Integrated Defensive Cyberspace System (IDCS)
Secure Platform Architecture for Real-Time Threat Analysis and Network Defense (SPARTAN)
Request for Information (RFI) 2 (FA8307-25-R-B057)

1 INTRODUCTION:

1.1 In accordance with FAR 52.215-3 Request for Information (RFI), this announcement is solely for market research purposes. The Government does not intend to award a contract on the basis of this RFI or otherwise pay for the information solicited. Although the term "offeror" may be used in this RFI, your response will be treated as information only, and not as a proposal. Our aim is to gather information to identify potential businesses capable of providing services related to the Integrated Defensive Cyberspace System (IDCS). Your responses will help shape our requirement prioritization, acquisition approach, performance work statement/statements of work/objectives, and performance requirements. Participation in, or omission from, this market research does not guarantee or preclude participation in any future solicitations or contract awards. Small businesses are encouraged to participate in this market research. Joint ventures or teaming arrangements are also encouraged. If you propose a teaming arrangement, please clearly identify the roles and responsibilities of each team member in your response.

1.2 The Defensive Cyber Systems Branch (AFLCMC/HNCD) is considering standing up a *Secure Platform Architecture for Real-Time Threat Analysis and Network Defense* (SPARTAN) Multi-Award Contract (MAC) Indefinite-Quantity Indefinite-Delivery (IDIQ) contract and is conducting market research to identify potential sources with the expertise, capabilities, and experience required for the development, fielding, and sustainment of an enterprise-wide, System-of-Systems (SoS) platform similar to IDCS. This complex and critical effort aims to protect and defend the Department of the Air Force (DAF)'s cyberspace domain. AFLCMC/HNCD seeks vendors demonstrating the ability to deliver outcomes promptly and adaptively, ensuring a rapid flow of operational value, enhanced by continuous learning and maturation of supporting processes and team infrastructure.

1.3 Aligned with the Secretary of Defense's directive of March 6, 2025, to accelerate software acquisition and maximize warfighter lethality, SPARTAN will be designed to rapidly deliver and iterate on critical defensive cyber capabilities, leveraging the flexibilities afforded by *DoDI 5000.87, Operation of the Software Acquisition Pathway*. To meet the urgency of evolving cyber threats and ensure our forces maintain a decisive advantage, we are seeking partners capable of demonstrating both innovative solutions and the agility to respond within accelerated timelines. Therefore, the response timeframe for this RFI is intentionally concise to identify vendors best positioned to support a rapid acquisition and deployment model, consistent with the Department's commitment to outpacing our adversaries in the cyber domain.

1.4 The objective of this RFI is to acquire contractor services that enable the IDCS program to deliver enhanced situational awareness, proactive threat detection, accelerated incident response, and effective cyber defense across the DAF enterprise, fulfilling IDCS requirements. Contractor performance shall align with IDCS Performance Requirements identified in Attachment 1, SPARTAN SOO 28 August 2025, Section 4 ensuring interoperability, scalability, and security across the IDCS SoS, and contributing to unified war-fighting capabilities for cyberspace operations forces.

2 CAPABILITY AREA-SPECIFIC QUESTIONS

(NOTE: The following sections are organized by SPARTAN SOO capability area (Attachment 1, SPARTAN SOO 28 August 2025, Section 4.5). Please reference your understanding of the SOO capabilities matrix (Attachment 1, SPARTAN SOO 28 August 2025, Appendix A. IDCS Capability Areas & Objectives Matrix) in your responses. Assumption: Currently, offerors have limited access to IDCS requirements, which may be provided at a later date. Meanwhile, the IDCS PMO is requesting that offerors provide the best answers/solutions possible with limited data.)

2.1 Cloud Services and Infrastructure Management *(NOTE: These questions focus on the vendor's ability to design, build, and maintain a secure, resilient, and scalable hybrid cloud infrastructure for IDCS.)*

2.1.1 *Cloud One and Platform One Integration & Secure Deployment:* Detail your experience integrating Cloud One and Platform One, providing specific examples of successful implementations. Describe the tools and techniques you will employ to ensure secure and automated deployments and maintenance in a multi-domain environment.

