Operational Test and Training Infrastructure (OTTI)

Commercial Solutions Opening (CSO)

FA2553-25-S-C001 Amendment 0010

7 November 2025

Note: This is amendment 0010 to the initial announcement. This amendment supersedes all versions of the OTTI CSO.

Record of Revisions

Revision	Description	Date
Amendment 0001	-Added Area of Interest 02 to Attachment 6 -Administrative update to paragraph 4.2 -Corrected numbering under paragraph 5.2	24 January 2025
Amendment 0002	-Added Area of Interest 03 to Attachment 6	31 January 2025
Amendment 0003	-Updated point of contact information in paragraphs 4.1, 4.1.1, 4.1.2, 4.2, 5.1.2, and 5.2.2 -Updated Attachment 2 instructions -Updated point of contact information in Attachment 6 -Added Area of Interest 04 to Attachment 6	21 March 2025
Amendment 0004	-Updated Area of Interest 04 Phase I Accepted Until date in Attachment 6	18 April 2025
Amendment 0005	-Updated Area of Interest 04 Phase I Accepted Until date in Attachment 6	2 May 2025
Amendment 0006	-Updated point of contact information in Attachment 6	15 July 2025
Amendment 0007	-Added Area of Interest 05 to Attachment 6	8 September 2025
Amendment 0008	-Updated Area of Interest 05 language in “Security Measures:” section in Attachment 6 -Updated Area of Interest 05 Phase I Accepted Until date in Attachment 6	15 September 2025
Amendment 0009	-Updated point of contact information in Attachment 6 -Added notification of pending updates to Area of Interest 05 in Attachment 6 -Updated Area of Interest 05 Phase I Accepted Until date in Attachment 6	2 October 2025
Amendment 0010	- Updated Area of Interest 05 language in “Security Measures” and “Cybersecurity Compliance” sections in Attachment 6 - Updated Area of Interest 05 Phase I Accepted Until date in Attachment 6	7 November 2025

Table of Contents

1. INTRODUCTION AND BACKGROUND 4
2. PURPOSE 4
3. CSO APPROACH 4
4. GENERAL INFORMATION 5
5. SUBMISSION INFORMATION 6
6. ADDITIONAL INFORMATION 8

ATTACHMENT 1: PHASE I – POWERPOINT BRIEFING 9
ATTACHMENT 2: PHASE I – WHITE PAPER FORMAT 10
ATTACHMENT 3: PHASE II – PITCH SESSION FORMAT 11
ATTACHMENT 4: PHASE III – TECHNICAL, SOW, AND PRICE PROPOSAL 12
ATTACHMENT 5: EVALUATION AND SELECTION PROCESS 16
ATTACHMENT 6: AREAS OF INTEREST (AOI) 18

1. INTRODUCTION AND BACKGROUND

1.1 The United States Space Force (USSF) Operational Test and Training Infrastructure (OTTI) Enterprise is issuing a Commercial Solutions Opening (CSO) in accordance with Defense Federal Acquisition Regulation Supplement (DFARS) 212.70 Defense Commercial Solutions Opening. Under the OTTI CSO, the Government may award proposals received in response to a general solicitation to acquire innovative commercial products, technologies, or services based on a review of solutions by scientific, technological, or other subject matter expert peers within OTTI. "Innovative" for CSO purposes, means any new technology, process, or method, including research and development (R&D), or any new application of an existing technology, process or method, as of the date of the submission of a proposal. Under this CSO, all products, technologies, and services shall be treated as commercial items; products, technologies, and services do not have to be "commercially available" to be submitted in response to this solicitation. If the solution meets the requirements of the regulation, the solution is treated as commercial whereby the Contracting Officer will utilize commercial procedures to develop and execute the resultant award.

1.2 OTTI is seeking innovative capabilities, solutions, and technological advancements for the OTTI Enterprise to include but not limited to space test, training, exercises, wargaming, ranges, systems, physical/live environments, synthetic/virtual environments, infrastructure, and sustainment of capabilities.

1.3 The primary North American Industry Classification System (NAICS) code for this CSO is 541715, Research and Development in the Physical, Engineering, and Life Sciences. There is a potential for an Area of Interest (AOI) to require a different NAICS code. Any deviation from the primary NAICS code will be identified in Attachment 6.

2. PURPOSE

2.1 This CSO, in accordance with DFARS 206.102-70(a), is a competitive solicitation focused on innovative technologies and services to meet the mission of the OTTI Enterprise. The Government seeks to obtain innovative solutions or potential new capabilities to fulfill requirements, close capability gaps, or provide potential technological advancements. The Government's AOIs appear in Attachment 6.

3. CSO APPROACH

3.1 This CSO seeks the innovative approaches to meet various OTTI objectives. The Government encourages proposals that span a wide spectrum of possible technical and business solutions in response to the specific AOIs. Each AOI will identify the OTTI Enterprise's interest for an individual program requirement or a broadly defined interest covering the full range of the program requirements. All submissions in response to any AOI will be governed by this CSO unless otherwise noted in the individual AOI in Attachment 6.

3.2 The Government anticipates the award of fixed-price type contracts, including fixed-price incentive contracts. In addition, the Government reserves the right to award Other Transactions (OT) for certain prototype projects in accordance with 10 U.S.C §4022.

3.3 OTs for Research, Prototype, and Production: Upon favorable review and available funds, the Government may choose to award an OT for Research, Prototype, and Production as deemed appropriate for the transaction. The Agreements Officer will negotiate directly with the Offeror on the terms and conditions of the OT, including payments, and will execute the OT on behalf of the Government. Upon successful completion of a prototype project under an OT for Prototype agreement, the Government and Offeror may negotiate a follow-on production contract or agreement without further competition as authorized under 10 U.S.C. § 4022(f). Any concept/technology/solution successfully proven through an OT for Prototype can be transitioned to production. Any resultant OT for Prototype awarded under this CSO will include language providing for the potential award of a follow-on production contract or agreement.

3.4 Awards resulting from this CSO will be made based on the evaluation results of a two or three phased process described in Section 5. The Government reserves the right to fund all, some, one, or none of the proposals submitted. The Government may elect to fund only part of a submitted proposal and may incrementally fund any or all awards under this CSO. All awards are subject to the availability of funds.

3.5 All coordination and communication between Offerors and the Government will be conducted using the www.sam.gov website and the point of contact associated with this CSO, as specified in Section 4.

4. GENERAL INFORMATION

4.1 *POINT OF CONTACT:* The Contracting Officer, Ms. Crystal Price, and the Contract Specialist(s) are the sole points of contact for the OTTI CSO. Each AOI will have its own Contracting Team which will be the sole point(s) of contact for the individual AOI. The Contracting Team AOI point(s) of contacts are listed in Attachment 6.

