

CALL FOR SOLUTIONS (CfS)

Enterprise-wide OT/ICS/FRCS Modernization and Integration Prototype 1.0

Project Number	ICED-603
US Army Open Solicitation (AOS) Number	W9128Z-25-S-A002
Call for Solution Title	Enterprise-wide OT/ICS/FRCS Modernization and Integration Prototype 1.0 (ICED-603)
Issued By	Army Contracting Command – Aberdeen Proving Ground (ACC-APG), Huachuca Division, Alpha Branch, on behalf of the U.S. Army Information Systems Engineering Command (USAISEC)
Submission Instructions	To respond to this Call for Solutions, please refer to Section 6.0 and Section 7.0 of this document.
Solution Briefs (White Paper Submission) Due Date/Time (Suspense)	September 1, 2026, at 1200 hours Eastern Daylight Time (EDT)
Agreements Officer (Point of Contact)	Karen E. Billick karen.e.billick.civ@army.mil
Agreements Specialist (Point of Contact)	Craig A. Metzger craig.a.metzger4.civ@army.mil

NOTE: Please advise the cognizant Agreements Officer and Agreements Specialist via email as soon as possible if your organization intends to submit a Solution Brief in response to this Call for Solutions.

Submissions are to be sent via email only to the Agreements Officer and Specialist listed in this Call for Solution.

**Any submissions received by the Agreements Officer after the suspense date/time listed above will be deemed late and will not be evaluated. It is the sole responsibility of the responding company to ensure its submission is successfully received in the designated email inboxes before the specified deadline.*

Questions and Responses are to be sent only to the Contracting Officer and Specialist listed in this Call for Solution. The following shall be utilized in the email subject line **"Call for Solution - [Your Company Name] – ICED_603" (Example: Call for Solution - ABC Corp ICED_603)**. Material questions and answers will be published and updated on www.sam.gov. The deadline to submit questions for Phase 1 is **19 August 2026 at 1500 EDT**.

AUTHORITY AND REGULATORY APPLICABILITY

This Call for Solutions (CfS) is issued under the authority of Revolutionary Federal Acquisition Regulation Overhaul (RFO) and in accordance with the Army Open Solicitation procedures detailed within Solicitation W9128Z-25-S-A002.

This Call for Solution is issued under the authority of Defense Federal Acquisition Regulation Supplement (DFARS) 212.70 – Defense Commercial Solutions Opening and may result in the Government awarding Federal Acquisition Regulation (FAR) contracts or non-FAR agreements. Other Transactions (OT) that may be awarded from this Call for Solution are not subject to the FAR or its supplements, as applicable.

1.0 BACKGROUND

U.S. Army Information Systems Engineering Command, on behalf of the Army Materiel Command (AMC), is seeking innovative, commercially available, or rapidly adaptable technology solutions to modernize and integrate its vast Operational Technology (OT), Industrial Control Systems (ICS), and Facility-Related Control Systems (FRCS) enterprise.

Threats to interdependent power grids, water resources, and control systems jeopardize critical military capabilities and power projection. To address these

systemic risks, the Army must rapidly modernize its OT/ICS/FRCS infrastructure, ensure it is cyber-resilient, and integrate disparate systems.

Achieving this readiness posture requires a pragmatic, execution-oriented "Break/Fix/Repair" (BFR) and replacement strategy. Rather than executing a costly and disruptive wholesale "rip-and-replace" of operational assets, this initiative focuses on deploying modern, software-defined or physical engineering fixes directly onto outdated, unsupported, or obsolete legacy systems, transforming legacy vulnerabilities into hardened, compliant operational endpoints.

2.0 PROBLEM STATEMENT

The Army faces a critical operational challenge in maintaining visibility, security, and control over its extensive and diverse portfolio of OT, ICS, and FRCS across Continental United States (CONUS) and Outside CONUS (OCONUS) installations. This technology, which includes manufacturing, utility, energy, water, and life-safety controls, is foundational to installation resilience and mission readiness.

The current operational environment is characterized by a wide variety of disparate, aging, and vendor-proprietary systems that lack interoperability, are vulnerable to cyber threats, and do not provide the enterprise-level data required for effective management and strategic decision-making.

To overcome these deficiencies, the Army requires a demonstrated, repeatable, and scalable prototype capability to securely engineer, integrate, harden, and sustain existing systems, establishing a modern, secure, vendor-agnostic, and scalable approach for these critical operational assets.

