Engineer Research and Development Center

Information Technology Laboratory
Commercial Solutions Openings (CSO)
Solicitation Number: W912HZ26SC006

SECTION A: INTRODUCTION

The Engineer Research and Development Center (ERDC), Information Technology Laboratory (ITL) is issuing a Commercial Solutions Opening (CSO) pursuant to 10 U.S.C. 3458 as implemented by RFO DFARS 212.7000. Under a CSO, the ERDC may competitively select proposals received in response to a general solicitation, similar to a Broad Agency Announcement (BAA), based on a review of proposal by scientific, technological, or other subject matter expert peers within the ERDC and/or other federal experts. This CSO will be used to acquire innovative products, services, or technologies, and under this CSO, all products, services, and technologies 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 DFARS regulation, the solution is treated as commercial whereby the Contracting Officer will utilize commercial procedures to develop and execute the resultant award.

This CSO contains broadly defined Areas of Interest (AOIs) that describe aspects of the ERDC mission, however more specific individual program requirements (IPRs) may be added in the future. The AOIs are intentionally broad in nature, generally have no known funding specifically available, and will be posted under this CSO on an open-continuous basis for one (1) year from the date of original posting. Any specific individual program requirements that are posted under the authority of this CSO will describe the desired end results, offer additional context for the needs that seek solutions, provide funding profiles, and will stipulate specific due dates for solutions.

ERDC intends to obtain "innovative" solutions that fulfill requirements, close capability gaps, or provide potential technology advancements within the AOIs advertised. Solutions may include existing technologies or procedures that are not currently in use that would enhance or streamline their mission capabilities.

AOIs for the current annual posting are listed below.

1. **Data and Data Science** – Unlock the power of Artificial Intelligence (AI)-driven analytics and engineering to shape the future of decision-making. By combining massive, heterogeneous datasets with advanced algorithms, this area reduces cognitive load and enables decision advantage for both tactical commanders and infrastructure planners.
2. **Cyber Resilience** – Protect the future of digital infrastructures, weapons systems, and national critical infrastructure with groundbreaking cybersecurity postures. This area shifts the paradigm from reactive perimeter defense to proactive, continuous monitoring, threat hunting, and automated remediation across all operational domains.
3. **Advanced Systems Engineering** – Revolutionize the design, testing, and lifecycle analysis of complex systems spanning land, air, sea, space, cyberspace, and vast

domestic infrastructure networks. This approach integrates interdisciplinary engineering principles to solve large-scale federal capability gaps.

4. **High-Performance Digital Engineering** – Accelerate engineering transformation through the development and widespread adoption of digital threads, digital twins, and model-based systems engineering (MBSE). This area permanently shifts the paradigm from document-centric processes to dynamic, model-centric capability development.
5. **Advanced Computing Technologies** – Push the boundaries of high-performance computing (HPC) and cutting-edge hardware architectures to solve the most computationally demanding physics, engineering, and intelligence problems.
6. **Autonomy, Sensing, and Robotics** – Shape the future battlespace and disaster response environments with autonomous platforms, intelligent robotic systems, and advanced sensing technologies that extend human capabilities and remove personnel from high-risk environments.
7. **Information Science and Visualization** – Transform massive, complex, and multi-modal information streams into intuitive, actionable insights. This area applies advanced data visualization and sensory fusion to ensure decision-makers are empowered by data rather than overwhelmed by it.
8. **Secure Software Engineering and Development** – Revolutionize the speed and security of software delivery by embracing modern agile methodologies and a strict "shift-left" security mindset, ensuring that mission applications are resilient by design.
9. **Collaborative Networking and Data Sharing** – Reimagine how mission-critical data is exchanged across the globe with decentralized architectures, hybrid cloud systems, and resilient tactical networks that break down legacy data silos.
10. **Enterprise Information Technology and Operational Mission Services** – Enable organizational excellence and seamless day-to-day operations through robust, scalable, and secure enterprise information technology services. This area bridges the gap between foundational administrative needs and the highly specialized technical requirements of an advanced engineering and development organization.
11. **Facilities and Infrastructure Modernization** – Technologies and capabilities to build, upgrade, and maintain premier research environments, high-performance data centers, and specialized secure facilities. This area recognizes that world-class research and development and classified computing operations require a world-class, highly adaptable physical infrastructure foundation.