4.1.1 CSO General Questions – General CSO Questions may be sent via email to the CSO Contacting Team at SSC.OTTI.CSO@spaceforce.mil. Due to the large amount of expected interest in this CSO, and to maintain a written record of questions, this is the only email address that will be used for general question communication. Material questions and answers will be published and updated on www.sam.gov.

The following shall be utilized in the email subject line: **OTTI CSO General Question(s)**.

4.1.2 AOI Specific Questions and Submittals - AOI specific questions may be sent via email to the AOI Contracting Team's point(s) of contacts listed in the AOI. Due to the large amount of expected interest in AOIs, and to maintain a written record of questions, the AOI Contracting Team's point(s) of contact email address(es) will be used for communication. Material questions and answers will be published and updated on www.sam.gov.

The following shall be utilized in the email subject line: **OTTI CSO AOI number** (ex., AOI 01, AOI 02, etc.).

4.2 *CLASSIFIED INFORMATION:* All Phase I submissions shall be unclassified. If higher classification is required for the Offeror to submit their solution in Phase II or Phase III, the Offeror shall coordinate with the AOI Contracting Team for submission instructions.

Offerors must possess all required personnel security clearances, facility clearances, and other infrastructure requirements necessary to perform any proposed classified work in accordance with the draft Contract Security Classification Specification (DD Form 254) without reliance on Government resources. As a wide variety of responses, as well as potential awards of diverse scope and associated classified classification levels under this CSO are possible, the Government will provide award specific security details for individual award actions as required. A draft DD Form 254 will be provided with a Phase III request for proposal, as necessary.

5. SUBMISSION INFORMATION

5.1 *SUBMISSION OVERVIEW:* The OTTI CSO will remain open indefinitely with annual updates. This CSO is open for Phase I submissions in accordance with the AOIs outlined in Attachment 6. The acceptance date for Phase I submissions will be identified by individual AOIs. The Government will amend the CSO to incorporate additional AOIs as needed.

5.1.1 The Government will not reimburse companies for the costs associated with submissions for any phase.

5.1.2 Submissions for all phases shall be sent to the Contracting Team's point(s) of contact listed in the individual AOI. In order to ensure submissions have been received by the Government, Offerors shall send a separate email (not containing attachments) to the Contracting Team's point(s) of contact listed in the individual AOI immediately after emailing a submission to confirm receipt. Hardcopies for any phase will not be accepted.

5.1.3 Offerors shall mark each page of the Phase I, Phase II, and Phase III submissions that contain proprietary information.

5.2 *TWO OR THREE PHASED SUBMISSION PROCESS:* This CSO may be conducted in two or three phases as follows:

5.2.1 Phase I - PowerPoint and White Paper: Phase I solutions will be requested by individual AOI. Solutions will be evaluated for each AOI. Interested Offerors must submit a PowerPoint briefing and White Paper in accordance with instructions provided in Attachment 1 and 2. Acceptance dates for the Phase I PowerPoint and White Paper will be located in Attachment 6 with the respective AOIs. Due to the broad requirements and financial scope of this CSO, Offerors must ensure that submissions are succinct yet descriptive.

5.2.2 Phase II - Pitch Session: Phase II submissions will only be accepted from Offerors who upon review of Phase I submissions, are invited by the AOI Contracting Team to a pitch session. Instructions for format and content are located in Attachment 3.

Please note: The Government reserves the right to forgo Phase II and go directly to Phase III.

5.2.3 Phase I & II Review, Evaluation, and Selection Process: Each Phase I and II submission will be evaluated by the Government in accordance with the process outlined in Attachment 5.

5.2.4 Notification of Selection: If a Phase I solution is selected and funding is available, the Government will contact Offerors via email either with an invitation for a Phase II Pitch Session or a Phase III request for proposal with a specific submission date. If a Phase I solution is selected and there is insufficient funding, the Government may request that the solution be maintained in the electronic library for consideration and subsequent funding availability up to one year after submission. A request for a Phase II or Phase III submission does not guarantee award. If a solution is not selected in Phase I or Phase II, the Offeror will be notified generally within 45 days of submission.

The Government reserves the right to select none of the submissions.

5.2.5 Phase III - Technical, SOW, and Price Proposal: Phase III proposals will only be accepted from Offerors who upon review of either Phase I or Phase II submission, have received a request from the Contracting Officer to submit a full proposal (Technical, Price, and Statement of Work (SOW)).

5.2.5.1 Proposal Submission: Upon notification for a request for proposal by the Contracting Officer, Offerors will typically have 30-45 calendar days to prepare and submit a proposal in accordance with the format and instructions in Attachment 4. Actual due dates for proposals will be included in the Phase III request for proposal.

5.2.5.2 Proposal Review, Evaluation, and Selection Process: Each proposal will be evaluated by the Government and the proposal must stand on its own technical merit. Offerors may be ineligible for award if all requirements of the CSO and individual request for proposal are not met. Proposals will be evaluated in accordance with the criteria and selection process specified in Attachment 5. Proposals need not be evaluated against each other since they are not submitted in response to a common performance work statement (PWS) or SOW. The Government reserves the right to negotiate proposal scope of work, price, and other terms and conditions as may be required.

5.2.5.3 Selection for Award: Award(s) will be made once a proposal is accepted based on the evaluation criteria in Attachment 5.

The Government reserves the right to award none of the submissions.

6. ADDITIONAL INFORMATION

6.1 *DATA RIGHTS:* It is the Government's intention to acquire only Technical Data, Computer Software, and Computer Software Documentation data rights necessary to satisfy agency needs. The data rights will be negotiated at the contract or agreement level.

6.2 *FOREIGN PARTICIPATION:* Foreign firms are advised that they will not be allowed to participate in this CSO. The research and test data produced under a resultant contract or agreement may contain Military Critical Technology List (MCTL) information whose export is restricted by Export Control Act (Title 22, U.S. Sec 2751, et seq.) or the Export Administration Act of 1979, as amended (Title 50, U.S.C., App. 2401, et seq.). Request certification and registration from the Defense Logistics Services Center (DLSC), Federal Center, 74 North Washington, Battle Creek, MI 49016-3412 as soon as possible.

6.3 *NON-GOVERNMENT ADVISORS:* In order to review submissions resultant from any phase, PROPRIETARY information may be given to Federally Funded Research and Development Centers (FFRDC), Systems Engineering and Technical Assistance (SETA), Systems Engineering and Integration (SE&I), and/or Advisory and Assistance Services (A&AS) contractors working for the Government. The non-Government advisors have signed a non-disclosure agreement with the Government.

