Note: the links and images in this document may point to external sources. Please review them before opening.

REQUEST FOR INFORMATION (RFI)

US Air Force Weather (AFW) Cloud Enterprise Operations and Modernization

1.0 Description

AFLCMC/ESAW (Weather Program Office) is seeking information on how an interested contractor could help operate, sustain, and modernize the USAF Weather (AFW) Cloud agile and secure operational information ecosystem for a future contract.

THIS IS A REQUEST FOR INFORMATION (RFI) ONLY. This RFI is issued solely for information and planning purposes – it does not constitute a Request for Proposal (RFP) or a promise to issue an RFP in the future. This RFI does not commit the Government to contract for any supply or service whatsoever. Further, the Air Force is not at this time seeking proposals and will not accept unsolicited proposals. Respondees are advised that the U.S. Government will not pay for any information or administrative costs incurred in response to this RFI; all costs associated with responding to this RFI will be solely at the interested party's expense. Not responding to this RFI does not preclude participation in any future RFP, if any is issued. If a solicitation is released, it will be synopsized on the SAM.gov website. It is the responsibility of the potential offerors to monitor this site for additional information pertaining to this requirement.

2.0 Background

AFW operates and modernizes a Department of War enterprise weather cloud, currently AWS-based, to deliver timely, accurate, and relevant weather and weather impacts services across three security enclaves (Unclassified, Secret, Top Secret). Utilizing fixed and tactical atmospheric sensing equipment around the globe, the AFW Enterprise outputs 600 TB of data daily from the High-Performance Computing system, and nearly 6PB of data annually, that are used to produce

weather information to include forecasts, climatology, mission support, and operations impacts for any National security interests at any time.

Fundamentally, our goal is to transform current cloud-based weather forecast and information processes and associated data flows. This involves ingesting vast amounts of world-wide environmental data, processing it using High-Performance Computing (HPC) and Artificial Intelligence (AI), and delivering decision-quality weather intelligence to end-users through intuitive applications. This entire process must operate seamlessly and securely across multiple security enclaves, from Unclassified to Top Secret/SCI. Access will be provided by the Government to consumption services for Secret and Top Secret systems that allow contractors to access and operate for the Government from any location.

Our approach will be grounded in agile methodologies, including the Scaled Agile Framework (SAFe®), to ensure we can "pay down technical debt" and continuously modernize the weather cloud enterprise. We intend to incorporate AI everywhere, not as a separate feature, but as a foundational element of our data processing, analytics, and operational management.

The RFI requirements are structured into six distinct sections, each representing a group of interrelated tasks. While these sections are designed to be independent enough that different vendors could potentially perform the work—allowing the government to define and manage workloads—it is critical that respondents understand the interrelated nature of these tasks. Success will require deep collaboration and integration across all areas.

2.1 **Limitations:** The scope is divided into six distinct sections representing interrelated tasks. Success will require deep collaboration and integration across all areas.

- **Security Requirements:** The solution must operate seamlessly and securely across multiple security enclaves, from Unclassified to Top Secret/SCI. Currently, the contractor will be responsible for managing the Risk Management Framework (RMF) process to achieve and maintain Authority to Operate (ATO) and Continuous ATO (CATO), but these solutions must be postured to meet future policy and strategy initiatives, such as Zero Trust.

3.0 Requested Information

The following sections provide a breakdown of the effort required to operate and modernize the AFW Enterprise. All sections are necessary to meet AFW

requirements. However, the Government recognizes that allowing interested parties to respond to individual sections may bring greater expertise to each section. Interested parties can respond to single sections, or to any combination of sections, including the entire RFI. The Government expects to hold the Lead System Integrator (LSI) role, but does not insist on it.

Whoever holds the LSI role, it must be emphasized that coordination is paramount between sections for tasks performed. Changes in any section can have significant impacts on many other sections. Configuration management, joint use of tools and workspaces and constant communication must be standard operating procedures.

3.1 Task Sections

For each section below, the RFI indicates the key tasks that have been identified, as well as questions as a starting point. Interested parties should feel free to add to these tasks any items that the Government may want to consider.

