21 Apr 26

MEMORANDUM FOR NAICS CODE 332710 – MACHINE SHOPS

FROM: AFMC/AFTC/PZIA (Arnold)
100 Kindel Drive
Arnold AFB, TN 37389-1332

SUBJECT: Request for Whitepaper: Arc Heater Component Manufacturing and Supply

1.0 Introduction and Purpose
The Arnold Engineering Development Complex (AEDC) requires a long-term, sustainable source for the manufacture and/or refurbishment of critical components for its Arc Heater test facilities to support Department of War (DoW) objectives.

The purpose of this Request for Whitepaper is to solicit a response from the vendor to establish the framework for a ten (10) year strategic agreement under the authority of 10 U.S.C. § 4022 (Other Transaction Authority for Prototype Projects). The entirety of this agreement will be executed under the prototype operational utility phase through yearly milestones (Year 1 through Year 10). When specific component orders are required, a modification will be issued to the corresponding yearly milestone to add a sub-milestone for that particular order. This RWP seeks to finalize the vendor's approach to intellectual property and statutory compliance, and to formalize the proposed business and pricing structure.

While this agreement establishes a ten-year ordering framework, it is intended to foster a resilient industrial base. The Government reserves the right to onboard additional vendors at any point during the period of performance. Should other qualified sources emerge, they may be added to the agreement to compete for future component orders.

2.0 Problem Statement
The Arc Heaters operate under extreme conditions, leading to a high consumption rate of specialized components. The consistent availability of these parts is paramount to meeting the high-demand testing schedule at AEDC. The Government requires a reliable partner that can produce parts in strict accordance with the Government-owned Technical Data Package (TDP), manage a complex supply chain, and maintain rigorous quality standards over a ten-year period.

3.0 Instructions for Vendors Whitepaper Response
Vendors shall submit a whitepaper, not to exceed ten (10) pages, addressing the following three parts.

Part 1: Business Process Prototype
The vendor's response to this section shall constitute the Business Process Prototype as defined in this RWP. In this section, the vendor shall provide the following components to formalize the business relationship and pricing structure:

- Manufacturing and Quality Process: A comprehensive description of the end-to-end manufacturing and quality assurance processes that will be employed to produce and deliver components in accordance with the TDP.

- 5-Year Pricing Structure: Firm-Fixed Pricing for all parts listed in the associated Statement of Objectives (SOO) for the first five (5) years of the agreement. Pricing for years 6 through 10 will be negotiated prior to the end of year 5 of the agreement.

Part 2: Intellectual Property (IP) Rights

The Intellectual Property (IP) terms for this agreement shall be based on the following framework. The vendor's response shall acknowledge this structure and must identify, with supporting rationale, any assertions to restrictions on technical data in an attached document. As no software is being delivered under this project, the IP terms do not extend to software or software licenses.

- Background IP: All technical data developed exclusively at private expense and not first produced, conceived, or reduced to practice in the performance of this agreement shall be considered Background IP. Ownership of Background IP remains with the originating party.
- Foreground IP: All technical data first produced, conceived, or reduced to practice in the performance of this agreement shall be considered Foreground IP. This explicitly includes technical data delivered as part of the Business Process Prototype in Part 1. For all Foreground IP, the Government shall receive, at a minimum, Government Purpose Rights (GPR). Government Purpose Rights are defined as the rights to use, modify, reproduce, release, perform, display, or disclose technical data within the Government without restriction; and to release or disclose such technical data outside the Government and authorize persons to whom release or disclosure has been made to use, modify, reproduce, release, perform, display, or disclose that data for any United States Government purpose.
- Data Marking: All technical data provided with less than unlimited rights must be marked in accordance with the guidance in the forthcoming agreement articles. Failure to mark data will be treated as an unlimited rights deliverable.

Part 3: 10 U.S.C. 4022(d) Appropriate Use of Authority

The vendor shall specify and provide supporting documentation justifying how their company plans to satisfy 10 U.S.C. 4022(d)(1)(A)-(C) by elaborating on one of the specified options (Nontraditional participation, Small Business participation, or Cost-Sharing).

(A) There is at least one nontraditional defense contractor or nonprofit research institution participating to a significant extent in the prototype project.

(B) All significant participants in the transaction other than the Federal Government are small businesses (including small businesses participating in a program described under section 9 of the Small Business Act (15 U.S.C. 638)) or nontraditional defense contractors.

(C) At least one third of the total cost of the prototype project is to be paid out of funds provided by sources other than the Federal Government.

NOTE 1: Non-Traditional Defense Contractor (NDC) = An entity that is not currently performing and has not performed, for at least the one-year period preceding the solicitation of sources by DoD for the procurement or transaction, any contract or subcontract for the DoD that is subject to full coverage under the cost accounting standards (CAS) prescribed pursuant to section 1502 of title 41 and the regulations implementing such section (see 10 U.S.C. §3014). The phrase "the solicitation of sources" refers to the initial agreement solicitation only. A nontraditional defense contractor is considered a nontraditional defense contractor for the duration of the prototype project/agreement's period of performance, or for any in-scope work modified under the same agreement.