6.4 *PROCUREMENT INTEGRITY, STANDARDS OF CONDUCT, ETHICAL CONSIDERATIONS, AND CONFLICTS OF INTEREST:* Any Offeror who currently provides A&AS, SETA, SE&I, or FFRDC support services to OTTI is precluded from providing a submission in response to any AOIs on this CSO. Submissions from conflicted companies will be discarded without evaluation. This includes any LLC's, subsidiaries, partnerships, or any affiliations that could create the appearance of an OCI.

6.5 *DEBRIEFINGS:* The Government will conduct written, post-award debriefings for Phase III proposals upon request only in accordance with FAR 52.212-1(l) and will address the evaluation factors contained herein only. It will not include a comparison of submissions against a common PWS or SOW as the CSO provides no common PWS or SOW that interested parties must respond to and instead represents opportunity for submission of a variety of innovative commercial items, technologies, and/or services that represent meaningful submissions of diverse scope and price.

6.6 *GOVERNMENT FURNISHED PROPERTY (GFP) AVAILABILITY:* GFP is not anticipated to be made available under any resulting contract or agreement, but a determination regarding GFP will be made for each award. In accordance with FAR 45.201(b), the contractor is responsible for all costs related to making the property available for use, such as payment of all transportation, installation, or rehabilitation costs.

6.7 *BASE SUPPORT/NETWORK ACCESS:* Base support will be determined for each award for testing, validation, and demonstration.

ATTACHMENT 1: PHASE I – POWERPOINT BRIEFING

Each Offeror shall submit their plans to provide an innovative solution to the individual AOI in Attachment 6. The following Quad Chart must be included as the first content slide in the Phase I PowerPoint briefing submission. Quad Charts shall not exceed 1-page in landscape view. Quad Charts must follow the formatting guidelines on the slide template below. All fonts must be Times New Roman ≥12pt. All PowerPoint briefings shall be limited to no more than five slides, not including a title slide and the Quad Chart, with file size not greater than 10MB. PowerPoint briefing submissions shall be provided in .pptx format. The PowerPoint briefings should provide visuals and further elaborate on the information provided on the Quad Chart. Graphics Interchange Format (GIFs), videos/movies, or clips are permitted. Phase I submissions will not be evaluated beyond page length limitations.

UNCLASSIFIED

Company - Project Title

Objective: Clear, concise (1-2 sentences) description of the goal of the effort. Which AOI is this addressing? (≥12pt font)

Description of Effort: Brief description of the solution or capability's technology, process, or method. *Must describe how this capability is innovative.* (≥12pt font)

Solution Approach: e.g., Modify existing or new build or other

State of Solution: Description of the current state of solution or technology proposed (e.g., technology maturation or technology readiness level) (≥12pt font)

Benefits: Brief statement that identifies the advantages of proposed solution in relation to the AOI it is addressing (≥12pt font)

Challenges:
- Bulleted list of technical or timeline challenges (≥12pt font)

Major Milestones to Capability Delivery (FY):
- Bulleted list must include major milestones and anticipated delivery dates of functioning capability (≥12pt font)

Rough Order Magnitude: Insert dollars/Government Fiscal Year (FY)

Year 1	Year 2	Year 3	Year 4	Year 5	Total
$	$	$	$	$	$

UNCLASSIFIED

1

ATTACHMENT 2: PHASE I – WHITE PAPER FORMAT

1. The White Paper narrative expands on the PowerPoint and must be 8.5 x 11 inches with one-inch margins, no longer than two pages, single-spaced, with text in Times New Roman, and no smaller than 12-point font. Each Offeror shall describe their plans to provide an innovative solution to the individual AOI in Attachment 6.

2. The White Paper shall contain a cover sheet* containing the following information. The cover sheet will not count against the page limitation.

   (a) CSO number, AOI number, and AOI name
   (b) Project Title
   (c) Full company name and address
   (d) CAGE code
   (e) Unique Entity ID number
   (f) Business Size Classification (large, small, or other)

3. White Papers must be submitted electronically as a PDF not exceeding a file size of 10 MB. Pages in excess of the page limitation will not be read or evaluated.

4. The White Paper should provide sufficient information on the technical approach being submitted to allow for an assessment by a technical expert. Expand as deemed necessary on the following sections of the PowerPoint: Objective; Description of the Effort; Benefits of the Proposed Approach; Technical Challenges; Solution Approach; State of Solution; Major Milestones by Government fiscal year and month; and the Rough Order of Magnitude (ROM) price estimate. Do not include corporate or personnel qualification, past experience or any supplemental information not requested in the PowerPoint.

***The requirement for a cover sheet is applicable for all Phase I White Papers submitted in response to new AOIs published on or after 21 March 2025.**

ATTACHMENT 3: PHASE II – PITCH SESSION FORMAT

1. During this phase, Offerors are invited to pitch and further discuss the proposed concept/technology/solution virtually. The Government will provide the Offeror 45 minutes for the Offeror's pitch and additional time if needed by the Government for follow-up questions/discussion.

2. Offerors shall provide a virtual pitch to demonstrate and provide further details on the technical and business viability of the concept/technology/solution. In addition to the pitch, the Government, at its discretion, may request an additional written submission to further supplement the information provided in Phase I solution brief.

3. During the pitch session, the Offeror must detail/address:

   (a) Estimated Price/Schedule: Provide a ROM price estimate and notional schedule.

   (b) Data Rights Assertions: The solution brief will identify any Intellectual Property (IP) involved in the effort and associated restrictions on the Government's use of that IP. Data rights will be negotiated at the contract or agreement level.

***Note: The Government reserves the right to forgo Phase II and go directly to Phase III.**

ATTACHMENT 4: PHASE III – TECHNICAL, SOW, AND PRICE PROPOSAL

The Phase III proposal submission shall conform to the following:

1. Cover Sheet: The following information shall be contained in a cover sheet submitted with the proposal:

(a) CSO number, AOI number, and AOI name

(b) Full company name and address

(c) CAGE code

(d) Unique Entity ID number

(e) Business Size Classification (large, small, or other)

(f) Offeror's socioeconomic status

(g) Point of contact, name, title, phone number, and email address

2. Technical Approach: The following describes the technical approach requirements:

(a) The Technical Approach shall describe the background and objectives of the proposed work, the approach, deliverables, the resources needed to execute, and additional details of data rights assertions. Include the nature and extent of the capability and how it addresses the AOI, the innovative aspect of the solution, the intended results, and address possible integration or testing needs. Include ancillary and operational considerations such as certifications, algorithms, and any engineering/software development methodologies to be used. Provide a graphic display of major program milestones. Measurable milestones should capture key activity points and should be clearly articulated and defined in time relative to the start of the effort. You may refer to previous submitted information from Phase I and II, but do not duplicate it.