Section A: Infrastructure as a Service (IaaS)

This section focuses on the foundational compute, storage, and networking infrastructure required to support all higher-level platform and software services. This includes provisioning, managing, and designing the core infrastructure.

- **Key Tasks:**
  - Provisioning and managing IaaS across multiple security enclaves.
  - Ensuring unclassified, classified and top secret enclaves have Continuity of Operations (COOP) and Return to Service (RTS) capabilities, including help desk support.
  - Implementing automation for infrastructure deployment and management.
  - Utilizing Artificial Intelligence for management, implementation and automation.
  - Providing access to and management of High-Performance Computing (HPC) resources (both classified and unclassified).
  - Establishing and managing secure connections to external organizations.
  - Maintaining Production, Test, Staging, and Development environments.
  - Monitoring, managing, and reporting on infrastructure health and performance.
  - Providing cost and utilization break downs to the project level.
- **Questions for Section A:**
  - **A.1.** Describe your experience provisioning and managing IaaS in a multi-enclave environment (Unclassified, Secret, TS/SCI). How do you ensure separation while enabling secure cross-domain data flow where required?

- **A.2.** What is your approach to infrastructure automation and managing Infrastructure as Code (IaC)?
- **A.3.** Describe your experience managing both on-premise and cloud-based HPC resources.
- **A.4.** Where would you incorporate AI to improve operations and management?
- **A.5.** What is your approach to RTS standards and uptime criteria for foundational IaaS, to include 24/7 help desk support in all 3 enclaves, and how would you monitor, correct, and report on these metrics?

Section B: Platform as a Service (PaaS)

This section focuses on providing and managing the platform layer that enables the development and operation of government-owned or third-party web applications and Software as a Service (SaaS).

- **Key Tasks:**
  - Providing and managing Identity and Access Management (IDAM) solutions.
  - Managing software licenses for platform-level tools.
  - Utilizing AI for management, implementation and automation.
  - Establishing and managing secure machine-to-machine connections and APIs.
  - Ensuring unclassified, classified and top secret enclaves have Return to Service (RTS) capabilities, including help desk support.
  - Maintaining Production, Test, Staging, and Development environments for applications.
  - Monitoring, managing, and reporting on platform health and application performance.
  - Providing cost and utilization break downs to the project level.
- **Questions for Section B:**
  - **B.1.** Describe your experience providing PaaS solutions that have hosted government-developed or COTS applications.
  - **B.2.** How do you approach IDAM and license management for a large, enterprise-level PaaS environment?
  - **B.3.** What is your strategy for enabling secure, reliable machine-to-machine connections for data exchange between applications and external partners?
  - **B.4.** Where would you incorporate AI to improve operations and management?

- **B.5.** What are your proposed RTS standards and uptime criteria for a PaaS environment supporting critical applications, to include 24/7 help desk support in all 3 enclaves?

Section C: SaaS, DevSecOps, & Other Software

This section focuses on the development, integration, and management of Software as a Service (SaaS) and other software applications, with a strong emphasis on leveraging DevSecOps to manage and reduce technical debt.

- **Key Tasks:**
  - Implementing and managing a robust DevSecOps framework.
  - Integrating and managing third-party SaaS solutions, particularly for weather and meteorological cloud operations.
  - Utilizing AI for improved capability, implementation and automation.
  - Developing, integrating, or managing weather/meteorological software applications for private, commercial, and government operations use.
  - Developing and sustaining custom software applications.
  - Supporting the transition of applications to full-time operations.
  - Provide artifacts necessary to meet cybersecurity requirements, including Certificates to Field (CtF).
  - Supporting connected and disconnected (DDIL) operations.
- **Questions for Section C:**
  - **C.1.** Describe your proven methodology for establishing and managing a mature DevSecOps pipeline for a DoD program. Describe your approach and experience with applications and data version management.
  - **C.2.** How would you approach the integration of a commercial SaaS product into a government system, ensuring it meets all security and data handling requirements?
  - **C.3.** Describe your company's experience with weather or meteorological cloud operations. Detail any software applications you have developed, integrated, or managed for private, commercial, or government use.
  - **C.4.** Where would you incorporate AI to improve capabilities and maintenance?
  - **C.5.** What are your proposed RTS standards and uptime criteria for a PaaS environment supporting critical applications, to include 24/7 help desk support in all 3 enclaves?
  - **C.6.** Describe your experience developing or managing software that must operate in DDIL environments.

