AIR COMBAT COMMAND A2 & AIR FORCE INTELLIGENCE COMMUNITY

(ACC/A2 & AF IC) COMMERCIAL SOLUTIONS OPENING (CSO)

SOLICITATION NUMBER: FA7037-26-S-C001

Date: 20 May 2026

The Government is not obligated to make any award under this CSO and any potential award consideration is subject to availability of funds.

Table of Contents

I. Overview

II. Areas of Interest

III. Cybersecurity Requirements and SAM Registration

IV. Price Determination: Fair and Reasonable

V. Definition of Terms

I. OVERVIEW

ACC/A2, in sync with the mission of the AF IC is offering a Commercial Solutions Opening (CSO) authorized by 10 USC 3458 and R-DFARS 212.70. Under a CSO, the Government may competitively award contracts to proposals received in response to a general solicitation, similar to a Broad Agency Announcement (BAA), to acquire commercial items, technologies, and services, based upon a review of proposals by scientific, technological, or other subject-matter experts within the USAF. Under this CSO, all items, technologies, and services shall be treated as commercial items.

“The USAF intends to obtain "innovative" solutions or potential new capabilities that fulfill requirements, close capability gaps, or provide potential technology advancements. Solutions may include existing technologies or procedures, not currently in use by the USAF, that would enhance or streamline USAF mission capabilities. "Innovative" is defined as any technology, process or method that is new as of the date of submission of a proposal. It also includes any new application of an existing technology, process, or method.

To maintain a strategic advantage in an era of peer competition, the Government, in sync with the mission of the AF IC is executing a decisive pivot to a data-centric, software-defined, and Artificial Intelligence (AI)-enabled enterprise. As warfare evolves into a complex, all-domain battlespace, our ability to achieve Decision Dominance hinges on accelerating this digital transformation. We are moving beyond legacy, hardware-defined systems to embrace agility, scalability, and speed. This CSO is a call to industry for a partnership to rapidly field innovative solutions that empower our warfighters and analysts with a decisive information edge.

All proposed solutions should be built upon and address the digital bedrock of our cloud computing ecosystem and be intrinsically designed around non-negotiable security principles. This includes a Zero Trust Architecture, which must be woven into the fabric of the solution with robust Identity, Credential, and Access Management (ICAM) and micro-segmentation, rather than being a standalone product. Furthermore, solutions must adhere to the Agile Risk Management Framework (RMF), the mandatory pathway to an Authority to Operate (ATO), by incorporating security automation, continuous monitoring (ConMon), and a clear strategy for rapid, iterative accreditation via modern Development, Security, and Operations (DevSecOps) practices for a continuous (cATO). Finally, a commitment to an Open Systems Architecture (OSA) is required, mandating adherence to standards like the Sensor Open Systems Architecture (SOSA) and Open Mission Systems (OMS) to ensure future interoperability, avoid vendor lock-in, and support a modular, open design with non-proprietary interfaces for seamless integration and rapid, component-level upgrades.

The purpose of this IC CSO is to solicit innovative solutions that directly address efforts that align with the **IC mission.** If there are DoD elements supporting the IC efforts, submissions must explicitly address and justify how the DoD elements directly support IC mission objectives.
We seek partners who can deliver secure, scalable, and cutting-edge capabilities in key areas such as AI-driven predictive analysis, Joint All-Domain Command and Control (JADC2) integration, advanced sensing, and resilient cyber operations. Your challenge is to bring us your best commercial innovation, ready to be integrated, secured, and deployed at the speed of relevance to deter, and if necessary, defeat our nation's adversaries.

This is a CSO with Calls. This solicitation *is not* requesting any white papers or proposals at this time. Further, unsolicited proposals will not be accepted. Funding *is not* available at this time. It is the responsibility of the potential responders to monitor this site for additional information pertaining to this CSO and for the posting of the Open Call Periods. This CSO is the overarching umbrella solicitation from which Calls will be issued by the Acquisition Management and Integration Center, Detachment 2 (AMIC Det 2).