NOTE 2: Non-profit research institution is validated by reviewing the vendor's 501(c)(3) tax-exempt status, which is required by the Internal Revenue Service.

NOTE 3: "Significant extent" and "significant participants" may be defined by the vendor providing rationale to one or more of the following variables:

a. Has a significant role / level of involvement in the development, production, or delivery of a product or service.
b. Has a significant impact on the design, development, or production of the product or service.
c. Has a significant level of material interest in the success of the product or service.
d. Has significant level of company's financial interest in the success of the product or service.
e. Has significant level of control over the development, production, or delivery of a product or service.
f. Other significant rationale provided by the vendor.

NOTE 4: Failure to provide supporting documentation may eliminate a company from being considered for an award.

Part 4: Cybersecurity Compliance Plan

The Technical Data Package (TDP) and associated technical data for this project are Controlled Unclassified Information (CUI), marked as Distribution D (DoD and DoD Contractors Only), and are subject to U.S. export control laws. As a condition of award, the vendor must demonstrate compliance with the following mandatory security and cybersecurity requirements.

In this section of the whitepaper, the vendor shall address both Criterion 1 and Criterion 2:

- **Criterion 1:** Joint Certification Program (JCP)
  The vendor must explicitly state that they hold a current and valid certification under the United States/Canada Joint Certification Program (JCP). The Government will validate this certification via the Defense Logistics Agency (DLA).

- **Criterion 2:** Cybersecurity Maturity Model Certification (CMMC)
  The vendor must address one of the following two compliance paths:
  - **(A) Current CMMC Level 2 C3PAO Certification:** If the vendor currently possesses a CMMC Level 2 Certification Assessment conducted by an authorized Certified Third-Party Assessment Organization (C3PAO), state this and confirm the certification is active. *(Note: A CMMC Level 2 Self-Assessment does not satisfy this condition).* The Government will validate this status.

  - **(B) Alternative Compliance Path:** If the vendor does not yet possess a full CMMC Level 2 C3PAO Certification, they must provide the following two elements:
    1. NIST SP 800-171 Assessment: Confirmation that a current (no older than three years) NIST SP 800-171 DoD Assessment is posted in the Supplier Performance Risk System (SPRS). The Government will validate this posting.

    2. CMMC Roadmap: A detailed compliance roadmap detailing the specific steps, milestones, and timeline the company will follow to achieve full CMMC Level 2 C3PAO Certification by the mandatory 10 November 2026 deadline. To be deemed sufficient, this roadmap must specifically address:
       - The timeline for closing out any open Plans of Action and Milestones (POA&Ms) to achieve full implementation of the 110 controls, acknowledging the strict 180-day limitation on POA&Ms under the CMMC rule.

- The vendor's planned timeline and evidence of engagement with a C3PAO to conduct the final certification assessment prior to the November 2026 deadline.

4.0 Whitepaper Evaluation Criteria

The Government will evaluate the whitepaper submission to confirm its suitability for establishing the long-term agreement. The evaluation will be based on the following criteria:

1. Clarity and Suitability of the Proposed Business Process Prototype: The degree to which the vendor's described manufacturing/quality processes and 5-year pricing structure are clear and comprehensive. The pricing for the first 5 years must be determined fair and reasonable by the Agreements Officer prior to award.
2. Acceptance of IP Terms: The vendor's acknowledgement of the IP framework and the justification for any asserted restrictions.
3. Compliance with 10 U.S.C. § 4022(d): The vendor's clear and satisfactory explanation, with supporting documentation, of how they meet the statutory requirements for participation.
4. Cybersecurity Compliance Approach: The vendor's submission will be evaluated on its ability and approach to meeting the mandatory security and cybersecurity requirements for handling Distribution D export-controlled technical data.
    - JCP Certification: The evaluation will include Government validation of the vendor's active Joint Certification Program (JCP) status.
    - CMMC Level 2 C3PAO Certification: If the vendor claims a current CMMC Level 2 C3PAO Certification, the evaluation will consist of Government validation of that status.
    - Alternative Compliance Path (Roadmap): If the vendor relies on the alternative path, the evaluation will assess the credibility and realism of the roadmap to achieve full CMMC Level 2 C3PAO Certification by the 10 November 2026 deadline. This assessment will specifically evaluate:
        - Government validation of the required NIST SP 800-171 assessment in SPRS (no older than three years).
        - The feasibility of the vendor's timeline to close out any open Plans of Action and Milestones (POA&Ms), acknowledging the strict 180-day limitation.
        - The realism of the planned timeline and provided evidence of engagement with an authorized C3PAO to conduct the final certification assessment prior to the deadline.