Section D: Cybersecurity

This section focuses on all aspects of cybersecurity, from achieving initial authorizations to continuous monitoring and defense. All Department of War standards and initiatives must be met, even as policy and requirements are changed.

- **Key Tasks:**
  - Managing the full lifecycle of the Risk Management Framework (RMF) process to achieve and maintain Authority to Operate (ATO) and Continuous ATO (cATO).
  - Implementing and managing CtF processes and coordination.
  - Streamlining cybersecurity processes and interactions with Air Force and Intelligence Community (AF IC) stakeholders.
  - Meeting current and impending cybersecurity initiatives, such as Zero Trust.
  - Incorporating lessons learned from past cybersecurity challenges.
- **Questions for Section D:**
  - **D.1.** Describe your experience and strategy for achieving a CATO for a complex system operating across multiple enclaves.
  - **D.2.** How do you propose to streamline interactions with AF IC entities for cybersecurity and authorization activities?
  - **D.3.** Where would you incorporate AI to improve security, operations and management?
  - **D.4.** Provide an example of a significant cybersecurity "lesson learned" from a past program and how you would apply that lesson to this effort.

Section E: Architecture and Design

This section focuses on the overall system architecture, data flow design, and user experience, emphasizing a Modular Open Systems Approach (MOSA).

- **Key Tasks:**
  - Developing and enforcing a MOSA-compliant digital architecture.
  - Designing and managing data flows and potential middleware solutions.
  - Integrating new capabilities with existing DoD C2 and mission planning systems, with a focus on the VAULTIS architecture.
- **Questions for Section E:**
  - **E.1.** Describe your experience developing and enforcing a MOSA-based digital architecture for a major DoD program.
  - **E.2.** Specifically detail your experience integrating new capabilities with existing DoD C2 or mission planning systems. Describe any experience you have with the VAULTIS architecture.

- **E.3.** What is your approach to data flow design in a multi-enclave system that needs to process and fuse data from unclassified, secret, and TS/SCI sources?

Section F: Digital Materiel Management/Digital Engineering

This section focuses on the digital engineering principles in the operation, management and enhancement of the AFW Enterprise. Digital Engineering enables the AFW Enterprise to respond quickly to changes in technology as well as extend capabilities in response to emerging requirements. The Government currently operates an Integrated Development Environment (IDE) based on Jira and Confluence, but is open to improved management methods.

- **Questions for Section F:**

  - **F.1. Infrastructure & Hosting:** Describe your company's capability to host, maintain, and architect an IDE that supports collaborative digital engineering. Do you primarily utilize commercial cloud environments (e.g., AWS, Azure), on-premise infrastructure, or hybrid models?
  - **F.2. Multi-Enclave Security:** How does your team manage collaborative engineering, data sharing, and model integration across multiple security enclaves (Unclassified, Secret, and TS/SCI)? What cross-domain solution (CDS) strategies or tools have you successfully implemented?
  - **F.3. Interoperability & Data Exchanges:** What is your approach to interfacing a contractor-managed IDE with Government-defined databases, Product Lifecycle Management (PLM) systems, or digital reference libraries? Detail your experience with automated data exchanges or synchronization.
  - **F.4. System Models:** What is your approach to using, extending, documenting and maintaining System Models?

3.2 Everything as a Service (XaaS) Integration and Management

The Government's intent is to move beyond traditional IaaS and PaaS procurement toward a consumption-based model for a wide array of capabilities. This includes, but is not limited to, Software as a Service (SaaS), Security as a Service (SecaaS), Identity as a Service (IDaaS), and Data Analytics as a Service. This section seeks to understand a vendor's capability to provide, manage, and integrate a diverse portfolio of "Everything as a Service" (XaaS) offerings.

- **Key Tasks:**
  - Identifying, planning and managing the transition from traditional Iaas/Paas to XaaS offerings.

