SOSSEC/AFRL C4ISR Software Development OTA
SOSSEC's Prototype Development OTA in support of AFRL's and the Air Force's
Open System Acquisition Initiative (OSAI)

.

Overall Objective

Under OSAI Other Transaction for Prototype Agreement (OTP), SOSSEC Consortium Members, supported by the business, management and technical engineering assistance of SOSSEC, Inc., will perform coordinated prototype development projects in conjunction with the Government that speeds development of Government, industry and academia capabilities in information system technologies proposed to be acquired or developed by the Department of Defense (DoD) to sustain U.S. military technological advantage. Additionally, this OTP will serve as a vital tool to help DoD achieve military integration that is critical to reducing the cost of defense information systems technologies.

Scope

The scope of the AFRL/SOSSEC Other Transaction for Prototype Agreement (OTP) is for the development, test, measurement, demonstration, integration, and delivery of prototypes for the DoD related to Command, Control, Communications, and Cyber, Intelligence, Surveillance, and Reconnaissance (C4ISR) information sharing information systems.

Projects for incremental improvements to these information systems will be made under this OTP. Through these efforts the OT Lead (SOSSEC) and Project-Level Performers (selected SOSSEC Consortium member) will iteratively prototype, modify, enhance, test, measure, document and integrate next-generation Open System Approaches (OSA) for capabilities and tools that satisfy requirements for open-architecture (hardware, software, applications).

Prototypes are to be *"plugged-into"* the information systems to provide new innovative capabilities that provide measurable improvements in performance, function, delivery, flexibility, cost, etc. for rapid transition and use in the field.

Goals

The goals of the AFRL OSAI OTA are as follows:

1. Leverage insights obtained via collaborative planning between Government and the Consortium members so that the Government is better informed on technologies emerging from the private sector and industry achieves greater understanding of emerging operational needs that can be addressed with related technology solutions.
2. Deliberately mature specified emerging technologies to the point of demonstrating the technology within operational evaluations.
3. Improve/advance/demonstrate the performance of command, control, communications, intelligence, reconnaissance and surveillance and recommend systems by the evaluation and the demonstration of new emerging technologies and techniques.
4. Improve the performance of specified and related technologies to achieve advancements in attributes such as reliability, range, speed, service life, sustainment and perception.
5. Advance training and tactics with new and improved technology tools and simulations.
6. Advance technologies to achieve greater levels of tactical autonomy such that entire tactical behaviors can be performed under human supervision vice direct human control.
7. Advance the development of relevant standards and architectures to enable interoperability, subsystem and component inter-changeability, and affordable pricing.
8. Advance the development of offensive and defensive cyber security technology in light of future threats.
9. Conduct technology development and maturation in a manner that enables effective transition of the technology to programs of record via early consideration of life cycle support aspects such as reliability, affordability, manufacturability, sustainment, training, and service life.
10. Conduct Human Factors operational evaluations to enable prevention and mitigation of event connected disabilities.
11. Advance technologies relating to the integration of advanced tactical systems into highly sophisticated air and ground mobile platforms to include manned, semiautonomous and autonomous.
12. Ensure the nature of the agreement facilitates the entry of small and non-traditional companies, such as academia and not-for-profit, into the defense marketplace.

Scope Details

The C4ISR OSAI OTA is for coordinated planning and prototype efforts designed to encompass the following as they relate to C4ISR Information sharing information systems:

- *Agile Engineering, Development & Support*: Develop, demonstrate, implement and transition C4ISR prototype technologies, systems, concepts and designs that address the broad and diverse capabilities in agile prototyping, testing, advanced engineering development and training for modernized information systems to achieve greater levels of resiliency, autonomy and security. Related areas of interest include: development of modern application services, service-based data architectures and designs, high-performance computing technologies, mobile sensors, Multi-Level Security domain information sharing and collaboration technologies, rapid prototyping and development of emerging cyber technologies.

- *C4ISR Capability Performance Analysis*: Develop, demonstrate, implement and transition prototypes to improve hardware and software performance concepts and designs that address system engineering and integration services for information systems, research and development programs, modeling and simulation, and using data to develop/improve/refine products and analysis tools. Related areas of interest include: development of prototype systems that identify vulnerabilities and key technology gaps

- *C4ISR Capability Ecosystems*: Develop, demonstrate, implement and transition prototypes to improve concepts and designs that address C4ISR information technology needs, including: information systems support and development, data architecture and design, enterprise solutions, product lifecycle management and training. Related areas of interest include: development of information systems that support client/server architecture, open system portability and scalability, Multi-Level Security mechanisms among and between security domains, improved mobile systems and automated application platforms.

- *C4ISR Information Systems Security*: Develop, demonstrate, implement and transition prototypes that balance information security with information sharing. This includes: cyber-warfare (both offensive and defensive); and cyber security tools, concepts and designs to address threats, vulnerabilities, and cyber security requirements of systems, and applications. Related areas of interest include: development of prototype software systems using applied system security engineering processes that enforce risk mitigation as well as implementing cost- effective countermeasures not limited to information assurance controls, software protection products, effective rigorous software development processes as well as enforcing software design rigor and information protection measures

- *C4ISR Information Systems Sustainment and Supportability*: Develop, demonstrate, implement and transition C4ISR prototype information technologies to improve engineering design, technical support data and software support services while lowering lifecycle management costs. Related areas of interest include: supportability design and analysis, engineering process improvement, field support, obsolescence, rapid prototyping, systems engineering, and technology insertion.