(b) Government Support Required: Identify the type of support, if any, the Offeror requests of the Government in general, such as facilities, equipment, data, and information or materials.

(c) The Government reserves the right to ask for additional technical information in the Phase III request for proposal.

(d) Due to the varying AOIs and potential solutions, Technical Proposal page limitations and formatting will be identified in the Phase III request for proposal.

3. Statement of Work (SOW): The following describes the SOW requirements:

(a) The SOW must be a separate and distinct document suitable for incorporation into the contract or agreement. Pages should be numbered, and the initial page should have a date (document date) shown under the title. DO NOT INCLUDE ANY PROPRIETARY INFORMATION IN THE SOW.

(b) The proposed SOW must accurately describe the work to be performed. The SOW must also contain a summary description of the technical methodology as well as the task

descriptions, but not in so much detail as to make the SOW inflexible. The SOW should include the following sections:

1. *OBJECTIVE:* This section is intended to give a brief overview of the project and should describe why the work is being pursued and what the Offeror intends to accomplish.

2. *SCOPE:* This section includes a statement of what the SOW covers. This should describe the AOI to be investigated, goals, and milestones for the effort. Provide a graphic display of major program milestones.

3. *BACKGROUND:* The Offeror must identify appropriate documents that are applicable to the effort to be performed. This section includes any information, explanations, or constraints that are necessary to understand the project tasks and requirements. This section should describe the effort's relationship to previous and ongoing efforts, if applicable.

4. *TASKS AND TECHNICAL REQUIREMENTS:* This section contains the detailed description of tasks that are necessary to perform the proposed work. These tasks will represent the work to be performed in any potential contract or agreement award, and, thus, shall be considered contractually binding. This section should be developed in an orderly progression and presented in sufficient detail to establish the feasibility of accomplishing the overall program goals. Note: The Government reserves the right to modify and negotiate the language in the SOW prior to any potential contract or agreement award.

   4.1. Task descriptions must be definite, realistic, and clearly stated. Use the phrase "the contractor shall" whenever the work statement expresses a provision that is binding. Use "should" or "may" whenever it is necessary to express a declaration of purpose. Use "will" in cases where no Offeror requirement is involved (e.g., power will be supplied by the Government).

   4.2. Do not use acronyms or abbreviations without first defining them. Place abbreviations and acronyms in parentheses following the first usage of the spelled-out phrase.

(c) Due to the varying AOIs and potential solutions, SOW page limitations will be identified in the Phase III request for proposal.

4. Price: The following describes the Price requirements:

(a) The Price submission must include pricing information sufficiently detailed for meaningful evaluation of the proposal. The Price Proposal does not have a page limit restriction.

(b) Since all proposals are considered commercial items, technologies, or services, the requirements of the Truthful Cost or Pricing Data Act are not applicable. However, if the Contracting Officer determines additional information is necessary to support a determination of a fair and reasonable price, other than certified cost and pricing data may

be requested.

(c) The responsibility for providing adequate supporting data and attachments lies solely with the Offeror. Further, the Offeror must also bear the burden of proof in establishing reasonableness of proposed prices; therefore, it is in the Offeror's best interest to submit a fully supportable and well-prepared price proposal.

(d) The Offeror shall prepare the Price submission to include an electronic version of the pricing model in a Microsoft (MS) Excel editable format. The electronic pricing model shall include active formulas demonstrating the mathematical calculation of the proposed price.

5. Additional Proposal Submission Content:

(a) Small Business Subcontracting Plan: Large business Offerors shall submit either an individual subcontracting plan and/or master subcontracting plan (if available) in accordance with FAR 52.219-9 Small Business Subcontracting Plan (Sep 2023), DFARS 252.219-7003 Small Business Subcontracting Plan (DoD Contracts) – Basic (Dec 2019) and DFARS 252.219-7004 Small Business Subcontracting Plan (Test Program) (Dec 2022) with their Phase III proposal. The Offeror's small business subcontracting plan shall include, but is not limited to, detailing the commitment/targets for each category of small business, veteran-owned small business, service-disabled veteran-owned small business, small disadvantaged business, HUBZone, and women-owned small business concerns. The plan shall describe for each category the total value subcontracted expressed in dollars and percentage of total subcontracted value if an individual subcontracting plan. The plan shall also state the extent and nature of work to be performed by small business concerns, the method used to develop goals, the method used to locate potential suppliers, if the goals include indirect costs (if so, describe the cost allocation method) and describe the efforts the Offeror will make to assure small businesses have an equitable opportunity to compete for subcontracts. If the planned goals do not meet or exceed DoD Fiscal Year (FY) subcontracting goals found at https://business.defense.gov/About/Goals-and-Performance, substantial explanation/rationale shall be provided. The plan shall also provide the name and duties of the contractor's subcontracting plan administrator.

If the Small Business Subcontracting Plan is not initially acceptable, the Contracting Officer may request additional information regarding the Small Business Subcontracting Plan.

(b) Organizational Conflict of Interest: The Offeror shall perform an Organizational Conflict of Interest (OCI) analysis and submit the results of that analysis as part of the Offeror's Phase III proposal. Specifically, the Offeror shall analyze the planned acquisition for actual or potential OCI situations associated with the Offeror or any of the Offeror's proposed teammate's or subcontractor's performance under any contract or agreement the Offeror or the Offeror's teammates or subcontractors has been or may be awarded by any federal agency or other entity. The Offeror shall describe in detail the methodology used to identify actual or potential OCI issues. If the Offeror identifies any actual or potential OCIs with respect to the performance of the Offeror or the Offeror's subcontractors or teammates, the contractor shall provide an OCI Mitigation Plan to be incorporated as an attachment to any resulting contract or agreement. Any proposed avoidance or mitigation techniques shall be consistent with FAR 9.5 and the

most recent decisions of the Government Accountability Office (GAO) and the U.S. Court of Federal Claims.

(c) Responsibility: The Offeror shall provide information that presents a brief verifiable self-assessment in the areas of responsibility as described in FAR 9.104 as supplemented by DFARS and Department of the Air Force Federal Acquisition Regulation Supplement. Elements of responsibility to address include but are not limited to, management of government property, capability, resources, competency, capacity, credit, integrity, perseverance, tenacity, and limitations on subcontracting.