This CSO will utilize a 2-Step Process for proposal review and selection for award:

Step 1: This announcement is being issued to solicit solution briefs ONLY. The purpose of the solution brief submissions is to identify potential partners that may have promising solutions relative to the AOIs specified herein. An offeror that describes a promising solution may be asked questions regarding their solution via email or requested to virtually attend a solution pitch with the Government project team. The Government reserves the right to move straight to Request for Proposal (RFP) based on solution brief only. Further, an offeror’s inability to accept an invitation to provide a solution pitch does not preclude them from receiving an RFP.

Step 2: If a solution is selected and funding is available, the Government will issue an RFP. If a solution is selected and funding is not available, the Government may request that the solution be maintained in the electronic library for consideration and subsequent funding availability up to three years after submission. If a solution is not selected, the offeror will be notified generally within 30 days of submission.

SECTION B: SOLUTION BRIEF PREPARATION AND SUBMISSION

NOTE: The Government reserves the right to not select a solution if it omits any of the required information below.

DO NOT INCLUDE CLASSIFIED OR PROPRIETARY INFORMATION

1. GENERAL FORMATTING REQUIREMENTS:

Solution briefs shall be no more than five pages and submitted electronically. All submissions must be clear, legible, and conform to the following general formatting guidelines:

1. Paper: Pages shall be 8.5 x 11 inches, single sided, with each page numbered "X of Y pages."
2. Margins: Minimum of 1 inch on all sides.
3. Type Font: 12-point Times New Roman, single spaced.
4. Acronyms: Spell out all acronyms the first time they are used.
5. Language: English.
6. Electronic file format: PDF, compatible with current Adobe Acrobat Reader. File size less than 20 MB.

2. TECHNICAL REQUIREMENTS

a. Proposed solution and mission impact

b. Overview of the concept in alignment with one of the Strategic Focus Areas. The proposed solution shall not simply repeat the Strategic Focus Area but rather provide convincing evidence that the proposed solution or potential capability fulfils a Government requirement, close capability gaps, or provide technological advancements. The following examples of convincing evidence are strongly encouraged –

   i. Authentic company URL or web address. Note: The Government may elect to use the information provided as part of its continuous market research. However, the government is not obligated to use the URL or web address as part of its evaluation process to determine the Selectee or Awardee.

   ii. Summary of product commercialization currently used in the open market.

   iii. Pictures, diagrams, models, or figures to depict the essence of the proposed solution.

c. Describe how the proposed solution is "innovative" and the feasibility of the solution solving an agency challenge, including examples demonstrating possible application

of the proposed innovation or existing use of the solution in the commercial marketplace.

"Innovative" is defined as any technology, process, or method, including research and development, that is new as of the date of submission of a proposal, or any application that is new as of the date of submission of a proposal of a technology, process, or method existing as of such date.

3. **ROUGH ORDER OF MAGNITUDE (ROM)** – Estimated price ONLY. Further details will be requested for full proposal if selected.

4. **SUBMISSION**

SAM Registration

It is critical that offerors are registered in the System for Award Management (SAM), https://sam.gov/; offerors will not be eligible for an award if not registered in SAM at the time of solution brief submission. Additionally, entities are required to be registered to receive contracts (not just assistance awards) and your address from the solution must match the registration information in SAM.

For a solution to be evaluated for possible selection, it must be submitted via the electronic form; submissions will be accepted through **5PM EST, 30 October 2027**. A hardcopy will not be accepted. Offerors may submit solution amendments any time prior to the deadline. When a submission is made, a confirmation email will be sent by the ERDCWERX portal to the email address supplied in the submission form.

Please ensure that the email address listed in your proposal is current and accurate. Please contact us by emailing info@erdcwerx.org to share details of changed email address and/or company points of contact after proposal submission.