2.1.2 *Diverse Hardware Platforms & Infrastructure as Code (IaC)/Configuration as Code (CaC):* Describe your technical approach to providing solutions for diverse hardware platforms (garrison, deployable, mobile, and sensor platforms), including specific examples of successful implementations and the tools/techniques used. Explain your IaC/CaC approach, highlighting specific examples of automating infrastructure provisioning, configuration, and management in similar DoD environments. List planned tools and technologies.

2.1.3 *Infrastructure Health & Performance Monitoring:* Outline your strategy for monitoring infrastructure health and performance. Describe proactive measures to prevent outages and ensure operational continuity, including specific metrics, thresholds, and automated remediation strategies.

2.1.4 *Cloud Services, Hybrid Architecture, and Scalability:* Describe your experience designing and implementing cloud services and hybrid architectures that meet demanding performance and scalability requirements in DoD environments (similar to IDCS), especially with Cloud One and Platform One. Provide specific project examples where you achieved challenging performance targets, scaled to meet demands, and ensured efficient resource utilization. Include supporting metrics and data.

2.2 Agile Software Engineering and DevSecOps *(NOTE: These questions focus on the vendor's ability to develop, deploy, and maintain secure and high-quality software using Agile and DevSecOps practices.)*

2.2.1 *DevSecOps Framework and CI/CD Pipeline:* Describe your DevSecOps framework and tools, detailing your CI/CD pipeline and its integration of automated security testing at each stage. Explain your approach to secure coding practices and code repository management.

2.2.2 *Software Component Integration and Interoperability:* Detail your approach to ensuring seamless integration and interoperability of software components from different vendors, including specific tools, processes, and governance structures.

2.2.3 *Agile Framework:* Explain how you would tailor your Agile approach (including SAFe or other frameworks) to address Task Orders with varying complexity and scope. Describe the criteria for determining when a full SAFe implementation is needed versus a lighter-weight approach, providing specific examples based on team size, project duration, and regulatory factors. Describe the specific Agile methodologies or practices you would employ in each scenario.

2.2.4 *Containerization and Orchestration:* Outline your approach to containerization and orchestration, specifying the platforms and tools you will utilize to ensure scalability, portability, and efficient resource utilization.

2.2.5 *Software Testing Methodology and Configuration Management:* Explain your software testing methodology, including specific testing types (unit, integration, system, performance, user acceptance) and tools employed. Describe your approach to managing software configurations, versions, and releases to ensure stability and minimize disruption.

2.3 Cybersecurity Operations and Compliance *(NOTE: These questions focus on the vendor's ability to implement and maintain a robust security posture, ensuring compliance with DoD regulations and protecting the IDCS SPARTAN system from cyber threats.)*

2.3.1 *Zero Trust Architecture in a System of Systems (SoS) Environment:* Detail your approach to implementing and managing a Zero Trust architecture within a SoS environment, including specific technologies and strategies for addressing the unique challenges of a SoS. Provide recommendations for addressing security gaps, including specific strategies, technologies, and best practices.

2.3.2 *Authority to Operate (ATO) and Cyber Survivability Attributes (CSAs):* How will you achieve and maintain Authority to Operate (ATO) for all IDCS components while ensuring compliance with Cyber Survivability Attributes (CSAs) as defined in the CJCS's Cyber Survivability Endorsement Implementation Guide , applicable DoDIs, and NIST publications? Include specific steps, timelines, and resources.

2.3.3 *Continuous Security Monitoring, Intrusion Detection, and Incident Response:* Describe your experience with continuous security monitoring, intrusion detection, vulnerability management, and incident response planning. What tools and technologies will you utilize and how will you integrate them to provide a comprehensive and proactive security posture?

2.3.4 *Supply Chain Risk Management:* Describe your approach to identifying, assessing, and mitigating supply chain risks, including specific tools, processes, and security measures you would implement to ensure the security and integrity of the IDCS SPARTAN supply chain.

