**Engineer Research and Development Center**
**High Performance Computing Modernization Program**
**Cybersecurity for Advanced Computing and Software Modernization**
**Commercial Solutions Openings (CSO)**
**Under Solicitation Number: W912HZ25SC002**

## SECTION A: INTRODUCTION:

The Engineer Research and Development Center (ERDC) is issuing a Commercial Solutions Opening (CSO) pursuant to DFARS Subpart 212.70. Under a CSO, the ERDC may competitively award proposals received in response to a general solicitation, similar to a Broad Agency Announcement (BAA), to acquire innovative commercial products, technologies, or services based on a review of solutions by scientific, technological, or other subject matter expert peers within the ERDC. “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. 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.

The U.S. Army Engineer Research and Development Center (ERDC) Information Technology Laboratory (ITL), High Performance Computing Modernization Program (HPCMP) in collaboration with OUSD(R&E), is seeking commercial solutions that advance the state of cybersecurity for emerging and future computing paradigms to transition forward-leaning cybersecurity technologies into operationally relevant prototypes that enhance the resilience, trustworthiness, and survivability of DoD digital infrastructure. This effort will support the development, prototyping, and demonstration of cybersecurity capabilities specifically designed for modern computing environments. The objective is to explore and validate transformative technologies/solutions capable of providing autonomous, verifiable, and resilient security in contested and complex cyber-physical scenarios. Solutions should provide strong alignment to critical modernization areas including AI-enablement, autonomy, cloud-native development, and distributed edge computing.

### Problem Statement:

DoD operational environments are rapidly evolving through the integration of artificial intelligence (AI), edge computing, distributed cloud-native systems, and autonomous technologies. These capabilities enable real-time decision-making and dynamic operations across multiple domains. However, traditional cybersecurity frameworks are inadequate to address the threat landscape, which includes sophisticated adversarial cyber operations, supply chain vulnerabilities, AI system manipulation, and quantum-era decryption risks.
The Department faces an urgent challenge in safeguarding the rapidly evolving landscape of advanced computing and software-defined capabilities. Traditional cybersecurity models were

not designed for the distributed, dynamic, and AI-driven systems now central to mission success. As the DoD integrates cloud-native architectures, edge computing, autonomous systems, and real-time data processing at scale, existing security frameworks reveal significant gaps in adaptability, visibility, and resilience. This expanding attack surface — compounded by adversarial threats, software supply chain risks, and the onset of quantum-era cryptographic vulnerabilities — demands a fundamental rethinking of how cybersecurity is engineered, deployed, and sustained. To ensure mission assurance in contested digital environments, the DoD must accelerate the adoption of groundbreaking cybersecurity solutions.

**Background:**

As the DoD accelerates its adoption of next-generation computing architectures and software ecosystems, cybersecurity must evolve in lockstep. Legacy security frameworks are no longer sufficient to meet the demands of modern digital infrastructure that includes edge computing, distributed systems, artificial intelligence, and cloud-native architectures. There is a pressing need for innovative, scalable, and adaptive cybersecurity capabilities that safeguard the integrity, confidentiality, and availability of critical DoD systems.

**Requirements:**

ERDC ITL invites white papers that introduce groundbreaking cybersecurity advancements in emerging and future computing paradigms. Offerors shall propose solutions that address one or more of the following objectives:

- Develop secure-by-design software frameworks for mission-critical applications.
- Implement secure orchestration for containerized and microservice-based architectures.
- Operationalize Zero Trust principles in edge, AI-enabled, and disconnected environments.
- Deliver post-quantum cryptographic protections suitable for real-time systems.
- Design autonomous cyber defense systems using machine learning or intelligent agents.
- Provide supply chain transparency and threat intelligence via SBOM analytics.
- Create decentralized identity and access control mechanisms for multi-domain operations.
- Enable real-time behavioral monitoring, threat detection, and adversarial resilience.

Proposed solutions should articulate a clear technical architecture, maturity level (e.g., TRL), expected outcomes, and alignment to defense modernization priorities. Emphasis should be placed on interoperability, scalability, and ease of integration with existing DoD environments.

**Constraints and Considerations:**

- Solutions must be designed to operate in resource-constrained and contested conditions.
- Solutions should not rely on persistent cloud access or centralized infrastructure.
- Submissions must avoid inclusion of proprietary or classified data.
- Offerors should be prepared to deliver technical documentation, operational test results, and participate in live or virtual demonstrations.

**Estimated Government Funding Profile**:
Funding for the initial effort is available and estimated at $1M to $3M. Funding availability may change based on fiscal year and/or solution capability. The Government may elect to issue multiple awards.

**Estimated Period of Performance:** 12 months after award date for single year awards; 24 months or longer for multi-year awards.

**Desired End-state:**
The anticipated outcome of this effort is the fielding of transformative cybersecurity capabilities that enhance the protection, assurance, and integrity of advanced computing systems. Solutions must demonstrate not only technical innovation, but also practical deployability in real-world mission environments.

Successful technologies will offer measurable improvements in threat detection, response speed, autonomy of defense actions, and resilience to adversarial activity. Furthermore, they should support integration with joint and allied architectures, minimize dependence on fragile centralized infrastructures, and enable mission-critical functions to persist in a contested environment.

**This request for solution briefs is a two-step project announcement:**

**Step 1:** This announcement is being issued to solicit solution briefs ONLY. The purpose of the solution brief submission is to identify potential partners that may have promising solutions relative to fulfilling the requirements 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 brief 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:
    - Paper: Pages shall be 8.5 x 11 inches, single sided, with each page numbered "X of Y pages."

- Margins: Minimum of 1 inch on all sides.
- Type Font: 12 point Times New Roman, single spaced.
- Acronyms: Spell out all acronyms the first time they are used. One page of the proposal body is allocated to spell out acronyms, abbreviations and symbols.
- Language: English.
- Electronic file format: PDF, compatible with current Adobe Acrobat Reader. File size less than 20 MB.

2. **TECHNICAL REQUIREMENTS**:
   - Describe the proposed solution and how it will enhance the mission effectiveness of the agency. The proposed solution shall not simply repeat the Strategic Focus Area but rather provide convincing evidence that the proposed solution or potential capability fulfill a Government requirement, close capability gaps, or provide technological advancements. The following examples of convincing evidence are strongly encouraged
     - 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.
     - Summary of product commercialization currently used in the open market.
     - Pictures, diagrams, models, or figures to depict the essence of the proposed solution.
   - 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 submission. Additionally, entities are required to be registered to receive contracts (not just grants) and the address from the solution must match the registration information in SAM.

   **Solution Submission:** For a solution to be evaluated for possible selection, it must be submitted via the electronic form at erdcwerx.org from the Cybersecurity for Advanced Computing and Software Modernization CSO Submit Solution link; submissions will be

accepted through **10AM CST, 08 September 2025.** 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 ERDCWERX by emailing info@erdcwerx.org to share details of changed email address and/or company points of contact after proposal submission.

Due to the large amount of 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. All questions must be received NLT **29 August 2025**. The questions and answers will be published on the ERDCWERX Frequently Asked Questions (FAQ) page.

## 5. SELECTION

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, 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 EVALUATION

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:

- **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.
- **Importance to agency** programs will assess the solution's potential to enhance the mission effectiveness of the agency.
- **Funds availability** will assess the availability of funding to procure the solution.

**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 DFARS subpart 212.209. 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: AWARD

All resultant contracts 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).

FAR / DFAR 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.

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.