3.0 DESIRED PROTOTYPE CAPABILITIES

Offerors are invited to propose innovative solutions that address the following core capability areas. Proposers must demonstrate their commercial readiness and ability to execute these performance objectives ~~during a physical, live-site demonstration phase.~~

Capability Area	Performance Objective
Unified Control System Integration	Demonstrate the ability to engineer, install, integrate, secure, and sustain a wide array of OT/ICS/FRCS equipment (e.g., SCADA, Direct Digital Control (DDC), Building Automation Systems

	(BAS), and various utility devices/sensors). The solution must be vendor-agnostic (where able), breaking the reliance on proprietary systems.
Telemetry & Data Integration Remediation	Demonstrate the capability to securely integrate, remediate, and normalize telemetry pathways from existing, legacy, and disparate distributed edge data points. The desired outcome is the continuous transmission of secure data to authorized repositories for real-time management, reporting, and analytics.
Cybersecurity & Resilience	Demonstrate a full-lifecycle approach to cyber resilience for Operational Technology (OT). This includes remediating, hardening, and sustaining secure system baselines for legacy devices, performing security assessments, vulnerability management, and supporting the Risk Management Framework (RMF) accreditation process. When identified and authorized by the Government, identity-based microsegmentation and zero-trust perimeter isolation shall be implemented.
Supply Chain Risk Management (SCRM) & Sourcing Compliance	Demonstrate a structured supply chain risk management approach to ensure all components, hardware, software, and firmware are compliant with NDAA Section 889, NDAA Section 5949, and contain zero components or services originating from Covered Foreign Countries or entities listed on the DoD 1260H List, and other applicable laws.
Security Pre-Requisites & Controlled Unclassified Information (CUI) Protection	Prior to receiving site discrepancy data (classified as CUI), the vendor shall demonstrate compliance with Cybersecurity Maturity Model Certification (CMMC) 2.0 Level 2 or

	possess a verifiable, active Supplier Performance Risk System (SPRS) score meeting Department of the Army Chief Information Officer (CIO) thresholds, ensuring secure handling of all Government-furnished targeting and vulnerability details.
Adaptive Engineering & Variance Management	Demonstrate a structured, rapid-response capability to identify, analyze, and manage physical or logical deviations in the event that discrepancies are encountered between Government-furnished information and the operational environment.
Phase 2: Demonstrate Technical Courses of Actions	After an initial down-select, selected offerors shall demonstrate their solution's capabilities by submitting Technical Courses of Action (COAs). These COAs shall be presented to the Government's technical representative as a decision package, detailing the technical approach, security/RMF posture, schedule impact, and cost-benefit analysis for 2 sample locations. The primary task for this demonstration is to evaluate the offeror's technical and engineering capability to plan, implement, and validate Break/Fix/Repair (BFR) remediation on OT/ICS/FRCS systems, resolving pre-identified physical and cybersecurity discrepancies. Offerors shall prove their engineering and integration competency through the development and written submission of these simulated remediation packages in lieu of physical execution on live networks. For more details see ICED-603_OTA Demonstrated Value ATT 1 and the Government sample locations

	information (to be provided to down-selected offerors).
--	---

4.0 AWARDING INSTRUMENT

The Call will be awarded in accordance with the Army Open Solicitation procedures detailed within Solicitation W9128Z-25-S-A002, found here:

<https://sam.gov/workspace/contract/opp/239ec285981a42ba9aa63258ccfb4407/view>.

This Call provides instructions to companies and how the Government will evaluate submissions.

5.0 SUBMISSION PHASES AND ACCELERATED "SPRINT TO AWARD" TIMELINE

To support the critical obligation of expiring fiscal year funding, this source selection is being conducted on an accelerated **40-day schedule**. This timeline is a material requirement of this solicitation. Vendor submissions must strictly adhere to all specified deadlines. The Government reserves the right to disqualify any offeror who fails to meet the required suspense dates.

Companies are reminded that all awards are subject to the availability of funds and the Government reserves the right to make multiple awards, a single award, or no award as a result of this Call.

Only a Contracting Officer has the authority to enter into, modify, or execute a binding instrument on behalf of the United States Government. All payment obligations are subject to Congressional appropriations.