    - Providing a managed service catalog or marketplace of approved XaaS offerings.
    - Identifying and vetting commercial or third-party XaaS solutions for mission suitability and technical feasibility.
    - Managing the integration of XaaS solutions into the Government's architecture, ensuring adherence to MOSA principles and interface standards.
    - Shepherding third-party XaaS offerings through the Government's security and authorization processes (e.g., RMF/ATO) to ensure they meet the required security posture for operation within Unclassified, Secret, and/or TS/SCI enclaves.
    - Managing the financial aspects of a consumption-based model, including cost monitoring, chargeback, and financial optimization.
    - Providing unified operational monitoring and reporting for the health, performance, and usage of all integrated XaaS offerings.
- **Questions for 3.2:**
- **XaaS Integration Experience:** Describe your experience acting as an "Everything as a Service" (XaaS) integrator for a U.S. Government or DoD customer. Please provide specific examples of the types of "as-a-service" offerings you have integrated (e.g., SecaaS, IDaaS, specific enterprise SaaS applications).
- **Security & Authorization Strategy:** What is your methodology for taking a commercial XaaS product and ensuring it can achieve a DoD Authority to Operate (ATO) at the required Impact Level? Describe your process for assessing a vendor's security posture and guiding them through the RMF process.
- **Consumption & Financial Management:** How do you propose to manage and provide transparency for the consumption and cost of a diverse portfolio of pay-as-you-go XaaS offerings? Describe any tools or processes you use for financial operations (FinOps), showback/chargeback, and cost optimization.
- **Service Catalog & Governance:** Describe your approach to creating and managing a unified service catalog of XaaS offerings. How would you govern the lifecycle of these services, from initial onboarding and integration to version updates and eventual retirement?
- **Return to Service:** Describe your methodology for designing and implementing a "Return to Service" plan for a fully integrated IaaS, PaaS, and SaaS stack. How do you manage and orchestrate recovery dependencies between these layers during a service disruption event? What is your approach to regularly testing and validating a full-stack recovery plan to ensure it meets defined RTO and RPO targets?

3.3 Scenario-Based Integration Question

- **Scenario:** A task order is issued requiring the integration of a new, government-owned operations weather impacts model into an existing DoD C2 mission planning system. The integration must follow a MOSA-compliant architecture (Section E). The NWP model will be hosted on a hybrid HPC environment (Section A) and must receive real-time data from a Top Secret/SCI cloud environment (Section A) that requires 24x7 operational monitoring. The entire software deployment and update process must be managed via a secure DevSecOps pipeline (Section C) and achieve a Continuous ATO (Section D).
- **Instructions:**
    1. Describe how your company, acting as the prime contractor, would approach the integration and management of this task order, touching on all relevant Sections.
    2. Identify the primary technical and programmatic risks you foresee and your strategies for mitigating them.

4.0 Responses

4.1 Interested parties are requested to respond to this RFI with a white paper structured into two separate sections as defined below.

4.2 White papers in Microsoft Word for Office 365 compatible format are due no later than **02 September 2026** at **17:00 ET**. Responses shall be submitted via e-mail only to Brett Maguire (brett.maguire@us.af.mil) with courtesy copies to Capt Christopher Thier (christopher.thier@us.af.mil) and Ashley Luck (ashley.luck@us.af.mil). Proprietary information, if any, should be minimized and MUST BE CLEARLY MARKED. To aid the Government, please segregate proprietary information. Please be advised that all submissions become Government property and will not be returned.

