAK must dynamically leverage diverse data transport pathways, including Military Satellite Communication (MILSATCOM) and commercial Proliferated Low Earth Orbit (pLEO) constellations.
- The system must demonstrate Primary, Alternate, Contingency, and Emergency (PACE) automated failover and feature anti-jamming resilience to bypass degraded or contested infrastructure.

4. Ensure Tactical Mobility, SWaP Optimization, and Shipboard Compliance
    - The system must be modular, utilizing standard transit cases manageable via a two-person lift.
    - It must be capable of full setup and network establishment in under 30 minutes.
    - The system must be compatible with standard shipboard power, comply with Hazards of Electromagnetic Radiation to Ordnance (HERO) standards, and seamlessly integrate into shipboard Emissions Control (EMCON) protocols (i.e., immediate RF shutoff capability).

Additional attributes are detailed below that would add more value to a proposed solution.

Primary Attributes (Highly desired)

1. A simplified, dashboard-driven configuration interface designed for standard operators, eliminating the need for an advanced IT or Cyber specialist to establish the network within a 30-minute window.
2. An integrated Uninterruptible Power Supply (UPS) and Active Power Conditioning module that maintains the network during shipboard power transitions (e.g., switching from shore power to ship generators) without dropping the multi-enclave connections.
3. Strict Form-Factor Limits: Maximum transit case dimensions (e.g., must allow unassisted transport through standard Navy shipboard hatches and passageways.)
4. Designed for shipboard environment:
    a. MIL-DTL Shock & Vibe Hardening, Internal components must use locking connectors, conformal coating, and shock-mounted chassis rails to prevent connections from shaking loose during combat operations
    b. Salt Fog & Corrosion: Exposure to marine air, salt spray, and high humidity will rapidly corrode standard commercial networking ports and cooling fans. IP67 Rating & Marine Hardening: Require sealed, fanless designs (or filtered intakes) with conformal-coated circuit boards and corrosion-resistant transit case hardware.

DOD Contract Security Classification Specification (DD254):

Due to the accelerated nature of the CSO timeline, the Government is requiring offerors to demonstrate the required facility clearance level at time of submission of the Solutions Brief. The contractor shall possess a Top Secret (TS) Facility Clearance with eligibility for Sensitive Compartmented Information (SCI) access to perform under this Area of Interest. Solution Briefs must contain the Cage Code for the prime contractor that would be identified on any resulting agreement. NIWC Atlantic will use the cage code provided in the Solution Brief to determine if contractor facility clearance requirements are met. Contractors that do not hold the appropriate level may not be considered for a Phase 2 Pitch.

The requirements under this AOI will be Top Secret with Sensitive Compartmented Information (TS/SCI).

Cybersecurity Maturity Model Certification (CMMC):

CMMC Level 2 (Self) will be required for agreements made against this AOI.

Potential Travel Locations:

The Government anticipates that travel may be required under any resultant award within the Continental United States (CONUS). Potential locations include but are not limited to the following: San Diego, CA; Panama City, FL; Charleston, SC.

Solution Briefs:

Interested companies shall submit a solution brief within the vulcan platform (vulcan-sof.com) no later than 2359 Eastern Daylight Time (EDT) 17 August 2026. Solution briefs shall not contain CUI and shall meet the requirements specified in CSO N65236-26-S-0001 paragraph 7.2. In addition, the solution brief shall detail how the nontraditional business participation as defined in CSO N65236-26-S-0001 paragraph 6.2 will be met. If proposing a teaming partner to meet nontraditional requirements, that teaming partner must be identified by name in the solution brief and their cage code provided for verification. If an offeror is proposing to meet the requirements by providing a cost share, this must be explicitly stated in the solution brief.

Late submissions will not be considered.

The Government reserves the right to limit the number of entities invited to pitch based on the evaluation consideration in accordance with CSO N65236-26-S-0001 paragraph 7.2.2. Solution Briefs that are selected for the Phase 2 Pitch will be notified in writing as soon as practicable.

Pitch:

The Government anticipates hosting a virtual Pitch via Microsoft Teams for this AOI. Tentative dates for the pitches will be 24 through 28 August 2026. It is anticipated that the pitches will be one hour.

Vendors will be notified in writing as soon as practicable with additional details if they are invited to pitch.

Point of Contact:

Questions related to this AOI can be submitted to Bridgette Clayton at bridgette.l.clayton.civ@us.navy.mil. Solutions Briefs emailed directly to Bridgette Clayton will not be accepted for this AOI. Solutions briefs must be submitted via the Vulcan platform to be evaluated.

Potential for Follow-On Production Contract:

Companies are advised that any prototype other transaction agreement awarded in response to this area of interest may result in the direct award of a follow-on production agreement without the use of further competitive procedures.

Restrictions on Public Announcements:

No press releases or public announcements regarding this AOI can be made ahead of notification from the Government regarding down select to Phase II pitches. Non-compliance with this policy may result in potential exclusion from further consideration in the AOI evaluation.

Enclosures:

See Enclosure 2 of the RCC CSO N65236-26-S-0001 for the TS/SCI DD254 applicable to this AOI.