This CSO allows for Calls to be posted indefinitely with an annual update, until terminated. This CSO can result in the award of Contracts or Other Transaction Agreements (OTAs) as codified in 10 U.S.C. §2371. The Government reserves the right to award all, part, or none of the proposals received. All Calls issued under this CSO will include specific instructions including dates and times for submissions, Topics, evaluation criteria and proposal instructions to potential offerors. While each offeror shall adhere to the instructions of this CSO, the Calls may contain additional information the offeror shall adhere to. While each Call will be announced on the Government Point of Entry SAM.gov, https://sam.gov/content/home/ , other media outlets and resources may potentially be used, and result in the award of a Contract or OTA, if deemed in the Governments best interest. The Calls will identify the broadly defined Topic Area/s and provide more specific problem sets or objectives. Prospective offerors shall focus on creating an integrated solution, covering the Topic area/s listed and the objectives outlined within the specific CSO Call they are responding to.

All details of the CSO Call process shall be governed by this CSO unless otherwise noted or expanded upon within each Call. The Government is not obligated to make any awards as a result of this CSO and/or Calls issued under this CSO. All awards are subject to the availability of funds and successful collaboration with the offeror. Additionally, any resultant award has the potential for an increase in value and level of effort as the Government explores the product/solution. The Government is not responsible for any monies expended by the offeror prior to the issuance of a contract award to include, but not limited to, bid and proposal cost. The Government reserves the right to amend the solicitation requirements of this CSO and each subsequent Call at any time.

Calls issued under this CSO will be utilizing a two-step process as outlined below.

Two-Step process:

1. Offerors must submit a White Paper and Quad-Chart for evaluation in response to a posted Call. Once the evaluations are complete, all offerors will be notified as to whether or not they have been selected to move to step-two of the CSO Process. Submissions resulting in an unfavorable evaluation will not be considered further.

2. Proposals will only be accepted from Offerors who upon review of Step-one submissions are invited by the Contracting Officer (CO) to submit a full proposal. To be considered for award under Step-two, offerors must be registered in SAM in accordance with RFO 4.203, be considered responsible within the meaning of RFO 9.1, have a satisfactory performance record, and otherwise be eligible for award based on federal law and regulation.

Note: Do not include Proprietary, classified, confidential, or sensitive information in responses.

II. AREAS OF INTEREST

TOPIC 001: Data, Artificial Intelligence, and Decision Dominance

AI-Driven Predictive Intelligence Analysis

- AF IC seeks solutions that leverage Artificial Intelligence and Machine Learning (AI/ML) to move from a reactive to a predictive intelligence posture. Capabilities should include the autonomous analysis of multi-intelligence (multi-INT) data to anticipate adversary actions, identify emerging threats, and drastically reduce the time required to generate and disseminate tactical intelligence.

Human-Machine Teaming for Accelerated Sense-Making

- To overcome information overload, AF IC seeks intuitive platforms that enable seamless collaboration between human analysts and AI agents. The Government is interested in solutions that augment human cognition, automate laborious tasks, and utilize advanced visualization to help analysts make sense of vast, complex datasets at machine speed.

Commercial Data Integration and Analysis

- AF IC requires innovative methods and platforms to rapidly identify, vet, ingest, and integrate commercially available information and data streams into our intelligence workflows. This includes, but is not limited to, commercial satellite imagery, Radio Frequency (RF) sensing data, public records, and internet-of-things (IoT) data to enrich and add context to classified intelligence.

Information Operations and Counter-Disinformation

- AF IC seeks solutions capable of monitoring the global information environment to detect, analyze, and track adversary propaganda and disinformation campaigns. Key capabilities include sentiment analysis, source attribution, and the generation of data-driven counter-narratives to ensure information superiority.

TOPIC 002: All-Domain Command & Control

Joint All-Domain Command and Control (JADC2), Data Integration and Fusion

- To realize the vision of AF IC, the JADC2 needs a robust "digital backbone" to fuse data from disparate sensors and platforms across all domains. The Government seeks solutions for a common data layer that can normalize, process, and share Intelligence, Surveillance, and Reconnaissance (ISR) data in a secure, resilient, and cloud-native environment to create a common operating picture.

