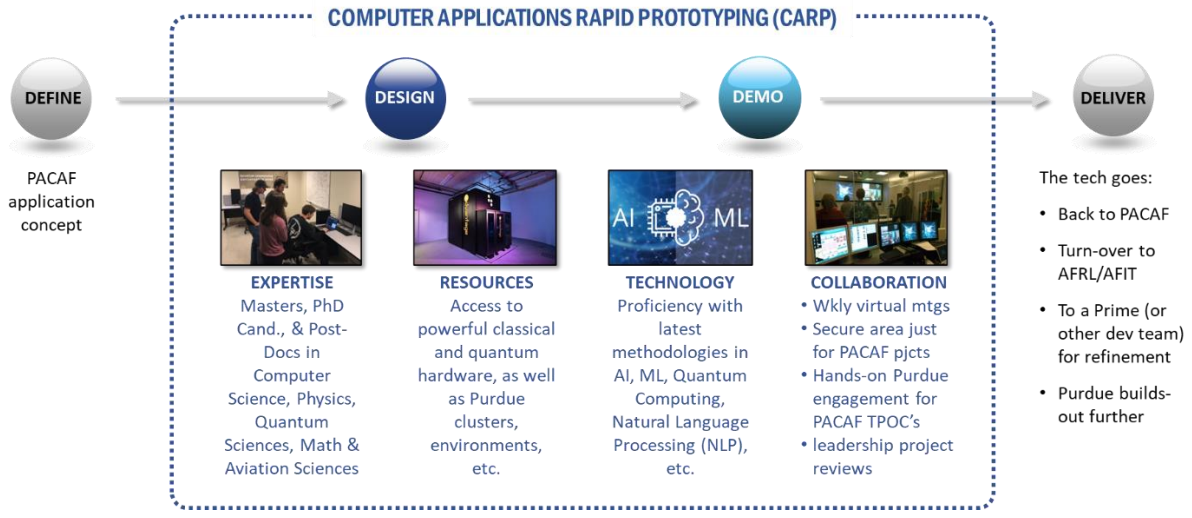
Computer Applications Rapid Prototyping (CARP)
Performance Work Statement (PWS)
September 3, 2024

1. GENERAL INFORMATION

A. **Introduction**. This effort will leverage one of the country's top coding teams to take 4 PACAF concepts per year and prototype/MVP them in less than 3 months each. This is a TRL 2 to TRL 6 "core" technology application using AI, ML, QC and other advanced coding methodologies.

B. **Background.** Applied research and advanced technology development on Machine Learning and Quantum Computing occurred in Contract # FA864919PA048, which was awarded under Small Business Technology Transfer (STTR) Phase I Open Topic Contract F19B-001-0054.

C. **Scope of Work.** Math, math models, algorithms and necessary programming for technology utilization will be applied to PACAF application concepts. Output will consist of Prototype/MVP applications that can be operationalized via a USAF approved U/I to PACAF users. See below figure for high-level development process.



D. **Applicable Documents**:

- Data.Gov
- System Award Management (SAM)
- DoD SAFE (Secure Access File Exchanger)
- DoD 5220.22-M: National Industrial Security Program Operating Manual (NISPOM)
- DoD SAFE (Secure Access File Exchange)
- Department of the Air Force Manual (DAFM) 23-122, 8/2/2022
- DAF Instruction (DAFI) 23-101
- DoDI 5000.0
- DoD Directive 8140.01
- DoD Manual 4140.01, Vol 2
- DoDI 4140.01
- DoD Manual 4140.01 Vol 1
- DoDI 5200.44
- AFI 63-150
- DoD Developer's Guidebook for Software Assurance (CMU/SEI-2018-SR-013)
- DoD Developer's Guidebook for Software Assurance (CMU/SEI-2018-SR013) Appendix F: Project Context Questionnaire
- CMU/SEI-2009-TR010, Secure Design Patterns
- DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks
- AFI 63-101/20-101, Integration Life Cycle Management, Section 6.9.2, Software Assurance
- NIST SP 800-161r1, “Cybersecurity Supply Chain Risk Management Practices For Systems and Organizations”, defines Cybersecurity Supply Chain Risk Management (C-SCRM)
- SP 800-160 Vol 1, “Systems Security Engineering” and SP 800-160 Vol 2, Revision 1 “Developing Cyber Resilient Systems: A Systems Security Engineering Approach.”
- NIST Special Publication (SP) 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
- Quantum Training Manual and User Troubleshooting Guide