In order to be eligible for award, companies must:

- Possess a Unique Entity ID (UEI) and be registered in the System for Award Management (SAM) prior to award and maintain active registration throughout the period of performance.
- Register in the prescribed government invoicing system (e.g., Wide Area Workflow).
- Accurately represent their small business size and status as required.
- Be determined responsible by the Contracting/Agreements Officer and not be suspended, debarred, or otherwise prohibited from receiving an award.
- Disclose any actual or potential Organizational Conflicts of Interest (OCIs) to the Contracting/Agreements Officer prior to award.

- Companies are responsible for monitoring SAM.gov for any amendments or updates to this Call.

Notice to Company(s): The Government reserves the right to cancel this open Call, either before or after the closing date. If the Government cancels this open Call, the Government has no obligation to reimburse an company for any costs.

All Solution Submissions will be valid for 180 calendar days after the submission date.

The Government will give preference to submissions that demonstrate an innovative, existing, and reference-verifiable commercial ability to accomplish the desired solution attributes listed for each capability need.

Resellers and academic research proposals are not desired.

The Government reserves the right to go directly from this Call for Solution to award.

The Government reserves the right to award more than one (1) award resulting from this Call for Solution or to make no award.

5.1 Overview of Submission Phases

- **Phase 1: Solution Brief (White Paper Submission):** Offerors submit a high-level summary of their proposed technology solution, organizational viability, and compliance matrices.
- **Phase 2: Demonstrate Technical Courses of Actions:** Down-selected offerors who pass the mandatory pre-requisite gates will be provided Government-Furnished Information (GFI) detailing physical and cybersecurity discrepancies for 2 standardized sample locations. Offerors shall demonstrate their technical capabilities by submitting a written Technical Courses of Action (COAs) package. The package shall detail propose technical implementation approach, security/RMF hardening posture, schedule impact, and cost-benefit analysis. No oral presentations or physical field deployments are required.
- **Phase 3: Prototype Proposal & Negotiations:** The highest-rated offeror from the Phase 2 demonstration will be invited to submit a detailed cost proposal and finalize the Model Agreement.

5.2 Accelerated Program Milestones

Milestone / Phase	Duration (in Business Days)	Target Completion Date	Description
1. Phase 1: Solution Brief (White Paper) & Gate 1 Screen	15 Days	September 1, 2026	CfS Release; 15-day response window. Immediate Pass/Fail screening on CMMC/SPRS/SCRM compliance upon receipt of Solution Briefs.
2. Phase 1 Down-Select	3 Days	September 4, 2026	Board evaluates written Solution Briefs using the qualitative factor rubric. Down-select to top 2-3 high-performing vendors.
3. GFI Transmittal	1 Days	September 4, 2026	Transmit CUI Site Discrepancy Reports (GFI) to down-selected vendors.
4. Phase 2 Sample Site	10 Days	September 14, 2026	10day response window.
5. Final Evaluation & Selection	4 Days	September 18, 2026	Phase 2 submissions will be evaluated. The Source Selection Authority (SSA) reviews and signs the Selection Memo.
6. Negotiations & Award	7 5 Days	September 25, 2026	Finalize Model Agreement, complete legal review, and formally obligate FY funds for the prototype OTA.

6.0 SOLUTION BRIEF SUBMISSION REQUIREMENTS (PHASE 1)

Offerors must submit their Phase 1 package via email to the Agreements Officer and Specialist listed in the header block no later than **September 1, 2026** ~~August 27, 2026~~ at 1200 EDT. The email subject line must strictly read: *Call for Solution - [Your Company Name] - ICED 603*.

6.1 Solution Brief Page and Formatting Constraints

- **Format:** Microsoft Word (.docx) file. Cost and Total Cost of Ownership (TCO) estimates must be provided in Microsoft Excel (.xlsx).
- **Length:** The Technical Discussion section must not exceed **twenty (20) pages**. Title pages, table of contents, and disclosures do not count against this limit. The Government will only evaluate the first **twenty** ~~ten~~ pages of any technical discussion; content beyond page **20** ~~10~~ will be discarded. Diagrams / figures are excluded from the page count.
- **Font & Margins:** Standard Arial or Times New Roman 11pt or 12pt font with 1-inch margins on all sides.