4.3 **Section 1 - Administrative & Corporate Information**
This section of the white paper shall provide administrative information and shall include the following as a minimum (drawn from standard corporate criteria and GSA structures):

- **4.3.1 Company Profile:** Company Name, primary Point of Contact (Name, Email, Phone), Company Website, Unique Entity ID (UEI), and CAGE Code.
- **4.3.2 GSA Contract Vehicles:** Identify all active GSA contracts or other pre-competed contract vehicles (e.g., IDIQs, GWACs) held by your company that are

applicable to this requirement:

- ( ) GSA Multiple Award Schedule (MAS)
- ( ) Alliant 2
- ( ) VETS 2
- ( ) Other(s): [Please specify]

- **4.3.3 Applicable SINs/Pools:** Based on the contracts your company holds, which SIN(s), Pool(s), or Constellation(s) would you recommend as applicable for this requirement?
- **4.3.4 Business Size & Socio-Economic Categories:**

  - Indicate business size: ( ) Large Business ( ) Small Business
  - Select all applicable socio-economic categories:

    - ( ) Small Disadvantaged Business (SDB)
    - ( ) Woman-Owned Small Business (WOSB)
    - ( ) Service-Disabled Veteran-Owned Small Business (SDVOSB)
    - ( ) HUBZone Small Business
    - ( ) Other: [Please specify]
  - *NAICS Code Reference:* Business type classification should be based upon NAICS code 518210, but please provide any other recommended NAICS codes. "Small business concern" means a concern, including its affiliates, that is independently owned and operated, not dominant in the field of operation in which it is bidding on Government contracts, and qualified as a small business under the criteria and size standards in 13 CFR part 121. Refer to Federal Acquisition Regulation (FAR) Part 19 for detailed information on Small Business Size Standards at Acquisition.gov.

- **4.3.5 Capability & Interest Matrix:** Complete the following table:

Inquiry	**Respondent Assessment (Yes/No/Comments)**
Does your company have the capability to perform all required services in the	

Draft Requirements document (Section 3.0)?	
Does your company have similar experience with the type of work outlined in the Draft Requirements document?	
Does the Draft Requirements document contain sufficient information that would allow you to adequately respond to an RFP?	
Based on the provided information, would your company submit a quote if this requirement was issued under your GSA Contract?	
Do you provide this service or product commercially?	

- **4.3.6 Lead Time:** How much lead time would your company need from notification of award to start of contract performance?

  - ( ) < 30 Days
  - ( ) 30-60 Days
  - ( ) 60-90 Days
  - ( ) > 90 Days
- **4.3.7 Subcontracting Estimation:** In your estimation, how much of this potential requirement would your company need to subcontract to other companies?

  - ( ) 0-25%
  - ( ) 26-50%
  - ( ) 51-75%
  - ( ) 76-100%
- **4.3.8 NDAs and Support Contractors:** Provide either:

3. Copies of executed non-disclosure agreements (NDAs) with the contractors supporting AFLCMC/ESAW in technical evaluations, or
4. A statement that the responder will not allow the Government to release its proprietary data to Government support contractors.

- *Note:* In the absence of either of the foregoing, the Government will assume that the responder does NOT agree to the release of its submission to Government support contractors.

- **4.3.9 Security Clearance:** State the facility security clearance of the offeror.
- *Note: The page count for Section 1 response elements does not count toward the Section 2 technical page limits.*

4.4 **Section 2 - Technical Capability Responses**

- Section 2 of the white paper shall answer the technical issues and scenarios addressed in Section 3.0 of this RFI and shall be limited to 20 pages.

5.0 Industry Discussions

AFLCMC/ESAW 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 certification risks.

6.0 Questions

Questions regarding this announcement shall be submitted in writing by e-mail to the Contracting Officer at Brett Maguire (brett.maguire@us.af.mil) with courtesy copies to Capt Christopher Thier (christopher.thier@us.af.mil) and Ashley Luck (ashley.luck@us.af.mil). Verbal questions will NOT be accepted. Questions will be answered by posting answers to the Government Point of Entry website; accordingly, questions shall NOT contain proprietary or classified information. The Government does not guarantee that questions received after **28 August 2026** at **17:00 ET** will be answered.

7.0 Summary

THIS IS A REQUEST FOR INFORMATION (RFI) ONLY to identify sources that can provide USAF Weather (AFW) Cloud enterprise agile operations, sustainment, and modernization. The information provided in the RFI is subject to change and is not binding on the Government. The Air Force has not made a commitment to procure any of the items/services discussed, and release of this RFI should not be construed as such a commitment or as authorization to incur cost for which reimbursement would be required or sought. All submissions become Government property and will not be returned.