Due to the significant expected interest in this CSO, and to maintain a written record of questions, the ERDC will be accepting individual questions through the ERDCWERX portal by using their Question Submission Form. The questions and answers will be published and regularly updated on the ERDCWERX Frequently Asked Questions (FAQ) page.

5. **SELECTION**

Submissions will be reviewed by ERDC or other Government subject matter experts.

Solutions received in response to this announcement will be selected based upon an initial review of how innovative and feasible the solution is at solving an agency challenge, the potential to enhance the mission effectiveness of the agency, and funding availability.

If a solution is selected and funding is available, an RFP will be issued by the Contracting Officer/Agreements Officer, which shall include a request for further details or documents prior to award (i.e., contractor self-developed Performance Work Statement (PWS) or Scope of Work (SOW), delivery details… etc.). A PWS is similar to a Service Level Agreement (SLA) used in the commercial marketplace. The PWS shall detail the proposed work to be completed during the period of performance, deliverables, etc. As many solutions will likely be performed/provided at military installations, the Government will provide the applicable

security requirements to be included in any award. As appropriate, the Government may engage in a collaborative process to develop the PWS/SOW, deliverables, data rights, and necessary terms and conditions for the award.

Issuance of a RFP does not guarantee award. Awards will be made once a proposal is accepted based on the proposal evaluation criteria in SECTION C.

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

SECTION C: PROPOSAL EVALATION

Proposals received in response to an RFP will be evaluated in accordance with the following evaluation criteria by scientific, technological, and/or other subject matter experts:.

a. The **technical requirements** will assess how innovative the solution is (as defined in this announcement) and the feasibility of the solution solving the agency's challenges.
b. The **importance to agency programs** will assess the solution's potential to enhance the mission effectiveness of the agency.
c. The **funds availability** will assess the availability of funding to procure the solution.

Additional evaluation criteria:

a. **Innovation:** Novelty and creativity of the solution.
b. Feasibility: Technical and operational viability.
c. **Vendor Lock-In Prevention:** Adherence to open standards, modularity, and interoperability.
d. Commercial Readiness: Use of commercially available technologies.
e. Cost Efficiency: Demonstrated cost savings and ROI.
f. Impact: Expected benefits and outcomes for the DoD.

NOTE: PWS shall not contain classified data or sensitive information. Proprietary information shall be clearly marked.

NOTE: If the proposed value of the full solution is valued at more than $900,000, and the offeror entity is not a small business, the solution will need to include a subcontracting plan prepared in accordance with RFO FAR 19.109

Price Reasonableness Determination: Price shall be considered to the extent appropriate, but at a minimum, the Contracting Officer will use market research as the primary method to determine that the price is fair and reasonable. The Government may elect to use external market research in the evaluation of the proposal. The ERDC must determine the price fair and reasonable prior to award using the procedures at RFO DFARS 212.204 In some circumstances, the Contracting Officer may request information from the offeror regarding recent purchase prices paid by the Government and/or commercial customers for the same or similar commercial items.

SECTION D: AREAS OF INTEREST AND INDIVIDUAL PROGRAM REQUIREMENTS

See Areas of Interest and specific Individual Program Requirements for this CSO by visiting

https://www.erdcwerx.org/information-technology-laboratory-cso/

Note: The AOIs and Specific Individual Program Requirements are subject to change at any time during the open continuous period. Revisions or additions of AOIs may be made on a monthly, quarterly, or as needed basis.

SECTION E: AWARD

All resultant awards will be firm-fixed price.

All items, technologies, and services (including research and development) procured via this CSO are treated as commercial. Applicants from universities and/or non-profit organizations should be aware that commercial clauses will be integrated into the award and should coordinate proposals with associated legal counsel prior to submission.

ERDC is conducting this CSO on a full and open basis and intends to award contracts in accordance with FAR part 12 and the FAR part that is deemed most appropriate for the solution proposed (i.e., FAR part 13, 15, and/or 35); the government reserves the right to award prototype agreements (e.g. Other Transaction Agreements), in accordance with 10 U.S.C. §2371b, if deemed appropriate and in the government's best interest.