6.2 Solution Brief Content Structure

At a minimum, the Phase 1 Solution Brief must include the following sections:

1. **Title Page (Non-counting):** Company Name, Proposal Title, Date, POC details, SAM.gov Unique Entity ID (UEI), CAGE Code, and the specific solicitation reference number.
2. **Executive Summary (One Page Max):** High-level summary of the proposed OT/ICS/FRCs modernization and remediation concept.
3. **High-Level Technology Solution/Concept:**
 - Detail how the proposed solution satisfies the Desired Capabilities outlined in Section 3.0.
 - Explain how the proposed technical approach is feasible, secure, and achievable utilizing modern best practices.
 - Explain how the proposed technical approach is supported by a technical team with the documented expertise and experience to accomplish the proposed solution/concept.
 - Outline the technical capabilities, interoperability, and global scalability of the proposed solution/concept across diverse AMC environments.
 - Detail how the proposed solution is vendor-agnostic where able and integrates with legacy field protocols (e.g., Modbus, BACnet) while minimizing unnecessary physical hardware replacements ("rip-and-replace").
 - Detail the offeror's **Variance and COA Management Plan**, by outlining a structured process to identify, analyze, and document physical or logical deviations, in the event that discrepancies are encountered between Government-furnished information and the

operational environment, and describe how these will be submitted in writing as decision packages to the Government.

- Describe the derived operational, sustainment, and security benefits of the proposed solution/concept as it applies to this Call for Solution.

4. **Company Viability:** Provide a brief financial and operational overview of the company, including current commercial footprint and capability to execute rapid, multi-site deployments.

Provide a summary of any proposed product/solution's commercialization and sustainment lifecycle.

5. **Intellectual Property Statement/Disclosures (Non-counting):**

Explicitly identify proprietary software, firmware, and hardware involved in the prototype, including any associated licensing restrictions or data rights limitations proposed for Government use.

6. **Technical Data & Software Rights Requirements (Non-counting):**

Offerors must submit an Intellectual Property (IP) and Data Rights Assertion Table identifying all technical data and computer software to be delivered with restrictions. The Government requires, at a minimum, **Government Purpose Rights (GPR)** for all newly developed software code, custom configurations, variance courses of action, and integration interfaces created under this prototype OTA, enabling the Army to replicate, modify, and sustain the prototype across the global AMC enterprise. Specifically, assertions must be structured in accordance with the following table:

Technical Data/Software to be Delivered	Basis for Assertion	Asserted Rights Category	Name of Person Asserting Restrictions
<i>[List item, e.g., Custom Modbus-to-BACnet translator]</i>	<i>[e.g., Developed exclusively at private expense]</i>	<i>[e.g., Restricted Rights / Government Purpose Rights]</i>	<i>[Name of Company/POC]</i>

Phase 2 Demonstrate Technical Courses of Actions

6.3 Technical Courses of Actions Page and Formatting Constraints

- **Format:** Microsoft Word (.docx) file. Cost and Total Cost of Ownership (TCO) estimates must be provided in Microsoft Excel (.xlsx).
- **Length:** The Technical Discussion section must not exceed **twenty (20) pages**. Title pages, table of contents, and disclosures do not count against this limit. The Government will only evaluate the first **twenty** ~~ten~~ pages of any technical discussion; content beyond page **20** ~~10~~ will be discarded. Diagrams / figures are excluded for the page count.
- **Font & Margins:** Standard Arial or Times New Roman 11pt or 12pt font with 1-inch margins on all sides.

