Closed Area of Interest (AoI) for SPEED CSO

1.0 Issued By

Program Office: Air Force Civil Engineer Center (AFCEC), JBSA-Kelly AFB
Contracting Office**:** AFMISC AFMC 772 ESS/PKS, JBSA-Kelly AFB

2.0 AoI Identifiers

AoI Title: Air Force Civil Engineering Center Business Systems Modernization
CSO AoI Number: Closed – 26 -02. POC: Christine Zogbi
AoI Release Date: 01/21/2026
Responses: See FA890326SC001 for submission instructions in addition to paragraph 5.0 below

3.0 AoI Information

The Air Force Civil Engineer Center (AFCEC) seeks innovative solutions to modernize its legacy Civil Engineer (CE) Information Technology (IT) portfolio. This effort requires implementing secure, cloud-ready architecture, executing comprehensive data modernization, and integrating Artificial Intelligence (AI)-enabled analytics to enhance installation readiness, resilience, and data-driven decision-making.

This Area of Interest (AoI), issued under the AFIMSC SPEED Commercial Solutions Opening (CSO) , solicits innovative technologies, processes, or methods to meet the objectives detailed in Section 4.0. Interested parties are encouraged to review the full SPEED CSO for submission and evaluation details.

This effort, aligned with Department of the Air Force and CDAO guidance, is essential for improving installation readiness, resilience, lifecycle management, and data-driven decision-making for Air Force installations.

This Area of Interest focuses on solutions that modernize legacy business systems and data environments while enabling responsible AI capabilities aligned with Department of the Air Force (DAF) and Department of War (DoW) enterprise strategies under the AFIMSC SPEED Commercial Solutions Opening FA890326SC001.

The vendor shall ensure that all performance, technical solutions, and deliverables adhere to the strategic directives, mandates, and policies set forth by Air Force Materiel Command (AFMC), the Secretary of the Air Force for Acquisition, Technology and Logistics (SAF/AQ) and Chief Information Officer (SAF/CN), the Chief Data and Artificial Intelligence Officer (SAF/CDAO), Headquarters Air Force Directorate of Logistics, Engineering and Force Protection (A4), Air Force Installation and Mission Support Center and the Air Force Civil Engineer Center (AFCEC) IEO Strategy.

The vendor's compliance framework shall be integrated into all project management and technical execution activities as follows:

Strategic Cloud and Data Alignment (SAF/CN & SAF/CDAO): The vendor shall strictly adhere to the SAF/CN Cloud Hosting Accountability Memo, ensuring all system

architectures and administration activities align with Air Force mandates for cloud consolidation within approved environments such as Cloud One. The vendor's data management, analytics, and Robotic Process Automation (RPA) methodologies shall be governed by the principles established by the SAF/CDAO to promote data-driven governance, interoperability, and analytic innovation.

Command and Functional Requirements (AFMC & A4): The vendor shall execute all tasks in accordance with AFMC standards for lifecycle and systems engineering management. All project management and development processes shall be fully responsive to the operational and mission-centric requirements defined by the A4 functional community, ensuring all IT solutions deliver direct and measurable value to the Civil Engineer mission.

Direct Mission Execution (AFCEC IEO Strategy): The vendor's day-to-day operations and strategic planning shall be directly mapped to the objectives of the AFCEC IEO Strategy. The vendor shall actively identify and leverage opportunities to reduce IT duplication, promote standardization, and enhance IT service delivery, ensuring all efforts directly enable AFCEC's strategic goals.

Through rigorous project management, continuous stakeholder engagement, and a comprehensive understanding of the regulatory landscape, the vendor shall maintain a persistent state of compliance and deliver solutions that are secure, efficient, and fully aligned with the warfighter's mission.

Interested parties are highly encouraged to review the SPEED CSO in its entirety to obtain more information on the process for submission and evaluation of the AoI responses.

This CSO AoI seeks to solicit innovative solutions that meet the objectives detailed in Section 4.0 below. The term 'innovative' is defined as any technology, process, or method, including research and development that is new as of the date of proposal submission; or any new application of an existing technology, process or method as of the proposal date.

AFIMSC is not obligated to extend a request for proposal or make an award as a result of posting this AoI; all awards are subject to the appropriateness or identified usefulness of the proposed offer, availability of funds, and ability to achieve successful negotiations.

This CSO AoI is not an authorization to begin performance, and in no way obligates the Government for any costs incurred by the Offeror associated with developing a Response. Prior to commencement of any activities associated with performance under this CSO AoI, the Government will issue a written directive or contractual document signed by the Contracting Officer with appropriate consideration established. ACC-RRAD reserves the right to modify the requirements of this CSO AoI.

The authority to issue this AoI is derived from the AFIMSC SPEED Commercial Solutions Opening FA890326SC001, dated 21 January 2026. The CSO authority is Section 803 of the National Defense Authorization Act for FY2022, Public Law 117-807, and Class Deviation 2022-O0007.

4.0 Scope of AoI

The Scope includes, but is not limited to:

- Modernization of legacy applications through refactoring, re-platforming, re-hosting, or replacement
- Data modernization, integration, and migration to support enterprise analytics
- Reduce internal IT duplication and increase interoperability/data integration
- System interface and workflow optimization
- Secure cloud or hybrid-cloud enablement
- Application sustainment and continuous improvement using Agile and DevSecOps practices

4.1 AoI Background

Interested ~~small business~~ vendors shall demonstrate experience and approaches in modernizing legacy business systems supporting civil engineering, installation management, environmental, energy, real property, and infrastructure lifecycle functions. Solutions should improve interoperability, reduce technical debt, and enable scalable analytics and AI adoption and must be measurable and aim to:

- Improve installation readiness and mission support
- Enhance data accessibility and decision quality
- Reduce system sustainment costs and technical debt
- Enable continuous modernization and future AI integration

4.2 Technical/Capability Requirements

Solutions must deliver the following key capabilities:

The business outcomes required to support the identified functions will enable AFCEC CBF to oversee the vision and roadmap for CE IT, this includes:

1. Cybersecurity & Risk Management Framework (RMF) Expertise

The contractor must provide comprehensive cybersecurity support, acting as the Information Systems Security Manager (ISSM). This requires deep expertise in the entire DoD Risk Management Framework (RMF) process to achieve and maintain Authority to Operate (ATO) for all systems.