Inability to perform in compliance with the limitations of subcontracting clause FAR 52.219-14 is a matter of responsibility for small businesses. The Contracting Officer will follow the Small Business Administration Certificate of Competency procedure at FAR subpart 19.6 when a small business concern would otherwise be selected for award but is considered not responsible.

(d) Space Contractor Responsibility Watchlist (CRWL): In accordance with Section 1612 of the National Defense Authorization Act (NDAA) for FY 2018 (P.L. 115-91) and SSC Instruction (SSCI) 64-101, the Contracting Officer may not award a contract to a contractor included on the CRWL without making a determination of responsibility and obtaining the approval of the SSC Commander. A contractor that has been notified that it has been added to the CRWL may respond to this CSO but must submit documentation describing how it has addressed the conditions that resulted in its inclusion on the CRWL and why those conditions will not impact performance on a contract resulting from this CSO. Proposed subcontractors must notify the prime Offeror if they receive notification from the SSC Commander that they have been added to the CRWL. In order to be considered for a subcontract, a proposed subcontractor that has been added to the CRWL must submit documentation describing how it has addressed the conditions that resulted in its inclusion on the CRWL and why those conditions will not impact its performance on a subcontract to a contract resulting from this CSO. The proposed subcontractor may submit CRWL-related documentation through the prime Offeror or directly to the Contracting Officer as long as the information is received prior to the proposal due date.

Note: CRWL does not apply to operation and maintenance contracts, professional services contracts for Government support (e.g., FFRDC, A&AS), or OTs.

(e) Rights in Technical Data, Computer Software, and Computer Software Documentation: An Offeror may provide with its submissions assertions to restrict, use, release, or disclosure of data and/or computer software and computer software documentation that will be provided in the course of contract or agreement performance. Rules governing these assertions are prescribed in DFARS clauses 252.227-7013, -7014, and -7017 and may be accessed at www.acquisition.gov.

ATTACHMENT 5: EVALUATION AND SELECTION PROCESS

The Phase I, II, and III submissions will be evaluated and selected as follows:

1. **Phase I – PowerPoint and White Paper:** The Government will review the Phase I submissions and select the Offerors that have the greatest potential to meet the needs of the OTTI Enterprise based upon the AOI outlined in Attachment 6. A determination will be made if an Offeror is technically qualified and has a comprehensive understanding to provide their innovative solution based on the information stated in the PowerPoint and White Paper. The Government will evaluate using the factors below:

    - Technical merit/applicability
    - Funds Availability

2. **Phase II – Pitch Session:** If Phase II is utilized, the Government will review the Phase II submissions and select the Offerors that have the greatest potential to meet the needs of the OTTI Enterprise based upon the AOI outlined in Attachment 6. A determination will be made if an Offeror is technically qualified and has a comprehensive understanding to provide the innovative solution based on the information presented during the Pitch Session as well as any additional written submissions requested by the Government. The Government will evaluate using the factors below:

    - Technical merit/applicability
    - Funds Availability

3. **Phase III – Technical, SOW, and Price Proposal:**

(a) The Government will review the Phase III proposals and award to the Offerors that have the greatest potential to meet the needs of the OTTI Enterprise based upon the AOI outlined in Attachment 6. A determination will be made if an Offeror is technically qualified and has a comprehensive understanding to provide the innovative solution based on the proposal. The Government will evaluate using the factors below. The evaluation factors are of equal importance.

- Technical merit/applicability
- Importance to agency programs
- Price

(b) The method of evaluation will include scientific, technological, or other subject-matter expert peer review process.

(c) Proposals need not be evaluated against each other since they are not submitted in response to a common PWS or SOW. The Government reserves the right to fund all, some, one, or none of the proposals submitted. The Government may elect to fund only part of a submitted proposal and may incrementally fund any or all awards under this CSO.

(d) Other Award Considerations

- In order to be considered for award under Phase III, Offerors must be registered in the System for Award Management (SAM) at www.sam.gov, be considered responsible within the meaning of FAR Part 9.1, Responsible Prospective Contractors, have a satisfactory performance record, and otherwise be eligible for award based on federal law and regulation. The Contracting Officer cannot award a contract unless the successful Offeror has updated the FAR 52.204-26 representation in SAM to account for the update to the provision published in October 2020.

- In accordance with DFARS 252.204-7019, the Contracting Officer cannot award a contract unless the successful Offeror has a current NIST SP 800-171 DoD assessment completed and posted in the Supplier Performance Risk System (SPRS) – see DFARS 252.204-7019 and DFARS 252.204-7020 for more information regarding the requirements.

ATTACHMENT 6: AREAS OF INTEREST (AOI)

OTTI is interested in innovative products, technologies, and services related to the AOIs listed below. The level of detail provided for each topic or the order in which they appear is not intended to convey any information regarding relative priority.

AOI 01: Advanced 1-Meter Class Commercial Off the Shelf (COTS) Electro-Optical (EO) Solutions Optimization

Space Systems Command OTTI Directorate's Physical Test and Training Branch (SSC/TIDP) is seeking innovative solutions that combine advanced Electro-Optical (EO) technology solutions and expertise to inform beyond state-of-the-art sensitivity, resolution, and data processing techniques using a 1-meter class COTS telescope. This AOI includes, but is not limited to adaptive optics, interferometry, spectroscopy, machine learning, and a Command and Control (C2) structure to enable artificial intelligence-driven automation of sensor tasking, sensor configuration, and various data processing applications designed to maximize COTS system performance. The resulting solutions, consolidated into an EO hub or Center of Excellence, will create a centralized hub for optical innovation and optimization to enable detection of very small objects in all orbital regimes (including cislunar), the ability to differentiate between closely spaced objects, and enable real-time Time and Space Position Information (TSPI). Access to a COTS 1-meter class telescope to verify and validate performance of prototypical hardware, software and processing techniques is necessary and proposed solutions should be scalable and adaptable to future technology advancements, with the flexibility to integrate emerging optical innovations. Submissions should detail the approach for integrating advanced optics expertise with COTS solutions and outline the structure, focus areas, and strategy for an EO hub or Center of Excellence.