6.4 Technical Courses of Actions Structure

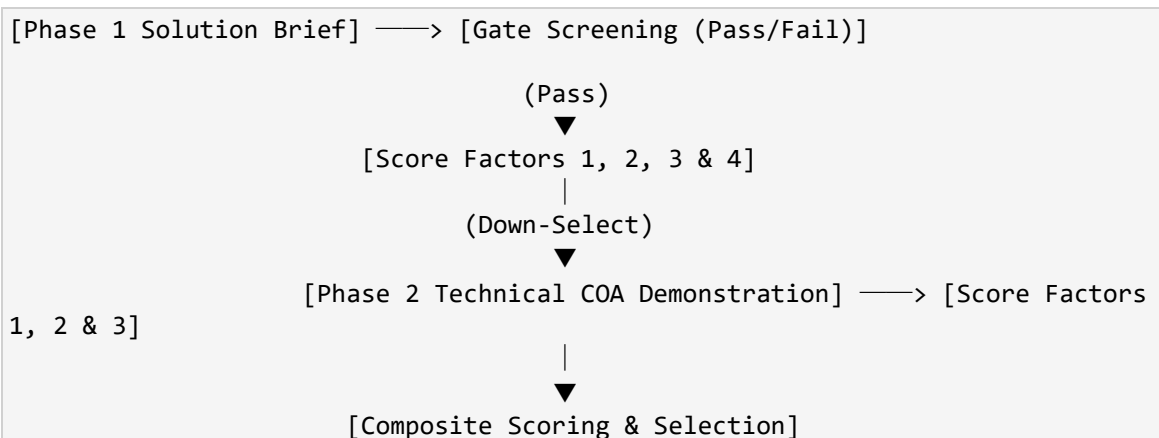
At a minimum, the Phase 2 Demonstrate Technical Courses of Actions must include the following sections:

1. **Title Page (Non-counting):** Company Name, Proposal Title, Date, POC details, SAM.gov Unique Entity ID (UEI), CAGE Code, and the specific solicitation reference number.
2. **Executive Summary (One Page Max):** High-level summary of the proposed OT/ICS/FRCS modernization concept.
3. **Technical Courses of Actions:**
 - Detail how the proposed solution satisfies the Desired Capabilities outlined in Section 3.0 per sample site.
 - Explain how the proposed technical approach is feasible, secure, achievable and utilizes modern best practices per sample site.
 - Explain how the proposed technical approach is supported by a technical team with the documented expertise and experience to accomplish the proposed solution/concept per sample site.
 - Outline the technical capabilities, interoperability, and scalability of the proposed COAs.
4. **Attachment 1 - Notional Schedule:** A proposed milestone schedule demonstrating initial operational capability (IOC) and full deployment of the prototype.
5. **Attachment 2 - Technical Architecture Diagrams (if applicable):** Logical and physical diagrams detailing the telemetry, any microsegmentation, and boundary security mechanisms for their proposed COAs.

6. **Attachment 3 - Total Cost of Ownership (TCO):** The Offeror shall provide an estimate of the Government's total cost of ownership (TCO) for the proposed solution over the next five (5) fiscal years. The estimate should provide a breakdown of cost categories, detailing licensing, software, hardware, recurring maintenance costs and their basis of estimate. Offerors who propose a cost-sharing agreement for the prototype should indicate that in their basis of estimate. The TCO estimate shall be submitted as a Microsoft Excel file (xlsx).

7.0 EVALUATION PROCESS & CRITERIA

The Government will execute a rigorous, multi-stage evaluation process to identify the solution providing the best overall value to the Army.



7.1 Gate Screening (Non-Scored, Pass/Fail Pre-requisites)

Upon receipt, all submissions will be vetted against the following mandatory gates. A rating of **Fail** on any single gate will result in immediate disqualification and removal from further consideration.

- **Gate A Submission formatting and completeness (Phase 1 and 2):**

Pass: The Solution Brief (White Paper) is submitted as a Microsoft Word file (.docx) and the TCO is submitted as a Microsoft Excel file (.xlsx) with active formulas intact. The Solutions Brief utilizes Arial or Times New Roman 11pt or 12pt font with 1-inch margins (headers and footers may be outside margins). The Solutions Brief does not exceed the twenty (20) page limit excluding diagrams. The submission includes clear, comprehensive details that support an initial compliance review with all required criteria (section 2 and 3); no essential elements are missing or unclear.

Fail: The Solutions Brief exceeds the twenty (20) page limit. The submission is not provided in the specified file format or does not adhere to the required font and margin specifications. The submission is missing detail or clarity to determine compliance with basic mandatory requirements; key elements are missing, incomplete, or ambiguous.

- **Gate B: CMMC 2.0 / SPRS Compliance (Phase 1):**

Pass: The offeror provides verifiable proof of Cybersecurity Maturity Model Certification (CMMC) 2.0 Level 2 (or higher) or an active, verified score registered in the Supplier Performance Risk System (SPRS) meeting the minimum threshold defined by the DoD Chief Information Officer (CIO) for secure handling of Controlled Unclassified Information (CUI). This information shall be submitted as part of the Phase 1 submission

Fail: Failure to provide verifiable proof of compliance or possessing an active score below the DoD CIO threshold.