FAR / DFARS clauses will be integrated into contracts on a case-by-case basis based on proposed scope.

Additional terms and conditions may be required as circumstances necessitate; examples of such would be data rights, security, R&D, educational institutions, etc.

The government does not plan to engage in the debrief process outlined in FAR part 15 but will provide feedback to unsuccessful offerors as appropriate and at its discretion.

Awards may be made using any appropriate vehicle (e.g., FAR-based contracts and Other Transactions) in accordance with applicable authorities that are effective at the time of the award.

Other Transaction (OT) Agreement:

To qualify for an OT agreement award, an offeror must satisfy at least one of the following:

a. The prototype project includes significant participation by at least one nonprofit research institution or non-traditional defense contractor (NDC),

b. All significant participants in the transaction other than the Federal Government are small business concerns, or

c. At least one-third of the total cost of the prototype project is to be paid out of funds provided by parties other than the Federal Government

An NDC is defined as an entity that is not currently performing and has not performed, for at least the one-year period preceding the solicitation of sources by DoD for the procurement or transaction, any contract or subcontract for the DoD that is subject to full coverage under the cost accounting standards prescribed pursuant to section 1502 of title 41 and the regulations implementing such section (see 10 U.S.C. 2302(9)).

FOLLOW ON ACTIVITES/ PRODUCTION: The USACE, ERDC is using competitive procedures to

select participants in a prototype transaction under 10 U.S.C 4022. If the prototype is determined successful, agencies may exercise authority under 10 U.S.C. 4022(f) to provide for, and award, a follow-on production transaction or FAR based contract without additional competitive procedures.

Award may be made using any appropriate vehicle (e.g., FAR-based contracts and Other Transactions) in accordance with applicable authorities that are effective at the time of the award.

AREAS OF INTEREST

Solicitation Number: W912HZ26SC006

1. DATA AND DECISION SCIENCE AREAS

Unlock the power of Artificial Intelligence (AI)-driven analytics and engineering to shape the future of decision-making. By combining massive, heterogeneous datasets with advanced algorithms, this area reduces cognitive load and enables decision advantage for both tactical commanders and infrastructure planners.

a. Key Technologies: Generative AI-Enabled Analytics, Predictive Maintenance Models, Logistics Optimization Algorithms, Model- and Data-Driven Decision Science, Large Language Models (LLMs), Reinforcement Learning for Wargaming, Natural Language Processing (NLP), and Advanced Machine Learning Pipelines.

b. Focus: Developing adaptive systems that support real-time decision-making in complex environments, from the tactical edge to domestic infrastructure management. This involves transforming disparate data into predictive insights for operational simulations, while simultaneously optimizing national asset management, forecasting disaster response requirements, and prioritizing critical infrastructure investments based on predictive environmental and economic modeling.

2. CYBER RESILIENCE

Protect the future of digital infrastructures, weapons systems, and national critical infrastructure with groundbreaking cybersecurity postures. This area shifts the paradigm from reactive perimeter defense to proactive, continuous monitoring, threat hunting, and automated remediation across all operational domains.

a. Key Technologies: Information Technology/Operation Technology/Control System (IT/OT/CS) Cybersecurity, Defensive Cyber Operations (DCO), Identity-Centric Zero Trust Architecture, AI-Driven Threat Detection (SIEM/SOAR), Automated Penetration Testing, Quantum-Resistant Cryptography, Secure Embedded Systems, and Endpoint Detection and Response (EDR).

b. Focus: Advancing secure, resilient solutions for dynamic cyber environments. This ensures the survivability of tactical networks while placing a major emphasis on securing the Industrial Control Systems (ICS) and SCADA networks that operate weapons systems, dams, locks, and power grids. The goal is to prevent catastrophic disruptions from state and non-state threat actors across all critical networks.

