Subcontractor Statement of Work (SOW)
For work under Alion Science and Technology
DS TAT (FA8075-14-D-0014) RMS#: DT-16-1308

Date: 19 January 2017

Contract Type: T&M

Alion Contracts POC		Alion Technical POC	
Name:	C. Scott Hooven	Name:	Amy Ghazle
Phone:	757-771-8907	Phone:	(315) 356-8131
Email:	Chooven@alionscience.com	Email:	aghazle@alionscience.com

1 INTRODUCTION

This Statement of Work (SOW) outlines the requirements for the Subcontractor in-house, organic software development, engineering, integration, and documentation for Command and Control Experimentation development effort (C2 X) and Program Manager Warfare (PMW) 150 architecture and engineering efforts. The objective of this Performance Work Statement (PWS) is to provide new technological capabilities to prototype systems for implementation into the C2 X environment.

This is a severable, level-of-effort type task order.

1.1 Project Background

PEO C4I PMW 150 Command and Control Division within the Space and Naval Warfare Systems Command, San Diego (SPAWARSYSCOM) provides research and development, systems engineering, integration, test, and life-cycle support for a wide range of Navy, Joint, and National Command Control Communications Computer and Intelligence (C4I) systems. These systems serve to consolidate Command Control and Intelligence functions along with cryptologic, navigation, environmental, and logistic capabilities to provide an integrated C4I capability to the warfighter. Currently, MTC2 SOA software suites are installed at COMPACFLT (CPF), COMSIXTHLT (C6F) and SPAWAR Systems Center Pacific as precursor systems to the POR release. These prototypes C2 capabilities require ingest of multiple data sources to provide necessary data supporting capabilities to C2 Battle Management Aids (BMAs).

1.2 Project Scope

The project scope for this will include the following:

1. Integration and handling of off-board data sources
2. Provenance and Pedigree analysis
3. Classification Tagging
4. Validation of data types
5. Development of ingest mechanisms for integrated software applications, and communications networks
6. Distributed engineering testing, validation, and verification of all source data into computing environment.

2 TECHNICAL REQUIREMENTS

2.1 Tasks

Within C4ISR, there is a desire for domain specific ontologies with the expectation that these can be mapped and reconciled for purposes of analytics. But this carries with it the burden (1) of accuracy and resolution of these models (2) analytical interoperability of these models, and (3) maintenance of models with concomitant adaptation of up and downstream systems. Furthermore, it doesn't provide a framework for handling of data in motion. It is required that a data model based on observation can represent data in any domain, including pedigree and provenance, whether in motion or at rest. This simplifies domain modeling, guarantees analytical interoperability, and reduces the burden of systems maintenance.

2.1.1 Task 1: Adapt SBIR and other S&T implementations

The subcontractor will review, define and document activities necessary to adapt SBIR and other S&T Battle Management Aid implementations to align with the evolving PEO C4I enterprise data strategy implementation of selected data domain as needed

2.1.2 Task 2: Data Domain Definition and Modeling

The subcontractor will participate in data domain definition and modeling as needed

2.1.3 Task 3: Logical Data Model and associated workflow Implementation

The subcontractor will investigate and document activities necessary to complete and develop the logical data model and associated workflows for demonstration and evaluation as directed

2.1.4 Task 4: Draft Concept of Operations

The subcontractor will draft, review and edit the Concept of Operations (CONOPS) documents for Battle Management Aids and associated infrastructure as required

2.1.5 Task 5: Functional Use Case Demonstration

The subcontractor will review engineering and functional test and demonstration plans, functional use cases, and other documentation associated with Battle Management Aid developmental efforts, and provide recommendations for revisions as needed

2.1.6 Task 6: C2 X Support

The subcontractor shall support C2 X in continuous process improvement efforts as it relates to the documenting requirements, managing product development, assisting in experimental and exercise deployments, and testing of Battle Management Aid software functions against operational requirements.

3 GENERAL CONSIDERATIONS

3.1 Travel

San Diego, Ca - Washington DC	4 trips	1 person
San Diego, Ca - Pearl City, HI	2 trips	1 person
San Diego – Manama, Bahrain	1 trip	1 person
San Diego – Naples, Italy	1 trip	1 person
San Diego – Underway / US Navy ship	2 trips	1 person

Other travel as required

3.2 Non-Disclosure Agreements

The subcontractor is responsible for obtaining all nondisclosure agreements with all applicable corporate, supplier, and sub tier vendors with proprietary, restricted, competition sensitive, or any other restricted (e.g. non-foreign disclosure due to public law) data that will be used or accessed during the execution of this contract.

3.3 Program Control

The subcontractor shall use an appropriate control system that maintains program cost and schedule performance data. This shall include forecasting, status reporting, trending, analyzing, and reporting of cost data. The subcontractor shall provide ROM estimates and ECP in response to requests and coordinate report/status of those actions.

4 PERIOD OF PERFORMANCE

The subcontractor shall support this SOW for approximately 8 months from award. The effort shall end no later than 30 September 2017.

5 PLACE OF PERFORMANCE

Performance is anticipated to be at the contractor's facilities and Government facilities in San Diego (e.g. SSC Pacific).

6 DELIVERABLES

All deliverables shall be provided to the Alion PM. Electronic format is preferable. Should that not be feasible, prior arrangements must be made with the Alion PM prior to submission. Electronic delivery is acceptable for *UNCLASSIFIED* material only. For higher classifications, arrangements must be made with the Alion PM before sending. All deliverables are subject to a 15 day review period by the Alion PM and Alion's customer. Subcontractor will have 15 days from receipt of comments to bring deliverables into conformance.