Multi-Domain Operations (MDO) Battle Management

- AF IC is interested in advanced battle management tools that enable the planning,

coordination, and synchronized execution of multi-domain operations. Solutions should provide the Government with decision-making aids to understand the cross-domain impacts of kinetic and non-kinetic effects in a dynamic environment. Digital Twin and Engineering for Mission Rehearsal, Tactics Development, and Training

- AF IC seeks to create a high-fidelity, continuously updated digital twin of the battlespace. The primary purpose of this environment is to enable the testing of tactics, rapid development and validation of new Tactics, Techniques, and Procedures (TTPs), and advanced mission rehearsal for aircrews, operators, and planners in complex, multi-domain contingencies, thereby improving readiness while reducing risk.

TOPIC 003: Resilient Cyber and Intelligence, Surveillance, Reconnaissance Operations

Advanced Sensing and Data Processing at the Edge

- As operations expand into contested, communication-denied environments, the Government requires solutions that enable the processing, exploitation, and dissemination (PED) of sensor data at the tactical edge. AF IC is interested in low Size, Weight, and Power (low-SWaP) hardware and software that can perform on-platform AI/ML inference to deliver time-sensitive intelligence directly to the warfighter.

Advanced Cyber Threat Intelligence

- To proactively defend our networks, the Government seeks predictive analytic platforms that can identify emerging cyber threats, TTPs, and malware before they are used against government systems. Solutions should provide actionable, machine-readable threat intelligence that can be automatically ingested by government defensive cyber platforms.

Quantum-Resistant Cryptography and Secure Communications

- AF IC requires a layered defense to detect, track, identify, and neutralize hostile Small Unmanned Aerial Systems (sUAS) threats. The Government is soliciting for commercial solutions for all aspects of the counter sUAS mission, including passive and active sensors, command and control integration, and kinetic and non-kinetic effectors.

Signals Intelligence (SIGINT) Modernization

- AF IC seeks to modernize government SIGINT capabilities with commercial technologies that leverage software-defined radios (SDR), advanced signal processing, and AI/ML for automated signal detection, classification, and geolocation across a congested and contested electromagnetic spectrum.

Cognitive Electronic Warfare (EW)

- AF IC seeks to modernize our SIGINT capabilities and develop a cognitive EW capability that leverages AI/ML for automated signal detection, classification, and geolocation. The Government is interested in software-defined systems that can autonomously sense and dynamically respond to novel threats across a congested and contested electromagnetic spectrum.

TOPIC 004: Foundational Digital Infrastructure

Multi-Cloud Abstraction, Orchestration, and FinOps for C2E

- The AF IC operates in a multi-cloud environment via the Intelligence Community's Commercial Cloud Enterprise (C2E) contract. The Government seeks a common abstraction layer or Cloud Management Platform (CMP) to provide a "single pane of glass" for managing, deploying, and securing applications across multiple classified cloud providers. Key capabilities include Infrastructure-as-Code (IaC) portability, unified security governance, and a robust Financial Operations (FinOps) dashboard to optimize cloud spending across the enterprise.

TOPIC 005: Enterprise Wide Integration and Architecture Modernization

The ACC/A2 seeks innovative solutions to support the integration of data across disparate monitoring phenomenologies and modernization of hardware/software architectures. This topic includes:

- New solutions to integrate data access and discoverability across varying monitoring phenomenologies to lower detection thresholds and/or increase efficiency of current operations.

- Technologies to modernize hardware/software architectures or implement improved software design and accrediting processes to more flexibly meet mission needs.

TOPIC 006: Enterprise Asset and Lifecycle Management Improvements

The ACC/A2 seeks innovative solutions that can provide enterprise-wide asset management visibility as well as improve our lifecycle management capabilities. This topic includes:

- Increase accuracy of forecasting of requirements and scheduling of procurements through the use and exploitation of supply chain demand data

- Supply chain management, specifically: Automated systems to reduce/eliminate inefficiency, improve asset control, decrease touchpoints and minimize inventory

- Automated identification and reporting of components and systems with substandard reliability

TOPIC 007: Air Force Intelligence Community Risk Management and Cybersecurity

The AF IC seeks machine learning and artificial intelligence solutions to transform the checklist-based ICD 503 RMF repetitive task to automated and predictive reporting process.

- Provide technology-based solutions to provide near-real-time cybersecurity posture information for the AF IC Enterprise.

- Provide detailed data analysis abilities in support of FISMA reporting.

