Amendment 03

04/28/2026

Area of Interest 1: Air Mobility Command (AMC) A6 – Base Information Technology Modernization – Please note that responses will only be accepted from Service-Disabled Veteran Owned Small Businesses (SDVOSBs)

***All amendment changes noted in red font.**

Introduction & Mission Objective

Air Mobility Command (AMC) seeks innovative partners to lead a comprehensive transformation of its Information Technology (IT) infrastructure. The current legacy environment is outdated, inefficient, and hinders the "Global Reach" mission by compromising operational speed, data sharing, and overall warfighter effectiveness.

The objective is to overhaul this system by assessing existing architecture, developing a forward-looking roadmap, and integrating modern technologies across core, cloud, and edge environments. The goal is to field a secure, scalable, and purpose-built IT infrastructure that enables data-driven, globally maneuverable airpower for modern joint warfare.

The Challenge: Critical Infrastructure Vulnerabilities

The IT infrastructure currently supporting AMC bases suffers from several critical vulnerabilities that directly impact mission readiness:

- **Operational Inefficiency:** Aging hardware and antiquated software result in slow performance, frequent outages, and an unsustainable maintenance burden, diverting critical resources from mission-focused activities.
- **Limited Data Sharing:** The lack of secure, accredited cross-domain solutions prevents the seamless flow of critical data between NIPRNET, SIPRNET, and other partner networks, hindering joint operational planning and execution.
- **Poor Scalability and Resilience:** The rigid, on-premises infrastructure cannot scale to meet new mission demands, surge capacity, or ensure rapid recovery from disruptions.
- **Degraded Warfighter Effectiveness:** These combined limitations create a slow and siloed system, directly impeding the rapid, data-driven decision-making essential for projecting modern airpower.

Detailed Scope of Work, Submission & Evaluation Process

The selection process will occur in two steps. Offerors are responsible for monitoring SAM.gov for any amendments to this solicitation.

Step One: White Paper Submission

Submission Details & Deadlines:

- **Questions Due Date:** No later than 10 April 2026, at 14:00 CST.
    - Q&A Matrix will be posted on the 10th following the question deadline with answers to outstanding questions.
        - Q&A Matrix will be posted once the Acquisition Strategy is determined (due to potential changes resulting from questions received during Q&A period).
- **White Paper Due Date**: On or before 12 May 2026, at 14:00 CST.
    - White Paper due date was extended after some changes brought about by the questions during the Q&A period.
- **Submission POC**:
    - **Contracting/Agreements Officer**: Lisa Pendragon (lisa.pendragon@us.af.mil)
    - **Contract/Agreements Specialist**: Elijah Dodd (elijah.dodd@us.af.mil)

White Paper Content & Technical Approach:

- **Section A: Title Page & Company Information**
    - Project Title / Title of the Submission.
    - Company Name, Business Size, CAGE number, and UEI number.
    - Points of Contact for contracting and technical matters (Name, Title, Date, E-Mail, Phone, Address).
    - A list of any subcontractors or additional team members.
    - An abstract providing a concise description of the approach.
- **Section B: Technical Solution & Approach Narrative**
    - A description of how your concept uniquely and innovatively meets the requirements detailed in the "Detailed Scope of Work & Technical Requirements" section.
    - Describe the background, objectives, technical methodology, and resources needed for the solution proposed in the White Paper.

    - Include the nature and extent of the anticipated results.
    - Detail any potential ancillary issues such as certifications, algorithms, or specific engineering/software development methodologies to be used.
    - Provide a Statement of Work (SOW) and a detailed project schedule. You may refer to the White Paper but should not duplicate its content.
- **Section C: Government Support Required**
    - Identify the type of support, if any, requested from the Government, such as facilities, equipment, data, or other materials.
- **Section D: Total Project Price**
    - Propose a total price and provide supporting data (e.g., commercial price catalogs) to help the Government determine a fair and reasonable price.
        - A Rough Order of Magnitude (ROM) will suffice for the purposes of Step One.

(White Papers shall not exceed 10 pages OR 15 slides excluding title page/slide and table of contents. Font shall be 12 pt Times New Roman. Pricing information and data is included in this page count. Title page, table of contents, SOW and detailed project schedule are excluded from the page limitation)

White Paper Evaluation:

White Papers will be evaluated and categorized as either **Selectable** (recommended to advance) or **Not Selectable**.

Step Two: Detailed Approach (By Invitation Only)

Companies whose White Papers are deemed "Selectable" will be invited to submit a fully written Detailed Approach. Companies are encouraged to discuss ideas and details with the Government during the writing process. The Government will provide information on equipment and software needed to complete step two as applicable.

Step Two – Detailed Approach:

After White Paper evaluation(s), selected offerors will be invited to design and implement a solution for AMC's IT challenges for step two. Air Force subject matter experts (SMEs) will be

available for consultation. The proposed solution must provide a detailed technical approach that meets or exceeds the following requirements:

Travel Assumption:

- For evaluation purposes only, assume one person travelling to **two** of the locations listed in "Location of Work" section down below and indicate which two were selected in your proposal. Price each trip at 2 weeks, including Air Fare, Lodging, etc.