All deliverables shall be sent via email to the Alion Technical POC. The following deliverables are required by this effort:

Deliverable ID	Deliverables	DACA	Number of Documents
A001	Monthly Status Report	35 DACA, Monthly thereafter	7
A002	UML Models	180 DACA; 300 DACA	2
A003	Draft Concept of Operations	270 DACA	1
A004	Operational Guide	300 DACA	1
A005	Draft Capabilities Document	300 DACA	1
A006	Final Technical Report	Contract End	1

6.1 Monthly Status Report (A001)

Monthly Status Reports (Microsoft Word® electronic format) which will include task funding profile (inclusive of task expenditures versus planned expenditures, an estimate at completion (EAC), graphic representation of expenses and hours), variance to plans and plan revisions to correct variances, technical progress including summaries of significant analyses, studies, modeling; and testing, with their relevant conclusions, schedule status, travel status, issues and recommendations. Additionally, the Monthly Progress Report shall identify deliverables completed within the previous reporting period, and will indicate what deliverables are scheduled to be delivered during the upcoming reporting period as well as travel requirements for the upcoming reporting period. MSR format would be agreed to between the Alion POC and subcontractor within first 15 days of award. This report is due within five (5) working days after the end of the reporting period, typically the end of the month.

6.2 UML Models (A002)

The subcontractor shall develop UML Models. This document shall provide additions/extensions to the data domain to include pedigree and provenance tags.

6.3 API Descriptions and Source Code (A003)

The subcontractor shall develop a document to provide API descriptions and source code.

6.4 Installation Guide (A004)

The subcontractor shall develop a installation guide document

6.5 Software Design Description (A005)

The subcontractor shall develop a Software Design document. This document shall provide a description of the software design.

6.6 Final Technical Report (A006)

This report will detail a final report summarizing the project. This will include details from task 1 – task 6. The exact scope of this report will be resolved with the Alion Technical POC and Government sponsors prior to generation. This report should be submitted at end of period of performance.

7 SECURITY

The security requirement for this tasking will be up to and including SECRET.

If foreign travel is required, all outgoing Country/Theater clearance message requests shall be submitted to the SSC Pacific foreign travel team for action. A Request for Foreign Travel form shall be submitted for each traveler, in advance of the travel, to initiate the release of a clearance message at least 40 days in advance of departure. Each Traveler must also submit a Personal Protection Plan 3 and have a Level 1 Antiterrorism/Force Protection briefing within one year of departure and a country specific briefing within 90 days of departure.

Each traveler must also submit a Personal Protection Plan and have a Level 1 Antiterrorism/Force Protection briefing within one year of departure and a country specific briefing within 90 days of departure. Anti-Terrorism/Force Protection (AT/FP) briefings are required for all personnel (Military, DOD Civilian, and contractor) per OPNAVINST F3300.53C. Contractor employees must receive the AT/FP briefing annually. The briefing is available at https://atlevel1.dtic.mil/at/, if experiencing problems accessing this website contact ssc_fortrav@navy.mil. Forward a copy of the training certificate to the previous email address or fax to (619) 553-6863. SERE 100.1 Level A Code of Conduct training is also required prior to OConus travel for all personnel. SERE 100.1 Level A training can be accessed at https://wwwa.nko.navy.mil. Other specialized training for specific locations may also be required. Contact the SSC Pacific foreign travel team to confirm.

As required by the National Industrial Security Program Operating Manual (NISPOM), Chapter 1, Section 3, contractors are required to report certain events that have an impact on the status of the facility clearance (FCL), the status of an employee's personnel clearance (PCL), the proper safeguarding of classified information, or an indication that classified information has been lost or compromised. Contractors working under SSC Pacific contracts will ensure information pertaining to assigned contractor personnel are reported to the COR, Contracts Specialist, and the Security COR (identified in Block 16 of the DD254) along with notifying the appropriate agencies such as the Cognizant Security Agency (CSA), Cognizant Security Office (CSO), or

Department of Defense Central Adjudication Facility (DoD CAF) when related to the denial, suspension, or revocation of a security clearance of any assigned personnel, any adverse information on an assigned employee's continued suitability for continued access to classified access; any instance of loss or compromise, or suspected loss or compromise, of classified information; actual, probable or possible espionage, sabotage, or subversive information; or any other circumstances of a security nature that would affect the contractor's operation while working under SSC Pacific contracts.

7.1 Operations Security

All work is to be performed in accordance with DoD and Navy Operations Security (OPSEC) requirements and in accordance with the OPSEC attachment to the DD254.

7.2 Cybersecurity Workforce

The following cybersecurity workforce categories, levels, training, and certifications are required for contractor personnel under the task order: The contractor will require privileged access to work in cybersecurity Technical (IAT) environments. As required by DoD 8570.01-M, within 60 days of task award personnel performing cybersecurity functions will be required to have certification. Most positions will, at a minimum require IAT level I and II certification for Linux and Windows 7 and/or Server 2003.

The contractor shall ensure that personnel accessing information systems have the proper and current cybersecurity certification to perform IA functions identified in the "Technical Requirements: section of the PWS in accordance with DoD 8570.01-M, Information Assurance Workforce Improvement Program. The contractor shall meet applicable information assurance certification requirement, including (s) DoD-approved cybersecurity workforce certifications appropriate for each specified category and level and (b) appropriate operating system certification for information assurance technical positions as required by DoD 8570.01-M. Contractor personnel who do not have proper and current certifications shall be denied access to DoD information systems for the purpose of performing information assurance functions.

The contractor shall provide documentation supporting the information assurance certification status of personnel performing information assurance functions, reporting current IA certification status and compliance using CDRL Contractor Roster, DI-MGMT-81596 in the format prescribed by the Contracting Officer's Representative (COR).

8 GOVERNMENT FURNISHED PROPERTY (GFP)/GOVERNMENT FURNISHED INFORMATION (GFI)

GFP is not anticipated.