Phase I	Accepted Until
Phase I PowerPoint and White Paper	11:59 pm MT on 21 January 2025

Contracting Team Points of Contact	SSC.TIP.CSO@spaceforce.mil

AOI 02: National Space Test and Training Complex (NSTTC) Range Control System Enhancements

Space Systems Command OTTI Directorate's Physical Test and Training Branch (SSC/TIDP) is seeking innovative solutions that can provide state-of-the-art software application development supporting tactical command and control capabilities for the physical ranges of the NSTTC. These physical ranges include the Orbital, Electromagnetic Spectrum Operations, and Cyber ranges. The proposed solution, which would be an expansion of software tools, visualizations, and data processing applications supporting range control software for the Orbital Range, will enhance the user interface and capabilities. Proposed solutions should be scalable and adaptable to future range control software enhancements, with the flexibility to adapt to changing multi-level-security (MLS) requirements. Submissions should detail the approach for integrating requirements into the design, enhancement, and creation of innovative graphical user interface (GUI) and tools through innovative software development and DevSecOps to existing commercial software applications. The ability to obtain and maintain an authority to operate (ATO) for any software capabilities are required.

Phase I	Accepted Until
Phase I PowerPoint and White Paper	12:00 pm MT on 11 March 2025

Contracting Team Points of Contact	SSC.TIP.CSO@spaceforce.mil

AOI 03: Distributed Synthetic Training Environment Evolution & Prototyping

Space Systems Command's OTTI Directorate's Digital Test and Training Branch (SSC/TIDV) is seeking innovative solutions to extend and enhance existing fielded USSF Space Flag distributed synthetic training capabilities to deliver the continuous, enduring, and integrated digital arena required to equip combat-ready Guardians for a Great Power Competition (GPC). This effort shall modify existing software in use by Space Training and Readiness Command (STARCOM) for mission analysis, readiness, and planning to yield low-fidelity synthetic training for priority USSF mission threads.

TIDV is seeking solutions that prototype a constructive simulation environment for training new classified mission systems driven by existing classified simulation data related to priority USSF mission threads. This AOI includes, but is not limited to, Minimum Viable Product delivery that fast-tracks a near-term ability to support Space Forces Generation (SPAFORGEN) to prepare for a near-peer conflict and establishes a baseline for future SPAFORGEN capabilities development.

Tasks may include, but are not limited to, enhancements to fielded and in-development software; upgrades to existing software architecture to prototype live range and mission system data over simulation integration; integration with third-party mission simulators, security accreditation of software modifications, including cloud-based solutions; mission thread model and scenario design; and enhancements to training data analysis and visualization functions. AOI submissions must address the evolution of fielded technology; methodology for integrating / onboarding third-party developed models, simulations, artificial intelligence (AI) tools, and other space operations training software tools; and relationship management with STARCOM stakeholders. Prototype solutions must be delivered and integrated within 18 months of contract award.

Offerors will include whether they have an existing/approved Facility Security Clearance and the level of this approval in the response.

Phase I	Accepted Until
Phase I PowerPoint and White Paper	12:00 pm MT on 24 February 2025

Contracting Team Point of Contact	aleksandr.oumarbaev@spaceforce.mil

AOI 04: Multirole Satellite Frequency In-field Test Suite (MSFITS)

Space Systems Command OTTI Directorate's Physical Test and Training Branch (SSC/TIDP) is seeking innovative solutions for a field-transportable satellite communications (SATCOM) environment monitor and emulator system in support of the National Space Test and Training Complex – Electromagnetic (NSTTC-E) range. This range enables the testing and training of Space Force Guardian's and the Joint Forces to support re-optimization for a great power competition.

TIDP is interested in a field-deployable, ruggedized system (10 Rack Units or smaller) that can receive, emulate, and transmit high-fidelity commercial and non-commercial radio frequency (RF) signals (SATCOM focus with potential expansion to additional capability). The system shall have multiple RF I/O channels (min 4 Rx, min 2 Tx) supporting coherent receive and simultaneous Rx/Tx operation from 10 MHz up to 6 GHz (min 950 to 2150 MHz) with up to 128 MHz of Instantaneous Bandwidth (IBW) per channel. Note this system encompasses a "backend" system only; assume antenna and any necessary down-conversion is accomplished via existing hardware.

The system must be dynamically reconfigurable to meet the needs of Joint Force SATCOM testing and training. The system must be configurable to operationally-represent contested environment with the ability to create, save, load, duplicate, modify, rename and delete configurations. The ability to be operated as a SATCOM transponder emulator (including channel effects and modem(s)) for hardware in the loop (HWIL) applications would be a desirable add-on capability (not necessarily within the stated Size, Weight, and Power (SWAP) profile). The ability to obtain and maintain an Authority-To-Operate (ATO) is required.

The system should:

- Be operator-focused from both physical and software-Graphical User Interface (GUI) perspectives.

- Provide the operator the necessary spectrum, time-frequency domain, Real-Time Spectrum Analysis (RTSA), and data-level visualization tools to understand the complete environment and inform real time decisions.

- Provide useful spectrum metrics/measurements to include (but not limited to) multi-signal Center Frequency identification, Power Spectral Density (PSD), total power in selected bandwidth, channel power, modulation type, Forward Error Correction (FEC) type/rate, anomaly detection/alarms, analysis of satellite carriers, selectable signal parameter change detection, up to 12 configurable signal traces.

- Include local data storage of at least 20 terabytes (TB) with the ability to two-way transfer data files (expandable to add additional capacity) for recordings (time-synched IQ/IQ snippets and operator screen recordings); all recording types must be able to be played back within the system.

- Support additional capability scaling by interfacing multiple units on an as needed basis.

- Have the means to provide configurable signal parameter delta measurements between selected signals (up to 12).

Phase I	Accepted Until
Phase I PowerPoint and White Paper	12:00 pm MT on 14 May 2025

Contracting Team Points of Contact	SSC.TIP.CSO@spaceforce.mil

AOI 05: Continuous Fitness Assessment (CFA)

Space Systems Command's OTTI (SSC/OTTI) is seeking innovative solutions to support the health and wellness of the USSF Guardians leveraging technology and science-based approaches utilizing a Portable Wearable Fitness Device (PWFD), and the software and infrastructure required to implement a program in compliance with DoD security requirements for Continuous Fitness Assessment (CFA). By implementing CFA, the USSF departs from normative standards and episodic, appointment-based assessments to a fitness monitoring capability that will both promote and require an enduring, uninterrupted application of exercise and purposeful physical activity (PPA). This innovative shift will leverage the potent effects of exercise and movement, to increase the protective factors associated with physical fitness. CFA data analysis enables Guardians to monitor their fitness metrics continuously while providing command teams with real-time insights into individual and unit-level readiness. This capability supports proactive decision-making, early intervention, and resource allocation as part of the broader Holistic Health Approach.