A. Assessment & Analysis Methodology:

- Describe the technical approach for conducting a comprehensive assessment of the existing IT infrastructure at two representative AMC installations.
- This must include a detailed methodology for evaluating legacy systems to identify specific operational inefficiencies, performance bottlenecks, and security vulnerabilities.
- Proposals must specify the tools, diagnostic techniques, and personnel expertise that will be used to map the current "as-is" architecture and operational workflows.
- Explain how findings will be analyzed and documented to establish a clear performance and security baseline for the transition roadmap.

B. Proposed Future State Architecture:

- Present a high-level concept for the target "to-be" architecture that is secure, scalable, and resilient. This design must encompass core data centers, edge computing environments, and cloud components (hybrid and/or multi-cloud).
- Specifically address the approach for implementing a secure and accredited Cross-Domain Solution (CDS) to enable seamless data exchange between NIPRNET, SIPRNET, and other required domains.
- Describe the strategy for migrating legacy applications and on-premises data to the proposed modernized environment while ensuring mission continuity and adhering to strict cybersecurity requirements.

C. Transition & Implementation Roadmap:

- Provide a notional, phased transition roadmap that logically sequences key activities, including pilot programs, testing, and phased installation across AMC sites to minimize operational disruption.
- The roadmap must identify major proposed milestones, critical dependencies between tasks, and key go/no-go decision points for each step.

- Define the key performance indicators (KPIs) and metrics that will be used to measure the success and effectiveness of the modernization effort at each stage.
- Include a detailed updated Statement of Work (SOW) identifying all work to be performed, key deliverables, and a project schedule outlining all phases of work.
    - Updated version of step one SOW with any new information learned or provided during step two.

D. Core Technical Capabilities & Approach:

- Detail corporate experience and the proposed approach for executing key technical functions, including:
    - **System Integration:** Integrating diverse, multi-vendor hardware, software, and cloud services into a cohesive, manageable system.
    - **Network Design:** Designing and implementing modern, resilient network architectures based on principles such as Zero Trust and Software-Defined Networking (SDN).
    - **Multi-Solution Testing:** Establishing a test and evaluation environment to validate integrated solutions and de-risk large-scale deployments.
    - **Large-Scale Installation:** The project management and logistical approach for deploying the approved solution across multiple geographically dispersed CONUS and OCONUS installations.

E. Cybersecurity & Compliance Framework:

- Demonstrate a robust understanding of DoD cybersecurity requirements by describing the approach to:
    - **Risk Management Framework (RMF):** The methodology for developing and delivering the necessary documentation to support the Assessment and Authorization (A&A) process and achieve an Interim Authority to Test (IATT).
    - **Cybersecurity Supply Chain Risk Management (C-SCRM):** The processes used to ensure full traceability of all hardware and software components and to verify compliance with the Trade Agreements Act (TAA).
    - **Classified Operations:** The technical and procedural controls that will secure the infrastructure and manage data at the NIPRNET and SIPRNET classification levels.

Detailed Approach Evaluation:
Proposals will be evaluated on **Technical Merit**, **Importance to Agency**, and **Price**. All factors

are of equal importance. They will be categorized as **Acceptable** (recommended for funding) or **Not Acceptable**.

Contract Administration & General Information

- **Funding:** The Government will review responses and seek funding for the most innovative and affordable solutions. All awards are subject to the availability of funds.
- **Pricing Strategy:** Any resulting award will be a firm-fixed-price contract subject to RFO FAR 12.205 *Solicitation provisions and contract clauses*.
- **Security Requirements:** Offerors will require access to classified information up to the SECRET level. All personnel must have a minimum of a Tier 3 Security Investigation with "SECRET" eligibility and be enrolled in Continuous Vetting within 30 days of award. A "SECRET" facilities clearance is required for this effort.
- **Location of Work:** Work will primarily be performed at government-furnished facilities at AMC installations. Contract management will be conducted at the offeror's facility. Travel may be required to the following locations:
    - **Joint Base McGuire-Dix-Lakehurst, NJ**
    - **Joint Base Charleston, SC**
    - **Pope Army Airfield, NC**
    - **Travis AFB, CA**
    - **Scott AFB, IL**
    - **Joint Base Pearl Harbor-Hickam, HI**
    - **Ramstein AB, Germany**
    - **Little Rock AFB, AR**
    - **Joint Base Lewis-McChord, WA**
    - **Joint Base Andrews, MD**
    - **Dyess AFB, TX**
    - **Dover AFB, DE**
    - **MacDill AFB, FL**
    - **McConnell AFB, KS**
    - **Fairchild AFB, WA**

Attachments:

Attachment 1 - Q&A Matrix – With Answers Provided