3. ADVANCED SYSTEMS ENGINEERING

Revolutionize the design, testing, and lifecycle analysis of complex systems spanning land, air, sea, space, cyberspace, and vast domestic infrastructure networks. This approach integrates interdisciplinary engineering principles to solve large-scale federal capability gaps.

a. Key Technologies: Complex Systems Engineering Design, System-of-Systems (SoS) Architectures, Digital Mission Engineering, Architecture Modeling for Multi-Domain Operations, Resilience Analysis for Critical Infrastructure Networks, and Multi-Disciplinary Optimization.

b. Focus: Driving next-generation resilient systems design. This ensures the interoperability and survivability of complex capabilities, ranging from joint combat platforms to large-scale domestic infrastructure projects. By applying systems engineering to interconnected networks—like integrated watersheds or coastal defense systems—this area mitigates cascading failures across all national security and public works domains.

4. HIGH-PERFORMANCE DIGITAL ENGINEERING

Accelerate engineering transformation through the widespread adoption of digital threads, digital twins, and model-based systems engineering (MBSE). This area permanently shifts the paradigm from document-centric processes to dynamic, model-centric capability development.

a. Key Technologies: Advanced Computational Technology, Model-Based Systems Engineering (MBSE), High-Fidelity Digital Twins and Virtual Prototyping, Physics-Based Simulation, Finite Element Analysis (FEA), Computational Fluid Dynamics (CFD), Computational Electromagnetics Modeling, Agentic AI for Engineering Automation, and Product Lifecycle Management (PLM).

b. Focus: Delivering rapid, accurate engineering solutions by integrating high-fidelity digital models. A major emphasis is the integration of agentic AI to autonomously navigate workflows and optimize designs. This approach accelerates the acquisition of advanced platforms and enhances the sustainment of aging public infrastructure, utilizing digital twins to simulate environmental stressors, predict structural integrity, and proactively schedule maintenance.

5. ADVANCED COMPUTING TECHNOLOGIES

Push the boundaries of high-performance computing (HPC) and cutting-edge hardware architectures to solve the most computationally demanding physics, engineering, and intelligence problems.

a. Key Technologies: High-Performance Computing (HPC), AI-Optimized Hardware Accelerators (e.g., Tensor/Neural Processing Units), High-End to Cloud to Edge Computing, Software-Hardware Co-Design, Neuromorphic Computing, Quantum Computing Applications, and specialized Edge Processing Units.

b. Focus: Leveraging next-generation architectures to accelerate simulation and analysis. This includes deploying specialized hardware to train large-scale neural networks. These computational advancements power a wide spectrum of mission requirements, from hypersonic modeling and intelligence processing to high-fidelity storm surge predictions, riverine flooding simulations, and long-term environmental and infrastructure assessments.

6. AUTONOMY, SENSING, AND ROBOTICS

Shape the future battlespace and disaster response environments with autonomous platforms, intelligent robotic systems, and advanced sensing technologies that extend human capabilities and remove personnel from high-risk environments.

a. Key Technologies: Autonomous Platforms and Unmanned Robotic Systems (UxS), Human-Machine Teaming, Advanced Sensing (LiDAR, Multispectral/Hyperspectral), Swarm Robotics, Collaborative Autonomous Navigation Systems, and Automated Target Recognition (ATR).

b. Focus: Advancing intelligent, adaptive robotics. This encompasses edge-based sensor fusion, autonomous logistics, and remote operations in heavily contested, GPS-denied, or hazardous environments. These technologies extend operational reach across all mission sets, enabling everything from tactical reconnaissance to remote structural inspections of critical bridges, autonomous hydrographic surveying, and rapid disaster response assessments.

7. INFORMATION SCIENCE AND VISUALIZATION

Transform massive, complex, and multi-modal information streams into intuitive, actionable insights. This area applies advanced data visualization and sensory fusion to ensure decision-makers are empowered by data rather than overwhelmed by it.

a. Key Technologies: Information Fusion, Interactive Visualization, Augmented and Virtual Reality (AR/VR) for Data Analysis, Geospatial Information Systems (GIS) Data Visualization, Cognitive Data Interaction Models, and Real-Time Digital Dashboards.

b. Focus: Enhancing human understanding and accelerating the Observe, Orient, Decide, Act (OODA) loop. This yields immersive command center displays and Common Operating Pictures (COPs) that provide multi-domain awareness. Furthermore, it supports emergency management and infrastructure planning by providing dynamic flood inundation mapping, structural health visualizations, and interagency dashboards to coordinate complex response efforts.