The system should provide the following:

Form Factor Device Requirements:

a. The CFA solution must leverage commercially available off-the-shelf (COTS) form factor devices with minimal configuration to meet CFA objectives.
b. Must include a feature to actively trigger and record physical activities.
c. Must provide sufficient storage to store at least 30 days of data locally on the device.
d. Minimum 10-day battery life under typical use conditions.
e. Must have a minimum 3-year operational lifespan.
f. Must provide customizable form factors or adjustable options to accommodate a wide range of user preferences and comfort needs.
g. Must ensure encryption at the device level.
h. The device must transmit data required for CFA to government-authorized systems or services. Transmission options must include both government-owned systems and personally owned devices (e.g., mobile phones), utilizing only authorized, government-approved platforms and applications.
i. The CFA solution must ensure that components are manufactured exclusively in non-adversary countries, with clear and transparent software provenance. All firmware, chipsets, and related hardware must be digitally signed by a trusted authority to verify authenticity and integrity.
j. The CFA Solution must accurately differentiate between intentional exercise and other physiological responses.
k. The CFA solution must have analytic capabilities to derive (e.g.) Metabolic Equivalent (MET) minutes, Training Impulse (TRIMPS), compliance, trend information.

Mobile Application:

a. The CFA solution must display individual CFA performance and compliance status.
b. Must provide immediate post-workout feedback and verification of assessment integrity.
c. Must enable configurable push notification capabilities to support updates, reminders, and other communications as defined by USSF policy.

d. Must display exemption status directly within the Guardian's mobile app interface, based on determinations made by authorized personnel or systems, to support user awareness and transparency.
e. Must support the capability to deploy configurable user surveys through the mobile app, with content and usage defined by USSF policy**.**
f. Must allow users to view their Fitness Index and compare it across configurable organizational levels, as permitted by policy and user role**.**

Cloud-Based Web Application:

a. The CFA solution must implement role-based access control (RBAC), configurable by system administrators.
b. Must provide role-specific data access and configurable dashboards that allow users (e.g., Admin, Government Resiliency Team (GRT)/Supervisor, Unit Fitness Program Manager (UFPM), Guardian) to monitor, analyze, and report on relevant fitness data based on their assigned permissions.
c. Must include visual compliance indicators viewable at the individual, unit, and organizational levels to quickly identify policy compliance status and support both self-monitoring and leadership oversight.
d. Must display real-time analytics for trend analysis and readiness assessment.
e. Must permit authorized users (e.g., GRTs, UFPMs) to manually input or update fitness performance data, such as Cardiorespiratory Fitness (CRF) and Body Composition (BC), in accordance with USSF policy.
f. Must include visual compliance indicators viewable at the individual, unit, and organizational levels to quickly identify policy compliance status and support both self-monitoring and leadership oversight.
g. Must include a built-in knowledge management solution that provides centralized, role-based access to fitness policy documents, guidance, Frequently Asked Questions (FAQs), and related resources.
h. Must calculate and display the Fitness Index (combined CRF and BC) analysis data at both the individual and unit levels.

Security Measures:

a. The CFA solution must identify a solution architecture planned to be leveraged (e.g. Secure Cloud Computing Architecture (SCCA) Zero Trust Registered Architect (RA), Identity, credential, and access management (ICAM) Platform One, etc.) to demonstrate compliance and interoperability with Government security requirements to include: database resiliency; Authority to Operate (ATO) at a minimum of Impact Level 5 (IL5), or at a minimum IL4 with a security overlay that meets IL5-equivalent protections; additional cloud hosted firewall protections; non-specific cloud service provider architecture; and retains obfuscation elements such as personally identifiable information (PII).
b. The system's architecture must prevent the passive or automatic collection of activity data without explicit user action.
c. Data must be encrypted both at rest and in transit in accordance with National Institute of Standards & Technology (NIST) Special Publication (SP) 800-53 security controls (e.g., SC-12, SC-28, SC-12(2)), using cryptographic methods validated under Federal Information

Processing Standards (FIPS) 140-3 to protect controlled unclassified information (CUI), PII, and other designated data types.

d. Data loss GPS prevention and secure data handling practices must be implemented.
e. Form factor devices must comply with the National Security Agency (NSA) security guidance: no embedded WiFi, no Long-Term Evolution (LTE), no modifiable memory.
f. Bluetooth connections must be secured using encryption and authentication protocols, as recommended by NIST SP 800-121, *Guide to Bluetooth Security*.
g. The government-approved or created app must undergo rigorous security testing and validation to ensure it meets all cybersecurity standards, as per DoDI 8500.01.
h. The IL5 government cloud must comply with Federal Risk and Authorization Management Program (FedRAMP) and DoD Cloud Computing Security Requirements Guide (SRG).
i. Data must be encrypted during transmission and storage in the cloud to ensure confidentiality and integrity.
j. Must provide helpdesk services for system troubleshooting and communications, FAQs, policy summaries, and contact information.
k. Must provide secure, standards-based Application Programming Interface (API) integration to export relevant fitness data to designated readiness systems (e.g., Log in Portal: myFSS), enterprise data lakes, in accordance with USSF data governance policies.
l. Must integrate with the USSF enterprise data layer, either natively or through adaptable interfaces that support interoperability and data standardization.
m. Must digitally represent USSF fitness policy standards and enable automated flagging of compliance to include identification of performance trends or other fitness indicators.
n. Must include functionality for updating medical or duty-based exemptions.
o. Must allow authorized personnel to pause or exempt Guardians from CFA enforcement.
p. Must enable user administrators (UFPM and GRT roles) to manage rosters, assign Guardians to units, and update biodemographic information.
q. Must implement a mechanism to periodically validate Guardian assignment and biodemographic information to ensure roster accuracy, with the frequency and method defined by USSF policy.
r. Must maintain historical CFA data tied to individual Guardians and organizational echelons, in accordance with applicable USSF data retention policies and cybersecurity standards.
s. The system must be accessible on both government-issued and personal mobile devices, either through a secure mobile application or a mobile-optimized web interface.

CFA Required Metrics:

a. Cardiorespiratory Fitness (CRF)
   The CFA Solution must approximate VO2 max within an acceptable margin of error:
   1. Mean Absolute Percent Error (MAPE) < 5%
   2. Mean Absolute Error (MAE) ≈ 4 points compared to metabolic cart standard
   3. Must be reliable and sensitive to changes over time (both improvement and decline).
   4. Support multiple measurement methods, including method that can be accomplished indoors on stationary equipment.
b. Exercise Volume & Intensity
   The PWFD primary means **o**f measuring exercise volume and intensity will be Heart rate (HR)-based monitoring.
   1. HR MAPE must be < 2% during ambulatory activities.
   2. Customizable HR thresholds for users with relevant conditions or medications.