2.4 Data Management, Analytics, Advanced Analytics and Intelligent Automation Integration *(NOTE: These questions focus on the vendor's ability to manage, analyze, and leverage data to enhance threat detection, prediction, and response capabilities.)*

2.4.1 *Data Pipeline Design and Management:* Explain your approach to designing and managing robust data pipelines for ingesting, processing, and storing large volumes of diverse data. Provide recommendations for addressing potential gaps, including specific technologies, processes, and compliance frameworks.

2.4.2 *Big Data Platform for Defensive Cyber Operations (DCO):* Describe your experience designing, implementing, and managing an enterprise big data platform for DCO (or similar). Explain how you would ensure data is readily accessible, properly governed, and securely managed for advanced analytics and threat intelligence. Address the challenges of ingesting, processing, and analyzing large volumes of diverse data sources in near real-time to support DCO missions. Provide specific examples of technologies, architectures, and data governance strategies, including how you would balance data accessibility with security requirements.

2.4.3 *Scalable Data Storage, Advanced Analytics (AI/ML), and Data Security:* Detail your experience implementing and managing scalable data storage solutions and developing advanced data analytics capabilities, including AI/ML, specifying the tools and technologies you will use. How will you ensure data security and privacy compliance with DoD regulations and policies, including specific measures for data encryption, access control, and data loss prevention?

2.4.4 *Data Sources and AI/ML for DCO:* Describe specific data sources and types you would leverage to support DCO operations, ensuring the data is timely, accurate, and relevant to DCO analysts and operators. Describe specific AI/ML algorithms and techniques you would use to enhance threat detection, prediction, and response in the IDCS SPARTAN environment.

2.5 System and Enterprise Integration Services *(NOTE: These questions focus on the vendor's ability to integrate diverse systems and components into a cohesive and interoperable architecture.)*

2.5.1 *System-of-Systems Integration (DoD Experience):* Describe your experience with large-scale system-of-systems integration, specifically within a DoD environment.

2.5.2 *DoD Enterprise Services Integration Challenges and Mitigation:* Provide a detailed analysis of the technical, security, and programmatic challenges associated with integrating with relevant DoD enterprise services, proposing mitigation strategies for each challenge.

2.5.3 *Interface Definition and Interoperability with DCO Legacy Systems:* Explain your approach to defining, documenting, and managing interfaces between IDCS components and external systems. How will you ensure interoperability with DCO legacy systems?

2.5.4 *DoD Networking Standards and Interoperability Requirements:* Describe your experience with specific DoD networking standards and protocols and how you would ensure compliance in the IDCS SPARTAN environment. Detail your experience designing and implementing systems that meet specific quantitative interoperability requirements in DoD environments similar to IDCS, particularly with Joint Cyber Warfighting Architecture (JCWA) and Advanced Battle Management System (ABMS). Provide specific project examples where you successfully integrated diverse systems, ensured seamless data exchange, and complied with relevant DoD standards and protocols, including supporting metrics and data.

2.6 Command, Control, Communications, Computer, and Cyber Intelligence (C5I) Support *(NOTE: These questions focus on the vendor's ability to provide C5I support for DCO operations, enabling effective situational awareness, command and control, and intelligence analysis.)*

2.6.1 *Command and Control (C2) and Cyber Intelligence Platform Integration:* Detail your experience integrating Command and Control (C2) applications and cyber intelligence platforms. How will you support the development and dissemination of operational orders in both human and machine-readable formats?

2.7 Enterprise Architecture and Requirements Management (NOTE: *These questions focus on the vendor's ability to develop and manage the IDCS enterprise architecture,* *ensuring alignment with DoD and DAF standards and supporting long-term scalability and interoperability.*

2.7.1 *IDCS Enterprise Architecture Development:* Explain your approach to developing, documenting, and maintaining the IDCS enterprise architecture, including specific frameworks, methodologies, and tools.