- Provide highly skilled technical expertise supporting NIST 800-53 and other AF and National IC Risk Management and Cybersecurity mandated requirements.

TOPIC 008: Dynamic Force Resiliency

Sustained Operations During Contingencies

- The AF IC seeks innovative solutions to maintain continuous operations during high-tempo deployments or wartime surges. The Government is interested in novel approaches and frameworks from industry that ensure uninterrupted operations of critical administrative, intelligence, and operational planning functions.

Dynamic Continuity of Operations and Institutional Memory

- The Government seeks methodologies, platforms, or support structures that seamlessly capture, manage, and transfer institutional knowledge, daily workflows, and standard operating procedures. Proposed solutions should ensure immediate integration with minimal spin-up time.

Agile Workforce Adaptation and Cross-Functional Support

- The Government is seeking innovative solutions that enable rapid adaptation to changing mission requirements and provide cross-functional support or surge capacity – ensuring depth, structural flexibility, and continuous support operations.

III. CYBERSECURITY REQUIREMENTS AND SAM REGISTRATION
(https//www.SAM.gov/)

Cybersecurity Requirements
Small businesses looking to contract with the U.S. Department of War (DoW) will have to show the ability to safeguard their systems and data. Each DoW RFP will list a Cybersecurity Maturity Model Certification (CMMC) level required for submission.

To help small businesses with the tools and training to meet this standard, DoW developed Project Spectrum, a free platform that:

- Assists in CMMC certification
- Provides tools and training for cybersecurity awareness
- Educates users on risk management
- Helps small businesses install or boost cybersecurity hygiene

Visit Project Spectrum to sign up, learn about what you need to get certified, or to complete a self-assessment of your company's cyber readiness.

Unique Entity Identifier
Before you can bid on government proposals, you need to get a Unique Entity Identifier (UEI). A UEI is a unique 12-character, alpha-numeric value. You will receive a UEI when you register on SAM.gov.

If your entity is already registered with SAM, your UEI has already been assigned to you. Learn how to view your UEI within SAM at the Federal Service Desk. For more information see: https://business.defense.gov/Work-with-us/Guide-to-working-with-DoD/ .

IV. PRICE DETERMINATION: FAIR AND REASONABLE

Price shall be considered to the extent appropriate, but at a minimum price will be determined fair and reasonable in accordance with the procedures at R-DFARS 212.7004. The CO may request information from the offeror regarding recent purchase prices paid by the Government and/or commercial customers for the same or similar commercial items. Specific pricing requirements will be stated in CSO Calls.

V. DEFINITION OF TERMS

CSO with Calls: This allows for publication of an umbrella CSO solicitation that contains overarching information but does not request white papers or proposals. The CSO functions as a framework identifying the technical areas and giving the basic terms and administrative information of the CSO. Open and/or Closed Calls may be issued under this CSO to request submission of white papers and/or proposals. Calls may be issued at any time during the open period of the CSO. Each Call will be tailored to best fit the acquisition approach identified by the Government. The Calls may also include specific terms that apply to that Call such as further technical details and any pertinent clauses. Proposals and/or white papers are submitted to the Government only when Calls under this CSO are published.

Open Period Calls: This type of Call allows for white paper and/or proposal submissions at any time within a specified period as set forth in the Open Period Call.

Closed Calls: This type of Call allows for white paper and/or proposal submissions at a specified date and time as set forth in each Closed Call. This process and the dates associated with it are more structured than Open Period Calls.
Topics: These are specific requests for innovative solutions the Government will describe in each Call. An offeror's innovative solution(s) should focus on addressing specific Topics.

White Paper: A brief (usually 2-5 pages) summary of the proposed technical approach with an accompanying rough-order-of-magnitude (ROM) price.

Nontraditional Defense Contractor: As defined in 10 U.S.C. § 2302(9) as an entity that is not currently performing and has not performed, for at least the one-year period preceding the solicitation of sources by the DoW for the procurement or transaction, any contract or subcontract for the DoW that is subject to full coverage under the cost accounting standards prescribed pursuant to 41 U.S.C. § 1502 and the regulations implementing such section. This includes all small business concerns under the criteria and size standards in 13 C.F.R. Part 121.

Small Business Concern: Defined in the Small Business Act (15 U.S.C. 632) and 13 CFR Part 121.