3. Support for passive (daily living) and active (workout) monitoring.
4. Verifiable against gold standard measures (e.g., METS).
5. If using proprietary algorithms, outputs must be auditable and accurate against laboratory benchmarks.
6. The PWFD should express CRF in the accepted scientific metric – $VO_{2\ max}$, or the maximum volume of oxygen that can be consumed and used for energy. $VO_{2\ max}$ is expressed as ml of O_2, per minute, per kg of body mass – or ml/min/kg.

c. Muscular Strength & Endurance
   1. The CFA solution must support Guardian self-assessments without supervision.
   2. Must include automatic repetition counting to standard (to failure).
   3. Have maximum counting error: ±2 reps per assessment.
   4. Exercises must be bodyweight-only, with no equipment required.

d. Fitness Index
   1. Must be computed as a composite of CRF and BC data.
   2. Must be accessible in both the web and mobile applications for individuals and units.
   3. Must serve as the primary readiness metric across the force.

Form Factor Software Development Kit (SDK)**:**

a. The CFA solution must collect device configuration data and support enterprise-wide firmware updates.
b. The CFA solution must include access to sensor data needed to compute fitness metrics.
c. The CFA solution must perform edge-based analytics to derive metrics such as CRF, exercise volume/intensity, and muscular endurance.

Cybersecurity Compliance:

a. Compliance Standards
   1. Cybersecurity compliance must be maintained throughout the lifecycle of the solution, including adherence to any updated or superseding DoDIs and standards.
   2. The system must comply with DoDI 8500.01, *Cybersecurity* and DoDI 8510.01, *Risk Management Framework for DoD Systems*.
   3. The system must follow NIST SP 800-53 *Security and Privacy Controls for Information Systems and Organizations* guidelines.
   4. The solution must be hosted within a DoD-approved cloud environment (e.g., Cloud One, Joint Warfighting Cloud Capability (JWCC)) that meets the applicable requirements outlined in the DoD Cloud Computing Security Requirements Guide (SRG).

b. Access Controls
   1. The CFA system must implement robust access control measures, including authentication and authorization, consistent with NIST SP 800-53 guidelines.
   2. The solution must provide a manual, user-initiated mechanism for recording activities. The manual mechanism must be a physical button or switch integrated into the COTS hardware device. The design of the physical button or switch shall incorporate features to prevent accidental activation during typical use. Examples include but are not limited to:
      a. Recessed or shielded button/switch housing to protect against inadvertent contact

b. A deliberate confirmation sequence for activation and deactivation, such as a "Press-and-hold" for a minimum of 3 seconds or a rapid "double-press".
c. Tactile and audible or haptic feedback to confirm successful activation or deactivation to the user. The functionality governing the physical button or switch must be embedded in the device's firmware and shall not be by passable or modifiable by external applications or phones.

3. System performance auditing mechanisms must be in place to track access-related events in alignment with applicable access controls and data logs.
4. Multi-factor authentication (MFA) must be enforced for all administrative access and user login portals. Access permissions must be role-based and follow the principle of least privilege, ensuring users are granted only the minimum access necessary for their role.
5. An incident response plan must be established, including detection, reporting, and recovery procedures, in alignment with *Cybersecurity Activities Support Procedures (*DOD Manual 8530.01, para 3.6) and DoD's Cyber Incident Response (DoDI 8530.03).

c. Device Management
1. A device management solution must be implemented to securely manage Bluetooth-enabled health and workout devices, ensuring proper configuration, updates, and policy compliance in alignment with NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*.
2. The solution must provide capabilities for remote monitoring, troubleshooting, and enforcement of security settings, , consistent with mobile device management best practices and aligned with the risk mitigation principles outlined in NIST SP 800-124, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*.

d. Audit and Monitoring
1. The CFA solution must support capabilities for audit logging, event monitoring, and data retention necessary to enable compliance verification with applicable security and privacy requirements per NIST SP 800-53 (e.g., AU-1 through 6, CA-7, SI-4) and DODI 8510.01.
2. The CFA solution must support detection, alerting, and reporting capabilities to enable timely identification and response to anomalies and security incidents by authorized personnel.

Data Privacy and Security:

a. Guardian Data
1. The CFA solution must provide multi-level security to meet Guardian needs and provide security for data at rest as well as data in transit.
2. The CFA solution must measure, and practices must be put in place to protect against unauthorized access, disclosure, alteration, or destruction.
3. The CFA solution must secure access to potential Personally Identifiable Information (PII)/Personal Health Information (PHI) and must be controlled at the database level.
4. CFA management must safeguard sensitive information and prevent data breaches, unauthorized data access, and data loss.
5. The CFA solution must comply with DoD Cloud Computing SRG and deliver a tested and validated PWFD utilizing commercial fitness form factor combined with secured Government-owned data platforms and analytics.

b. System Data

1. The CFA solution must integrate configuration management capabilities that support remote account disablement, sync control, and policy enforcement through a DoD-compliant mobile device management (MDM) solution, aligned with NIST SP 800-124, *Guidelines for Managing the Security of Mobile Devices in the Enterprise* and applicable Zero Trust architecture guidance.
2. The CFA solution must protect Global Positioning Satellite (GPS) and other sensitive data using robust encryption or equivalent security measures to ensure secure transmission from the form factor device to authorized government applications aligned IAW FIPS 140-3*, Security Requirements for Cryptographic Modules* validated encryption and restricting data transmission to approved endpoints.
3. The CFA solution must support Geofencing and Internet Protocol (IP) filtering to enable USSF ability to limit locations of form factor functionality.
4. The CFA solution must include a user-configurable option to disable GPS tracking when operationally permissible, without impacting the device's ability to perform core CFA functions or meet data integrity requirements.
5. The CFA solution must implement safeguards to prevent users from modifying or accessing unauthorized components of the form factor's software, firmware, or broader device ecosystem.
6. The CFA solution must enable USSF to remotely manage and enforce settings, features, and access controls on the selected form factor, ensuring centralized policy enforcement and configuration control.
7. The CFA solution must ensure solution components align with applicable Zero Trust pillars (e.g., Identity, Device, Data), and include mechanisms for testable and auditable enforcement of associated security controls, in accordance with DoD Zero Trust architecture guidance.
8. The CFA solution must Implement secure supply chain risk management practices in accordance with NIST SP 800-161, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* and DoD guidance, including verified sourcing, timely delivery of security updates, and validation of software and hardware components through approved government or commercial marketplaces.

Phase I	**Accepted Until**
Phase I PowerPoint and White Paper	12:00 pm MT on 5 December 2025

Contracting Team Points of Contact	SSC.OTTI.CSO@spaceforce.mil