2.7.2 *DoD/DAF Architecture Alignment and Stakeholder Engagement:* Explain how you will ensure alignment with broader DoD and DAF architectures and how you will actively engage stakeholders throughout the process.

2.7.3 *IDCS Architecture Assessment:* How would you rapidly assess and gain a comprehensive understanding of the current IDCS architecture? What artifacts or deliverables would you prioritize examining? How would you identify potential weaknesses, redundancies, or areas for improvement within the existing architecture?

2.7.4 *SPARTAN SOO Technology Assessment and Roadmap Development:* How can the SPARTAN SOO better address technology assessments and roadmap development for the IDCS effort and future Task Orders? Provide concrete recommendations for improving the SOO's coverage of technology assessments and roadmap development, including specific methodologies, tools, and processes.

***2.8* Test, Evaluation, and Validation Services** *(NOTE: These questions focus on the vendor's ability to provide comprehensive testing, evaluation, and validation services, ensuring the IDCS SPARTAN system meets its performance requirements and security objectives.)*

2.8.1 *Test and Evaluation Master Plan (TEMP) and Testing Methodologies:* Describe your approach to developing and implementing a Test and Evaluation Master Plan (TEMP), specifying the testing methodologies and tools you will utilize.

2.8.2 *Automated Testing for IDCS:* Describe specific automated testing tools and techniques you would use to improve test efficiency and coverage in IDCS.

2.9 Service Management, Training, and Sustainment Operations *(NOTE: This question focus on the vendor's ability to provide effective service management, training, and sustainment operations, ensuring the long-term availability and usability of the IDCS SPARTAN system.)*

2.9.1 *Multi-Tiered Service Desk/Help Desk:* Explain your approach to establishing and operating a multi-tiered service desk/help desk.

2.9.2 *IDCS User Training Programs:* How will you develop and deliver training programs for IDCS users?

2.10 Program Management, Governance, and Innovation *(NOTE: These questions focus on the vendor's ability to provide effective program management, governance, and innovation, ensuring the successful execution of the SPARTAN (IDCS) MAC IDIQ and continuous improvement of its capabilities.)*

2.10.1 *Program Management Approach:* Detail your program management approach, including specific tools and techniques for planning, execution, monitoring, and risk management.

2.10.2 *Enterprise Architecture Sustainment and Innovation Transition:* Provide specific examples of projects where you successfully transitioned the sustainment and limited innovation of an existing enterprise architecture in a complex, regulated environment (ideally DoD/DAF). Quantify the benefits achieved during those transitions (e.g., cost savings, improved performance, reduced downtime).

2.10.3 *SPARTAN SOO Subcontractor Management and Governance:* Provide concrete recommendations for improving the SPARTAN SOO's coverage of subcontractor management and governance processes, including specific contract clauses, oversight mechanisms, and performance metrics.

2.11 General Questions

2.11.1 **General Implementation Approach** *(NOTE: These questions address the vendor's overall approach to implementing IDCS, ensuring a cohesive and integrated solution.)*

2.11.1.1 *Innovative Technologies/Capabilities:* If your company offers a technology or capability not currently outlined in the SPARTAN SOO objectives (e.g., Kubernetes edge hosting platforms design and implementation, not explicitly in CA 6), provide details for government consideration.

2.11.1.2 *SPARTAN SOO Implementation Strategy:* Describe your overall implementation strategy for meeting the objectives outlined in the SPARTAN SOO. How will you prioritize tasks and manage dependencies between different CAs? Provide a detailed and realistic implementation plan, including key milestones, dependencies, and risk mitigation strategies, justifying your prioritization.

2.11.1.3 *Scalability and Interoperability Implementation:* Describe your overall implementation strategy for ensuring the IDCS system meets quantitative scalability and interoperability requirements across all CAs, as outlined in the SPARTAN SOO. How will you prioritize tasks, manage dependencies, and mitigate risks? Provide specific examples of how you will monitor progress and adapt to changing requirements.

2.11.1.4 *Inter-CA Integration:* How will you ensure seamless integration and interoperability between the different CAs throughout the project lifecycle?

