

Fiscal Year 2026 (FY26) Call #1.1:

Link-182 Space-to-Space Comms System Development and Demonstration

The Space Systems Command Spectrum Warfare Delta (SSC/SZW) is seeking state-of-the-art technology advancements for the United States Space Force's (USSF) space-based communications architecture utilizing a **two-phase BAA approach**. The Government believes that the best approach for a low size, weight, and power (SWaP) solution in support of Golden Dome (GD) space-based interceptor (SBI) risk reduction and notional comm requirements will fall within the L/S-Band Spectrum and use the Link-182 waveform. The period of performance (POP) for Call 1.1 is **12 months**. Due to this schedule constraint, the Government expects Contractors will need to utilize high heritage components and systems that require minimal development modifications.

In Call 1.1 white paper submissions (following instructions set forth in the overall BAA Posting section 5.12), prospective Offerors shall submit a technical approach that describes a proposed solution for the following deliverables:

1. Final design of a Link-182 waveform space qualified flight radio capable of operating from low earth orbit (LEO) to geosynchronous Earth orbit (GEO) and that can be scaled to delivery quantities of 10,000 within a nominal period of two to five (2-5) years (to be included in a productionization plan).
 - Radios must: 1. weigh less than 1.36 kilograms (kg), 2. consume less than 30 watts (W) of power, 3. have a seven (7) year design life, and 4. be able to connect to the National Security Agency (NSA) Type-1 cryptography (crypto)
2. A LEO space-to-space communication demonstration between a Link-182 payload and Link-182 radio integrated onto an independent flight test asset of the vendor's choosing that simulates an element of SBI vehicle flight (nominal distance from transceiver-based spacecraft and nominal vehicle relative velocity) and must occur within the 12-month POP.
 - An end cryptographic unit (ECU) is not required to be included in the demo
 - Using an engineering unit for the Link-182 radio component with a design life of 30-90 days will be sufficient for the demo
3. Development and deployment of an Application Programming Interface (API) to enable space-to-space pointing of the Link-182 payload.

During contract execution, the Offeror will also be required to participate in interactive discussions of their delivered results, so the Government may understand the Contractor's analytical and technical basis for performance and cost conclusions. These discussions may include but are not limited to: mission payload designs/technical details, waveforms, link budgets, modeling and simulation, threat assumptions, cyber security architecture, networking techniques, concept of operations (CONOPS) in contested environment, and part/material selections.

The white paper rough order of magnitude (ROM) shall include the following cost details and fulfill the requirements stated in the overall BAA Posting (see section 5.12) as applicable to the Offeror's proposed solution:

- Radio modification and testing to meet mission parameters
- Space demonstration of a Link-182 payload and Link-182 radio
- API development
- Interactive discussions
- Final report inclusive of the Offeror's: design, productionization plan, test summaries, and demonstration results

For Call 1.1, a Controlled Unclassified Information (CUI) document titled Link-182 Waveform Specification is available to interested vendors that plan to submit white papers. There is an Operations Security (OPSEC) requirement to ensure all recipients of the CUI file meet access criteria in accordance with (IAW) 32 Code of Federal Regulations (CFR) Part 2002, the National Industrial Security Program Operating Manual (NISPOM), and Department of Defense Instruction (DODI) 5200.48 titled "Controlled Unclassified Information" as CUI is not releasable to the public. To request and obtain the specification, please follow the process below. Please allow up to one week to process your request.

1. Contractor Requirements for CUI Access

A. Self-Attestation of Compliance

- Contractors must implement the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 (110 controls) for protecting CUI in non-federal systems.
- Vendors must submit a self-assessment score in the Supplier Performance Risk System (SPRS), per Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7019.
- If not fully compliant, Offerors must have a System Security Plan (SSP) and a Plan of Action & Milestones (POA&M).

B. Flow-down Requirements

- If an Offeror plans to share this CUI with a subcontractor, they must ensure that subcontractor also complies with DFARS 252.204-7012 and NIST 800-171.

2. Contractor Verification

Prospective Offerors must send an email to the security and technical Government POCs (listed below) with the subject line "S2S Comm BAA Call 1.1 Request for CUI – (company name)".

Security POC:

Mr. Steven Mafla

SSC/SZW

Email: steven.mafla.ctr@spaceforce.mil

Technical POC:

Maj Justin Mayfield

SSC/SZWM

Email: justin.mayfield.7@spaceforce.mil

Submit the following information for security verification:

- Submitter's Name and Parent Company (if applicable)
- Mailing Address/Facility: Street address, City, State, NINE-Digit zip code
- Commercial and Government Entity (CAGE) Code
- Unique Entity Identification
- Any Active Government Contract Number
 - If the prospective offeror doesn't have an active Government Contract Number, the following must be submitted from the company's Facility Security Officer (FSO): A FSO signed letter on company letterhead confirming 1. eligibility to receive CUI and 2. CUI data handling and storage is in place.
- Point of Contact (POC)
- POC Telephone number and email address

3. Vetting and Approval

The Government representative will review the submitted information to confirm that the company meets the required access criteria, IAW regulations like the NISPOM and relevant CUI rules. Requests that do not include the required Contractor verification information will be denied.

4. Secure Document Transmission

Once a Contractor is vetted and approved, the CUI document will be sent via DOD Secure Access File Exchange (SAFE). The Contractor POC will receive two emails: 1. with a link to the online secure pickup location and claim code and 2. with a passphrase for access to the encrypted file.

5. Required Protection of the Document

After receiving the CUI document, the contractor is responsible for protecting it according to CUI policy. CUI must be handled and stored on systems that align with minimum security requirements, such as those specified in the NIST SP 800-171.