FAQs – Cybersecurity for Advanced Computing and Software Modernization

Last updated August 22, 2025

The CSO encourages submission of "Summary of product commercialization currently used in the open market". Does this mean that a solution that has not been commercialized for sale in the open market is not of interest?

Section A of the CSO Solicitation Document states that “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.”

For proposals addressing Zero Trust in HPC/edge (specifically for the High Performance Computing Modernization Program Cybersecurity for Advanced Computing and Software Modernization CSO), how important is cryptographic proof-of-action and immutable operational logging compared to detection-only capabilities and are there specific HPCMP mission scenarios where such capabilities would be prioritized for testing?

It would be inappropriate for the Government to provide relative priorities of different aspects of this solicitation. Additionally, there are no specific mission scenarios that can be shared at this time.

We wanted to ask if this opportunity was eligible for an 8(a) sole source by chance?

This opportunity is available to small and large businesses.

If our technology can satisfy two or more of the eight listed requirements, can we have multiple submissions that center on fulfillment of that individual requirement? For example, if our product is both a operationalizes ZT principles in a disconnected environments and delivers post quantum protections, trying to explain both in five pages could be challenging.

No. ERDC is looking for a single five-page submission from each offeror that encompasses the area(s) they are proposing.

Will the Government allow multiple solution brief submissions from a single offeror under this CSO? Specifically, if our organization has developed multiple distinct cybersecurity solutions that address different objectives listed in the Requirements section, may we submit separate solution briefs for each solution or are we limited to one submission per organization?

Multiple solutions may be submitted by a company, provided that each approach addresses the problem and requirements differently.

The solicitation says funding available is $1-3 million. Is that $1-3 million for a single solution or for all awards planned? If the latter, what is the desired award size ERDC is seeking for proposals?

This is only an initial estimate and funding availability may fluctuate. The dollar value should be aligned to the proposed solution. If the vendor would like to submit a white paper with scalable solutions, that is acceptable.

The announcement states that "Funding for the initial effort is available and estimated at $1 million to $3 million." Is this the total funding available, or is this the funding available per funded project? If the former, how many awards are planned?

This is only an initial estimate and funding availability may fluctuate.

Further, the announcement states that the POP is 12 months for single year awards; 24 months or longer for multi-year awards. Is it up to the proposer to determine whether to propose a single-year or multi-year POP?

This indicates flexibility of time for proposed solutions. The proposer will determine the POP.

To ensure our solution is optimized for performance and resilience in the target operational environments (edge, disconnected), could you provide any available details on the anticipated data characteristics? Specifically, common software languages, data/file types, and expected data volumes (e.g., average/maximum file sizes) would help us tailor the solution to meet the agency's challenges effectively.

The Government is looking for innovative responses from industry. These additional details cannot be released and will be discussed with the awardee post-award.

Regarding the physical and virtual hosting environments, can you clarify the expected deployment footprint? For instance, will the solution need to operate on bare-metal servers, in government-furnished virtual machines, or within specific cloud instances (e.g., AWS, Azure)? Understanding this will help us detail a deployment model that maximizes security and resilience.

The offeror’s response should be agile in order to operate in any environment.

The solicitation mentions enhancing mission effectiveness, which often involves seamless data exchange. Could you elaborate on any required integrations with existing systems? For example, are there specific requirements for interfacing with SIEM/SOAR platforms, or are there established API standards we should plan to accommodate?

The Government cannot provide these specific details at this time. The proposal should be able to exchange structured data (e.g., JSON, XML, etc.) via APIs.

In evaluating 'adversarial resilience,' could you share any information on the primary threat models the agency is focused on countering (e.g., insider threat, ransomware, supply chain attacks)? This would allow us to provide a more targeted explanation of how our architecture mitigates these specific risks.

No, the Government cannot provide this information at this time.

Regarding the desired end-state of 'integration with joint and allied architectures,' can you provide any guidance on the primary database platforms or data exchange standards currently prevalent in the target operational environments? This will help us detail the interoperability pathways for our data-centric security solution.

No. The offeror's response should be agile in order to operate in any environment.

The solicitation emphasizes solutions that do not rely on centralized infrastructure. Could you clarify if this constraint also applies to the underlying database technology itself, or is the focus primarily on avoiding dependence on centralized management and security platforms?

The intent behind this statement is to ensure resiliency.

