Focused Interest Period – IT System Transformation (22 November2024 – 06 December 2024)

1.1. For the period of 22 November 2024 to 06 December 2024 Air Force CyberWorx has a focused interest in exploring methodologies, processes, and solutions in support of organizational process transformation in highly secure, and scalable multi and cross-domain environments.

1.2. Air Force Cyberworx will rely on process provided submitters to:

1.2.1. Assess current and proposed system architectures and operational process flows for operational and security optimization opportunities.

1.2.2. Develop proposals for innovative and transformative changes to combinations of policy, process, systems - IT architectures and integrations to maximize benefit from the identified opportunities.

1.2.3. Acquire and field new technologies and material solutions to implement and integrate approved proposals.

1.3. Initial use-case for proposal purposes is to evaluate the IT infrastructure at two Air Force installations, one on each coast of the United States (CONUS), identifying limiting factors and shortfalls in the operational support and security postures of the respective installations, and propose to-be architecture(s) maximizing operational capability and security posture, with a roadmap for upgrade/transition.

1.4. Submission guidelines

1.4.1. Follow same submission guidelines as outlined in the body of the CSO.

1.4.2. Vendor must have past experience and solutions developed and delivered under this effort will require the vendor to:

1.4.2.1. Demonstrate lead system integration capabilities utilizing industry best practices across both commercial, government and DoD IC communities.

1.4.2.2. Demonstrate engineering, design and architectural expertise in network creation and solutions.

1.4.2.3. Demonstrate multi-solution testing in a secure and remote access environment.

1.4.2.4. Performa installation, configuration, integration, and scaling for integration of multiple base-level environments supporting tens of thousands of users.

1.4.2.5. Develop Risk Management Framework Certification and Accreditation (C&A) services package elements in support of interim authorization to test (IATT).

1.4.2.6. Demonstrate Cybersecurity Supply Chain Risk Management (C-SCRM) process to ensure traceable custody of critical components from foundry to the tactical user; verifiable Original Equipment Manufacturer (OEM) reseller certification status and ability to meet Trade Agreements Act (TAA) requirements.

1.4.2.7. Perform work up to and including TS/SCI classification with access to Special Access Programs.

1.5. Response timelines

1.5.1. Submissions during the focused period of interest will receive an initial confirmation of receipt from the contracting officer. Final evaluation feedback and potential requests for follow-up (Phase II) pitches will be released in the first week following the end of the focused interest period.