Assessment & Authorization (A&A): Develop, manage, and update A&A packages in eMASS, including the System Security Plan (SSP), Security Test Plans (STP), and Plan of Action & Milestones (POA&M).

Vulnerability Management: Perform continuous monitoring using tools like Assured Compliance Assessment Solution (ACAS), conduct vulnerability analysis, and remediate findings from Security Technical Implementation Guides (STIG) and Security Content Automation Protocol (SCAP) scans to ensure system compliance.

Security Engineering: Integrate cybersecurity requirements into all phases of the software development lifecycle (SDLC) and manage the Ports, Protocols, and Services (PPS) Matrix.

2. Software Engineering & Development

The contractor must provide full lifecycle support for existing applications, focusing on sustainment, maintenance, and minor modernization.

Programming Languages & Tools: Expertise in the Microsoft Visual Studio suite, C#, and SharePoint Designer is required to support legacy applications.

Database Interfacing: Ability to develop and maintain interfaces with Microsoft SQL and Oracle databases.

DevSecOps: Experience with software security code analyzers and Azure DevSecOps platforms in a DoD cloud environment is desired.

Systems Engineering Process (SEP): Must develop and maintain all required SEP documentation, manage configuration changes through a Configuration Control Board (CCB), and perform comprehensive testing (unit, system, regression).

Personnel: Must provide a Senior Software Developer meeting IASAE Level II certification requirements with an active Secret clearance.

3. Functional & Business Systems Analysis
The contractor needs the ability to bridge the gap between functional user needs and technical development teams, particularly for the EESOH-MIS system.

Agile Methodologies: Use Agile to elicit and document business needs and functional requirements.

Requirements Management: Create artifacts such as Use Cases, Epics, Features, and Stories using the Atlassian toolset (Jira, Zephyr, Confluence).

Domain Knowledge: A deep understanding of the EESOH-MIS system or a similar large-scale DoD enterprise system is required for the Senior Functional Task Lead.

4. AI and Advanced Analytics Enablement
Solutions shall enable AI, machine learning (ML), and advanced analytics capabilities to enhance AFCEC business processes and mission outcomes, including:

- Predictive analytics for infrastructure sustainment, asset condition, and lifecycle forecasting
- Intelligent automation of civil engineering business workflows
- Data-driven decision support for installation planning, readiness, and resource allocation
- Natural language processing and analytics to improve insight from structured and unstructured data

AI-enabled solutions must be designed to be secure, explainable, auditable, and responsible, consistent with federal and DoD AI ethical principles and governance requirements.

5. SharePoint Database Systems Re-engineering
The contractor shall re-engineer three separate AFCEC/CXA SharePoint databases (Inventory Management, Chemical Database, and Operations Work Order) into a single, consolidated web application hosted in a cloud environment like TaMIS. The contractor must manage the following:

- Entire project lifecycle, which includes planning, analysis, agile development, data migration, testing, RMF Security Assessment and release to production "Go Live".

- Key responsibilities include creating a unified graphical user interface for the three databases , ensuring the new system complies with all Risk Management Framework (RMF) CyberSecurity requirements for NIPRNet access, and delivering the final CXA 1.0 web application
- The contractor must also provide specific deliverables, including an Integrated Master Schedule, monthly status reports, and all necessary cybersecurity documentation.

6. Platform Development/Fire Certification

The contractor shall design, develop, test, and deploy a comprehensive, secure Student Records and Certification Management Platform for a DoD-wide audience including:

- A web-based system to centralize and automate the management of student records and certifications, including issuance, revocation, and reporting, while integrating with Government-furnished SharePoint Online and SQL Server environments
- Adhere to a structured project management methodology and culminate in a fully operational platform that meets stringent DoD security standards, including compliance with the RMF to achieve a mandatory Authority to Operate (ATO).

4.3 System Requirements

AOI will involve the following systems: Environmental Restoration Program Management System (ERPIMS), Integrated Information Tool (IIT), AFCEC Portal, Administrative-IR, Research Development Modeling & Simulation (RDM&S), Inventory Management, Chemical Database and Operations Work Order SharePoint Tools as well as any new additions to the CE IT IEO-managed IT portfolio.

4.4 AoI Constraints

Vendors are expected to be cleared for Secret and will need to have access to EMASS. Access to government systems and network necessitating a Government Common Access Card. Ability to travel CONUS.

5.0 Submission Requirements

A Spiral 1 white paper brief must be sent via e-mail submission with subject line stating "Air Force Civil Engineering Center Business Systems Modernization" to the POC listed in paragraph 6.0 by the date and time this AoI closes - 5:00 P.M. (CST) on 10 March 2026.

Spiral 1 ~~3~~ written solution briefs received after the specified due date and time will be discarded and not be evaluated by the Government.

6.0 Points of Contact

Questions may be sent to:
Christine Zogbi, christine.zogbi.1@us.af.mil

Contracting Officer:
Michael Grasso, michael.grasso.3@us.af.mil

Contract Specialist:
Krystle Zapata, krystle.zapata.1@us.af.mil