To ensure our solution brief provides the most relevant evidence, could you share any target metrics or Key Performance Indicators (KPIs) the Government will use to evaluate 'measurable improvements' in areas like threat response speed, data exfiltration prevention, or the resilience of autonomous systems?

The offeror's response should discuss relevant KPIs that could be used to quantify improvements or effectiveness of the proposed capability. Evaluations will be consistent with Section C of the CSO Solicitation document.

In evaluating 'post-quantum cryptographic protections,' will the assessment prioritize novel cryptographic algorithms, or will it also consider architectural solutions that inherently mitigate quantum decryption risks for data-at-rest, regardless of the encryption algorithm used?

All solutions will be considered.

For the purposes of a potential prototype demonstration, what are the likely characteristics of the government-furnished test environment (e.g., available operating systems, network constraints, existing software licenses)? This will help us scope the technical requirements for a successful demonstration.

Per the solitication, "Offerors should be prepared to deliver technical documentation, operational test results, and participate in live or virtual demonstrations."

The CSO requires solutions to function in disconnected and resource-constrained environments. In the context of a Cloud-Native Application Protection Platform (CNAPP), could you clarify the government's performance and security expectations for cloud workloads

when they are operating completely isolated from their central management plane and cloud provider APIs?

Please refer to the solicitation. Specific performance and security tradeoffs will be discussed with the awardee.

Regarding the protection of containerized and microservice-based architectures, is the primary concern external threats attacking the workload, or is there an equal focus on securing the software supply chain and preventing malicious or vulnerable code from being deployed in the first place (i.e., 'shift-left' security)?

The Government cannot provide these details at this time. Evaluations will be consistent with Section C of the CSO Solicitation document.

When evaluating 'adversarial resilience' on endpoint systems, will the assessment prioritize preventative technologies that aim to block unknown threats pre-execution to ensure mission continuity, or will it focus on post-compromise detection and response capabilities?

The Government cannot provide these details at this time. Evaluations will be consistent with Section C of the CSO Solicitation document.

To better illustrate how our endpoint security enhances mission effectiveness, could you provide any general insight into the types of mission-critical applications and specialized operating systems (e.g., real-time OS, embedded systems) that are most critical to protect at the distributed edge?

The Government cannot provide these details at this time. Evaluations will be consistent with Section C of the CSO Solicitation document.

The desired end-state calls for 'measurable improvements in...resilience to adversarial activity.' Would the government be open to a solution that provides an autonomous, continuous validation capability to empirically test and measure the resilience of deployed systems against the latest adversarial techniques?

All solutions will be considered that meet the solicitation's requirements.

In pursuit of designing 'autonomous cyber defense systems,' would the evaluation consider a capability that autonomously discovers and prioritizes high-impact attack paths across the entire digital infrastructure? This would enable the government to proactively harden systems and tune defensive controls based on verified vulnerabilities rather than theoretical risks.

All solutions will be considered that meet the solicitation's requirements.

The CSO calls for 'autonomous cyber defense systems' and 'measurable improvements in... response speed.' In this context, how does the government view the human-in-the-loop role for directing these autonomous systems? Would a capability that allows operators in a contested environment to command, triage, and re-validate security actions using a low-bandwidth,

natural language interface (e.g., CLI) be considered a critical enabler for achieving practical and rapid resilience?

All solutions will be considered that meet the solicitation's requirements.

Regarding the use of AI and the need for 'verifiable' security, could you clarify the evaluation criteria for systems that employ natural language processing? Specifically, is there an advantage for solutions that use NLP to translate operator intent into deterministic, provable commands, thereby ensuring that all actions are auditable and safe, as opposed to relying on generative AI models for operational execution?

All solutions will be considered that meet the solicitation's requirements.

To ensure 'practical deployability in real-world mission environments,' how much weight is given to solutions that democratize advanced cybersecurity functions? For example, would a platform that enables a broader range of personnel, from SOC analysts to GRC teams, to safely execute and manage penetration testing operations be viewed as a significant force multiplier that enhances overall mission assurance?

All solutions will be considered that meet the solicitation's requirements.

To ensure our proposed solution is appropriately scoped for the 'scalability' and 'practical deployability' required for real-world mission environments, could you provide an estimated range for the number and type of assets within a typical operational environment? For example, an approximate count of endpoints, servers, cloud instances, and edge devices, or the general size of the IP address space, would be highly valuable for tailoring a feasible and resource-aware architecture.

The Government cannot provide these details at this time. Evaluations will be consistent with Section C of the CSO Solicitation document.