5.0 Successful Prototype Definitions

For the purposes of this effort, a successful prototype is defined by the following two elements:

- **Definition 1: Business Process Prototype:** A successful prototype is the formal establishment of the business relationship. This is achieved through the vendor's whitepaper submission, which will clearly explain its manufacturing/quality processes and provide the Government with Firm-Fixed Pricing for all parts listed in the SOO for the next five (5) years. This submission itself constitutes the business process prototype.

- **Definition 2: Proof of Concept (POC) Prototype:** For new vendors who submit a Business Process Prototype that the Government deems credible, the Government may, at its discretion, request the vendor to produce a Proof of Concept (POC) to validate their asserted capabilities. A successful POC is defined as the manufacture and delivery of a representative component which is

subsequently verified through Government inspection and acceptance to be in strict conformance with the Government-provided Technical Data Package (TDP).

- **Definition 3: Operational Utility Prototype:** A successful prototype is the ongoing delivery of manufactured components that provide direct operational utility to the DoW throughout the life of the agreement. Operational utility, within the Department of War, refers to the degree to which a system, weapon, technology, capability, or process contributes to the successful completion of military missions and objectives within the operational environment. It encompasses mission effectiveness, integration, logistics, cost-effectiveness, and adaptability within the completed deliverable, which ultimately contributes to the lethality of the Department of War.

6.0 Submission Details
Whitepapers must be submitted electronically to the Agreements Officer, Greggory C. Jones, at greggory.jones.4@us.af.mil. The whitepaper submission shall not exceed 10 pages in length.

A. Submission Deadline for Known Capable Source
Market intelligence confirms that Neodora, LLC is currently the only known and proven vendor with the unique capabilities required to meet the entirety of this project's requirements. Therefore, the submission from Neodora, LLC is due no later than **21 May 2026, Close of Business (COB)**.

B. Ongoing Opportunity for Additional Vendors
To ensure competitive procedures are used to the maximum extent practicable over the life of this ten-year effort, this Request for Whitepaper will remain open after the initial submission deadline. This provides an ongoing opportunity for other vendors to prove their capabilities.

Any interested vendor may submit a whitepaper in accordance with the instructions herein at any time. If the Government reviews a submission and finds validity in the vendor's asserted capabilities, the Government may, at its discretion, initiate additional communications with that vendor to further validate their actual production capabilities, which may include a request for a formal technical and manufacturing audit. This process may lead to the onboarding of additional qualified vendors to compete for future orders under this agreement.

7.0 Attachments
Atch 1 - 13591-26-001 Arc Heater Component Manufacturing SOO-Distro D Export Controlled.pdf
Atch 2 - Arc Heater Component Projection-FY26-FY30
Atch 3 - Arc Heater Component Drawings-Distro D Export Controlled.pdf
Atch 4 - Arc Heater Component Manufacturing and Supply-Articles.pdf

Vetting Criteria for Release of Controlled Technical Documents
1.0 Purpose
The Technical Data Package (TDP), Statement of Objectives (SOO), and other attachments associated with the Arc Heater Component Manufacturing and Supply requirement are designated as Distribution D (DoD and DoD Contractors Only) and are subject to U.S. export control laws. Unauthorized access or distribution is prohibited.

Therefore, any vendor must be vetted and confirmed to meet all of the following criteria prior to receiving the controlled technical documents.

2.0 Mandatory Vetting Criteria

The Government shall verify that the requesting vendor meets the following two mandatory criteria before releasing the controlled documents:

- **Criterion 1: Joint Certification Program (JCP) Certification**
  - Requirement: The vendor must possess a current and valid certification under the United States/Canada Joint Certification Program (JCP).
  - Verification: The Government will validate the vendor's active DD Form 2345 status using the official Defense Logistics Agency (DLA) search tool.

- **Criterion 2: Cybersecurity Compliance for CUI**
  - Requirement: The vendor must demonstrate the capability to protect Controlled Unclassified Information (CUI). This shall be verified by confirming one of the following conditions:
    - (A) CMMC Level 2 C3PAO Certification: The vendor has a current Cybersecurity Maturity Model Certification (CMMC) Level 2 assessment conducted by an authorized Certified Third-Party Assessment Organization (C3PAO). *(Note: A CMMC Level 2 Self-Assessment does not satisfy this condition).*

    - (B) NIST SP 800-171 Assessment: The vendor has a current (no older than three years) NIST SP 800-171 DoD Assessment posted in the Supplier Performance Risk System (SPRS). *(Note: Vendors utilizing this alternative path to receive the documents will be required to submit a detailed CMMC Level 2 C3PAO compliance roadmap as part of their formal whitepaper submission).*
  - Verification: The Government will validate the vendor's cybersecurity status and assessment dates directly within the Supplier Performance Risk System (SPRS).

3.0 Process

No vendor will be granted access to the controlled technical data package until a Government representative has successfully verified compliance with both Criterion 1 and Criterion 2. Failure to meet these mandatory prerequisites will preclude the vendor from receiving the Request for Whitepaper documents and participating further in this acquisition process.

GREGGORY C. JONES
Agreements Officer, USAF