2.11.1.5 *Project Management Methodology and Agile Principles:* Describe your proposed project management methodology and its alignment with Agile principles. How will you incorporate feedback and adapt to changing requirements throughout the implementation process? Provide a detailed description of your methodology, including specific tools, processes, and techniques, and how it leverages Agile principles.

2.11.1.6 *Multi-Vendor Environment Management:* How will you manage a multi-vendor environment, ensuring collaboration and cohesive SoS integration? Describe your approach, including specific strategies for fostering collaboration, resolving conflicts, and ensuring SoS integration, providing examples of successful multi-vendor collaborations.

2.11.1.7 *CA Implementation Challenges and Risks:* How will you address potential challenges and risks associated with implementing the objectives within each CA, providing specific examples and detailed mitigation strategies?

2.11.1.8 *CA Implementation Assumptions and Dependencies:* What are your key assumptions and dependencies for successfully implementing the objectives within each CA? Clearly state and realistically assess potential dependencies.

2.11.2 **Labor Category (LCAT) Analysis:** Use Attachment 2, SPARTAN LCATs Table 28 August 2025, (an Excel workbook with two tabs). The purpose of each tab is described below:

2.11.2.1 In Tab 1, *LCAT Table*: this tab is a list of proposed LCATs that the Government has determined would be needed to execute the requirements associated within the SOO.

2.11.2.2 In Tab 2, *Skill Level Definitions*: this tab is a list of requirements that highlight the skill levels, descriptions and typical experience associated with needed positions.

2.11.2.3 Analyze the IDCS Capability Areas & Objectives Matrix (*ref Attachment 1, SPARTAN SOO 28 August 2025, Appendix A)* against Attachment 2 to help identify any missing IDCS CA positions that can be added to Tab 1. If any LCATs need to be added, briefly describe the position(s), desired skill level, and any required industry certifications relevant to the SOO.

2.11.3 **Additional Beneficial Questions:** *(NOTE: These questions address additional considerations that may be relevant to IDCS.)*

2.11.3.1 *Open Standards and DoD Interoperability:* How does your proposed solution leverage open standards and promote interoperability with existing and future DoD systems and architectures? Describe your experience implementing and adhering to relevant DoD standards and specifications (e.g., JCIDS, DoDAF, MOSA).

2.11.3.2 *Scalability, Adaptability, and Emerging Technologies:* How is your proposed solution designed to scale and adapt to evolving threats and mission requirements? Describe your approach to incorporating emerging technologies and adapting to changing operational needs.

2.11.3.3 *Government Personnel Training and Knowledge Transfer:* Describe your approach to providing comprehensive training and knowledge transfer to Government personnel. How will you ensure that Government personnel are able to effectively operate, maintain, and evolve the IDCS SoS?

2.11.3.4 *Supply Chain Risk Management:* Describe your approach to supply chain risk management. How will you ensure the security and integrity of the IDCS supply chain and mitigate risks associated with counterfeit or compromised components?

2.11.3.5 *Data Rights and Intellectual Property:* What is your approach to data rights and intellectual property? How will you ensure the Government has the necessary rights to access, use, and modify the IDCS system and its associated data?

2.11.4 **SPARTAN SOO Clarity Feedback:** To improve the clarity of the SPARTAN SOO, please identify any areas where additional content or detail is needed to fully understand the requirements and vendor expectations. Provide specific examples and suggest the type of information that would be helpful.

3 CONTRACTOR WHITE PAPER RESPONSE

3.1 Content and Structure: Interested parties shall respond to this RFI uIAW Attachment 3, SPARTAN Whitepaper Template. Clearly indicate (cite) the question number being answered at the start of each response.

3.2 Documentation Marking/Proprietary Information:

3.2.1 Proprietary information, if any, should be minimal and MUST BE CLEARLY MARKED.

3.2.2 To aid the US Government, please segregate proprietary information into a separate section or appendix of your whitepaper.