- **Gate C: Prohibited Sourcing Compliance (Phase 1):**

Pass: The offeror certifies that all proposed hardware, software, and firmware components are free from prohibited foreign sources as defined by NDAA Section 889, NDAA Section 5949, and the DoD 1260H List. This information shall be submitted as part of the Phase 1 submission.

Fail: Failure to certify compliance, or identification of any covered foreign technology in the proposed Bill of Materials (BOM).

7.2 Scored Qualitative Evaluation Factors

Proposals passing the initial Gate Screening will be evaluated on the following four (4) factors. The final selection will be based on a single, combined score derived from ~~the written proposal~~ Phase 1 Solution Brief and ~~the live-site demonstration performance~~ Phase 2 Demonstrate Technical Courses of Actions.

Evaluation Factor	Weight	Evaluation Method
Factor 1: Successful Discrepancy Resolution & Cybersecurity Posture	45%	Written Proposal (Phase 1 & 2)

Factor 2: Interoperability & Backwards Compatibility	30%	Written Proposal (Phase 1 & 2)
Factor 3: Logistical Viability & SCRM	15%	Written Proposal & Sourcing Analysis (Phase 1 & 2)
Factor 4: Adaptive Engineering (Variance & COA)	10%	Written Proposal (Phase 1)
Total Weighted Score	100%	

7.3 Factor Descriptions:

Factor 1: Successful Discrepancy Resolution & Cybersecurity Posture (45%):

Evaluates the offeror's ability to successfully and securely execute BFR tasks. Evaluation assesses the completeness of the physical remediation, the technical soundness of the implemented fix, and the resulting security baseline (compliance with DISA STIGs and Army security directives).

Factor 2: Interoperability & Backwards Compatibility (30%): Evaluates the capability to integrate with existing legacy OT/ICS/FRCS infrastructure. Evaluators will assess compatibility with legacy protocols (Modbus, BACnet, LonWorks) and the degree to which the solution minimizes physical hardware replacement.

Factor 3: Logistical Viability & SCRM (15%): Evaluates the risk associated with the proposed supply chain. Evaluators assess the documented Bill of Materials (BOM) sourcing strategy, lead times, component authenticity, and mitigation plans for hardware obsolescence.

Factor 4: Adaptive Engineering (10%): Evaluates the offeror's structured risk-management and Course of Action (COA) generation methodology. This is evaluated **solely on the written white paper proposal** (specifically the Variance and COA Management Plan section) to maintain a standardized, fair playing field under the compressed 40-day timeline.

7.4 Rating Scale and Scoring Rubric

Evaluators will utilize the following 10-point scale to assign raw scores for each of the qualitative factors:

Rating	Score Range	Definition
Exceptional	9.0 - 10.0	The proposed solution is exceptionally strong and comprehensively exceeds all requirements, offering significant and highly advantageous benefits, substantial innovation, and a superior solution that presents minimal risk and maximum value for the Army in this specific criterion.
Good	7.0 - 8.9	The proposed solution meets all requirements and includes enhancements or added value in one or more areas, demonstrating clear strengths, innovative elements, or distinct advantages that provide noticeable benefits or reduced risk for this specific criterion.
Acceptable	5.0 - 6.9	The proposed solution fully meets all required criteria but does so only at a basic level. It presents a sound, competent solution for this specific criterion.
Marginal	1.0 - 4.9	The proposed solution provides a barely acceptable response, presents notable weaknesses or risks, or requires substantial clarification and/or improvement to meet the expected quality or performance for this specific criterion.
Unacceptable	0.0	The proposed solution for this specific criterion is significantly flawed, poses high risk, or fails to address critical aspects of the requirement, indicating a fundamental lack of understanding or capability despite passing the initial gate screen.