2. WORK REQUIREMENTS

A. **Tasks.**

- Contactor shall convene on-site contract launch meeting with PACAF at PACAF, at Purdue, or virtually (using MS Teams).
- Contractor shall convene kick-off meeting for each individual project on-site at Purdue or virtually (using MS Teams).
- Contactor shall establish USAF accounts for independent and secure use of

technology (as required by the USAF).
- Contactor shall identify fast-track to initiate software installation on a PACAF or USAF end-user terminal.
- Customer shall download Contractor's program(s) to an operational computer after permissions are given from cybersecurity/information technology specialists.
- Contractor shall initiate IL5 Cybersecurity processes (if IL6 or higher is needed, additional costs may be considered).
- Contactor shall work with PACAF, USAF and/or other experts on software integration and software development, as needed.
- Contactor shall hold weekly working meetings with PACAF end user or other personnel.
- Contactor shall hold monthly leadership meetings with PACAF.
- Contactor in collaboration with the PACAF shall identify data sources and methods to be used to make queries.
- Contactor shall identify controls, testing methods and security needed for soft/hardware (functional and non-functional requirements).
- Contactor shall use/test/improve applications, collect feedback and improve end-users' experience.
- Contactor shall address soft/hardware (virtual and physical components) requirements and changes and integration to ensure PACAF user mission needs.
- Contractor shall implement existing USAF System Security Plan
- Contractor shall implement end of performance review.

B. **Deliverables.**

- Programs, coding and applications for each project
- Post Award, Project Contract launch meeting
- Project kick-off meetings
- Weekly Working Telecoms
- Monthly Leadership Meetings
- End of Performance Period project review
- System Security Plan (SSP)
- Non-Disclosure Agreements (NDAs)

3. SUPPORTING INFORMATION

A. **Security.**
- Physical Security: We have 2 offices. Office #1 is located within the Physics building on the Purdue University campus. The office has only one door, which is always locked. This office has computer access that is IL5 secure through the Purdue Weber Cluster. Office #2 is located near the Purdue campus and directly across from the local county courthouse. This building has only one door. The office has only one door, which is always locked. Access control is via employees being allowed in the office. There is 24x7 security camera monitoring

and a recorded video security system. There are no individual offices (it is open space) and well lit. No work higher than IL5 is conducted in the office. No computers or paperwork is left in the office unattended.

- Information Security: We use MFA, Password Management, Firewalls and VPN encryption. IL5 work only occurs via the Purdue secure system. The following docs are on file:

  1. System Security Plan (SSP)
  2. Incident-Handling Capability Plan (IHCP)
  3. Incident Response Plan (IRP)
  4. Cybersecurity Plan Of Action and Milestones (POA&M)
  5. Media Protection Plan
  6. Security Awareness and Training Plan
  7. Insider Threat Program (ITP) Management Plan
  8. Security Assessment and Authorization Plan

- Transmission/transportation of information: There will be no manual handling or shipping of data. Electronic transmission will be direct to a secure cloud environment from a secure device via the Purdue secure network.

- Disposal and destruction of information: Data will only be stored in a cloud-based folder. No paper or disc data is anticipated, but if so, it will be shredded or burned.

- Reproduction of information: Secure cloud server access can be approved for appropriate users to obtain the data and reproduce it. However, no reproduction of data is anticipated.

- Cybersecurity or network protection: There will be access control, virus and antivirus software, application security, network analytics, firewalls, and VPN encryption. Any work needing protection will take place on the Purdue secure network.

- Procedures if information for this effort is compromised: Notify the QRS, Purdue and AF administrators. Refer to and follow appropriate sections in the System Security Plan (SSP), Incident-Handling Capability Plan (IHCP) and Incident Response Plan (IRP)

- Our Information System Security Officer (ISSO): Jeff King, CISSP, 30+ year's experience

B. **Places of Performance.** 130 North 3rd Street, Lafayette, Indiana 47901

C. **Period of Performance**. 1-year base period with four (4) 1-year options