3.2.3 Be advised that all submissions become US Government property and will not be returned.

3.3 Documentation Marking/Proprietary Information:

To expedite market research processes, it is important for AFLCMC/HNCD to understand any existing relationships between Respondents and the SETA (Systems Engineering and Technical Assistance) and A&AS (Advisory and Assistance Services) support contractors assisting IDCS efforts. Please inform us if your organization has any relevant partnerships, collaborations, or competitive interactions with the entities in ***Table 2, AFLCMC (IDCS) Support Vendors***. The government maintains Non-Disclosure Agreements (NDAs) with these contractors, and this information will help us streamline data flow while protecting proprietary information, if and when applicable.

3.4 Controlled Unclassified Information (CUI)

3.4.1 If your response contains CUI, you must mark it in accordance with Department of Defense Instruction (DoDI) 5200.48, "*Controlled Unclassified Information (CUI)*," and 32 CFR Part 2002. This includes applying appropriate banner markings, portion markings, and CUI category designations. *(ref Section 7, for how to transmit CUI)*

Table 2. AFLCMC (IDCS) Support Vendors

AFLCMC (IDCS) Support Vendors	
Applied Research Solutions (ARS)	BEAT
MITRE	Odyssey
Astrion	Information Systems Group (ISG)
Colsa	Quantech
Abacus	Valiant-X Technologies (VXE)
Insight Global	Nyla

4 INDUSTRY DISCUSSIONS

IDCS Program Office representatives may or may not choose to meet with potential offerors. Such discussions would only be intended to get further clarification of potential capability to meet the requirements, especially any development and integration risks.

5 QUESTIONS

5.1 Questions regarding this RFI shall be submitted in writing by e-mail to stacy.wilson.1@us.af.mil, sean.danzy.1@us.af.mil and christian.davis.33@us.af.mil. Verbal questions will **NOT** be accepted. Questions will be answered by posting questions/answers to this posting via www.sam.gov website; accordingly. Questions shall **NOT** contain proprietary or classified information. The Government does not guarantee that questions received after **5 September 2025 at 2:00PM CST,** will be answered.

6 RESPONSES

6.1 Responses must be received no later than the close of business on **19 September 2025 at 2:00 pm CST**. (Note: Adhere to the page limitations specified in this template for each section of your white paper. Responses exceeding the specified page limits will not be considered.)

6.2 Responses must be sent electronically via email to: stacy.wilson.1@us.af.mil, sean.danzy.1@us.af.mil and christian.davis.33@us.af.mil; or DoD SAFE (https://safe.apps.mil/) ATTN: IDCS RFI# FA8307-25-R-B057 RESPONSE (followed by your Company Name).

6.2.1 All responses containing CUI information MUST be sent electronically via an encrypted email to: stacy.wilson.1@us.af.mil, sean.danzy.1@us.af.mil and christian.davis.33@us.af.mil; or DoD SAFE (https://safe.apps.mil) ATTN: IDCS RFI# FA8307-25-R-B057 RESPONSE (followed by your Company Name).

7 SUMMARY

THIS IS A REQUEST FOR INFORMATION (RFI) ONLY to identify sources that can provide integrated defensive cyber capabilities. The information provided in the RFI is subject to change and is not binding on the Government. Please note that the Government may choose to conduct industry discussions with potential offerors to further clarify potential capabilities and address any development and integration risks. Your participation in this RFI does not guarantee an invitation to such discussions. All RFI submissions become Government property and will not be returned. In accordance with Executive Order (EO) 14179, *Removing Barriers to American Leadership in Artificial Intelligence,* and the Office of Management and Budget (OMB) memorandum *Accelerating Federal Use of AI through Innovation, Governance, and Public Trust, dated 3 Apr 25*, AFLCMC/HNCD will leverage generative AI in the IDCS effort. This integration aims to enhance data analysis, expedite the adoption of AI throughout the government, and improve our decision-making processes. These efforts will be carried out while remaining compliant with all applicable EOs, as well as DoD and the DAF policies and guidelines.