8. SECURE SOFTWARE ENGINEERING AND DEVELOPMENT

Revolutionize the speed and security of software delivery by embracing modern agile methodologies and a strict "shift-left" security mindset, ensuring that mission applications are resilient by design.

a. Key Technologies: Agile Development and DevSecOps Integration, Continuous Integration/Continuous Delivery (CI/CD) Pipelines, Test-Driven Development (TDD), Static/Dynamic Application Security Testing (SAST/DAST), Software Bill of Materials (SBOM) Management, Containerization, and Microservices.

b. Focus: Embedding security and compliance checks into every phase of the software lifecycle. By leveraging advanced DevSecOps pipelines, ITL ensures the rapid, reliable deployment of secure capabilities. This rigorous approach is applied universally, protecting highly classified command and control systems as well as the engineering software suites, project management tools, and public databases required to administer the nation's infrastructure.

9. COLLABORATIVE NETWORKING AND DATA SHARING

Reimagine how mission-critical data is exchanged across the globe with decentralized architectures, hybrid cloud systems, and resilient tactical networks that break down legacy data silos.

a. Key Technologies: Cross Domain Solutions (CDS), Multi-Level Security (MLS) Architectures, Hybrid Cloud Networking, Decentralized Data Architectures (Data Mesh/Fabric), Peer-to-Peer (P2P) and Software-Defined Networking (SDN), 5G/6G Tactical Edge Networks, and Blockchain for Data Integrity.

b. Focus: Empowering secure, efficient, and scalable data exchange. This focuses heavily on Multi-Level Security and robust Cross Domain Solutions to automate secure data flows across classifications, coalition partners, and interagency stakeholders. It also architects reliable bridges between secure government enclaves and public clouds, enabling seamless

data sharing with federal, state, and local authorities during both routine planning and crisis response.

10. ENTERPRISE INFORMATION TECHNOLOGY AND OPERATIONAL MISSION SERVICES

Enable organizational excellence and seamless day-to-day operations through robust, scalable, and secure enterprise information technology services. This area bridges the gap between foundational administrative needs and the highly specialized technical requirements of an advanced engineering and development organization.

a. Key Technologies: Enterprise Network Architecture and Security (Firewalls, IDS/IPS), Identity and Access Management (IAM), Cloud Service Brokerage and Management, Endpoint Security and Management, Information Technology Service Management Platforms, Software and Hardware Lifecycle Management, and Automated Provisioning.

b. Focus: Providing a secure, reliable, and modern information technology backbone that supports all organizational functions. This encompasses the strategic procurement, rapid deployment, and rigorous lifecycle management of essential enterprise security tools, networking hardware, software licenses, and services, ensuring the workforce has the modern, compliant resources required to execute their mission efficiently.

11. FACILITIES AND INFRASTRUCTURE MODERNIZATION

Build, upgrade, and maintain premier research environments, high-performance data centers, and specialized secure facilities. This area recognizes that world-class research and development and classified computing operations require a world-class, highly adaptable physical infrastructure foundation.

a. Key Technologies: Adaptive Modular Data Centers, Flexible Secure Facility Systems (e.g., Modular Sensitive Compartmented Information Facilities), Smart Building and Facilities Management Systems, High-Density Power and Liquid Cooling for High-Performance Computing, Uninterruptible Power Supply (UPS) and Enterprise Generator Systems, Physical Security and Access Control Systems, and SCADA for Infrastructure Monitoring.

b. Focus: Ensuring research and computational facilities remain state-of-the-art by strategically planning, modernizing, and maintaining critical infrastructure. This prominently features the deployment of modular data centers and modular secure facilities (including IL-7) designed for extreme flexibility. These units can be rapidly developed and integrated into the interior of existing building footprints to utilize current space, or deployed as temporary, self-contained facilities with full exterior exposure to support rapid scaling and expeditionary mission requirements. The core focus is on delivering resilient, scalable, and energy-efficient physical foundations to support next-generation capabilities.