7.5 Final Score Calculation Methodology:

The composite score is calculated by multiplying the raw score assigned by the evaluation board for each factor by the factor's assigned weight, and summing the results to produce a final composite score out of 10.00 (equating directly to a percentage out of 100%).

$$\text{Composite Score} = \sum(\text{Raw Score} \times \text{Factor Weight})$$

Scoring Example (Vendor X):

If Vendor X passes all mandatory Go/No-Go Gates and completes the evaluation phases with the following raw scores:

Factor 1: 8.0 (Good)

Factor 2: 7.0 (Good)

Factor 3: 6.0 (Acceptable)

Factor 4: 9.0 (Exceptional)

The composite calculation is:

Evaluation Factor	Raw Score (A)	Factor Weight (B)	Weighted Score (A × B)
Factor 1: Discrepancy Resolution	8.0	45% (0.45)	3.60
Factor 2: Interoperability	7.0	30% (0.30)	2.10
Factor 3: Logistical Viability & SCRM	6.0	15% (0.15)	0.90
Factor 4: Adaptive Engineering	9.0	10% (0.10)	0.90
Final Composite Score	N/A	100%	7.50 / 10.00 (75.0%)

Conclusion: Vendor X receives an overall composite score of **7.50 out of 10.00 (75.0%)**, resulting in an overall qualitative rating of **Good**.

8.0 ITERATIVE PROTOTYPING

In accordance with AOS, Section F, iterative prototyping will be conducted in multiple phases, with each phase building upon the outcomes of the previous one. At

the end of each phase, the Government and stakeholders will review deliverables and provide feedback, which will be incorporated into subsequent iterations. The scope of the prototype may be modified by mutual agreement to adapt the technology for additional unique and discrete purposes or mission sets, which may be identified by the Government during the prototyping process. Progress will be evaluated against predefined milestones and deliverables, and adjustments will be made as necessary to ensure continued alignment with project objectives and requirements. The iterative prototyping process may result in separate phased prototype awards or modifications to the original award, as appropriate, and will continue until all milestones to completion have been achieved to the satisfaction of the Government

9.0 SUCCESSFUL COMPLETION OF PROTOTYPE

In accordance with AOS, Section G, successful completion of the prototype will be determined by the Government, through written determination by the appropriate approving official, based on the achievement of all agreed-upon deliverables, performance metrics, and acceptance criteria as outlined in the prototype agreement. The Government will conduct a final evaluation to confirm that all requirements have been met prior to considering any follow-on production activities. The Government may also, prior to full completion, transition any complete and substantive aspect of the prototype determined to provide utility into production, as appropriate.

10.0 FOLLOW-ON PRODUCTION

In accordance with AOS, Section H – Follow-On Production of a Prototype, and pursuant to 10 U.S.C. 4022, companies are advised that any prototype awarded in response to this Call may result in the award of a follow-on production contract or agreement without the use of further competitive procedures, contingent upon successful completion of the prototype and determination by the Government. The follow-on production contract or agreement may be available for use by one or more organization(s) within the Department of Defense (DoD), and the scope and magnitude of the follow-on award could be significantly larger than that of the prototype effort.

11.0 NON-GOVERNMENT ADVISORS

In accordance with AOS, Section I the Government will use non-Government advisors from the following contractors with the contact information provided:

CONTRACTOR NAME: The MITRE Corporation.

INSERT CONTRACTOR ADDRESS: 6000 Redstone Gateway SW, Huntsville, AL 35808

INSERT CONTRACTOR POC NAME: Ken Butler

INSERT CONTRACTOR POC PHONE NUMBER: 256-890-3343

INSERT CONTRACTOR EMAIL: kenneth.f.butler3.ctr@army.mil

As a reminder, by submitting information to the Government, the Company further understands that it had an opportunity to enter into a NDA directly with the Non-Government Advisor and therefore waives any and all claims against the Government for any disclosures of proprietary information by the non-Government personnel. Such NDAs are the responsibility of the Company, and the Government shall not be a party to them. Companies shall provide a copy of the signed NDAs to the Government with submissions

12. ORGANIZATIONAL CONFLICT OF INTEREST (OCI)

The Offeror shall perform an OCI analysis and submit the results of that analysis in addition to the Solution Brief submission. Specifically, the Offeror shall analyze the details of the Call and the implementation of their proposed Solution for actual or potential OCI situations associated with the performance of the Offeror, or any of the Offeror's proposed teammates or subcontractors, under any contract or agreement the Offeror or the Offeror's teammates or subcontractors have 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. The level of detail for OCI analysis may not be the same for all vendors. FAR 9.5 may be used as guidance for OCI analysis. If no conflicts are identified, a risk mitigation plan is not required; however a description of the analysis methodology, and an affirming statement that no conflicts are identified shall be included. This section will not count against submission page limits.

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.

OCI information shall be submitted with Phase 1 as an Appendix and does not count in the twenty pages limit.