STATEMENT OF WORK
FOR
CYBER WARFARE SUPPORT
30 OCT 2009

1.0 INTRODUCTION

1.1 BACKGROUND

Cyber Warfare is warfare in the Cyberspace domain, which is defined by the SECDEF as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems and embedded processors and controllers." Cyber Warfare encompasses Computer Network Operations (e.g. Attack, Defend and Exploit,) Information Assurance, and the network operations that encompass Command, Control, Communications, Intelligence, Surveillance and Reconnaissance (C4ISR) and Information Operations (IO) functions that occur within the Cyberspace domain. This includes Computer Network Operations (CNO) against automated systems (e.g. C4ISR), and the interaction between the physical, social and biological networks that define human-machine interaction. The Space and Naval Warfare Systems Center, Pacific (SSC PAC), as the principle Navy Research, Development, Test and Evaluation (RDT&E) and Acquisition Center for C4ISR and IO is responsible for functions which include: mission analysis, assessment and development of technology base, basic research, demonstration of technology, engineering in support of production, support to operating forces; supporting doctrine, policy, and strategy development; and integration of numerous National and Tactical systems in the area of Cyber Warfare.

Increasingly, SSC PAC, DoD and other Government customers require advice, assistance, coordination and products necessary to support operational planning, assessment, integration and execution and technology development required to assure superiority for the warfighter in the Cyberspace domain. Specific activities of interest required to achieve superiority in Cyberspace include, but are not limited to:

- Computer Network Operations (e.g. Attack, Defend and Exploit functions) as they relate to the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems and embedded processors and controllers.
- Computer Network Attack (CNA) and Computer Network Exploitation (CNE) against automated systems, and the interaction between the physical, social and biological networks that define human-machine interaction.
- Information Assurance (IA) and Computer Network Defense (CND) measures to protect and defend Naval, Joint and National systems.
- Cyber Warfare Mission Assurance and Mission Planning.
- Understanding aspects of human behavior and cognitive functions to influence adversary decision making (e.g. Psychological Operations (PSYOP) and Military Deception (MILDEC)).

- Electronic Warfare (EW) to include Electronic Attack (EA) Electronic Support (ES) and Electronic Protect (EP) in the RF, millimeter wave, and optical environments.
- Monitoring, analyzing and mitigating Operations Security (OPSEC) vulnerabilities.
- Command and Control (C2) of Cyber Warfare capabilities.
- Intelligence, Surveillance and Reconnaissance (ISR) aspects of Cyber Warfare (including Space Operations).
- Ubiquitous Communications and Computing Environment.
- Countermeasures including the capabilities and expertise to develop source identification tools, cyber data management, and methodologies for object correlation and referencing
- Modeling, Simulation and Visualization of the future environment in which communications, computing, data, sensors and networks are interoperable, ubiquitous and transparent to humans.
- Understanding networks as a science and developing models which can provide clarity into how networks operate and resist or deter attack.
- Convergence of physical, biological and social networks and how this will effect human interactions and decision cycles.
- Understanding of Cyber Warfare Doctrine, Tactics, Techniques and Procedures (TTP)

The work to be conducted under this contract will support SSC PAC in creating capabilities and providing technical services to support technical and operational activities in the Cyberspace domain by the Navy, DoD and other Government agencies.

1.2 SCOPE

The scope of this contract will include efforts to examine the architecture, engineering, functionality, interface and interoperability of Cyber Warfare systems, services and capabilities at the tactical, operational and strategic levels, to include all enabling technologies. This will include operational exercise design and construction, operations and requirements analysis, concept formulation and development, feasibility demonstrations and operational support. This will include efforts to analyze and engineer operational, functional and system requirements in order to establish national, theater and force level architecture and engineering plans, interface and systems specifications and definitions, implementation, including hardware acquisition for turnkey systems. Additional efforts will include software design and implementation as well as systems integration, test and evaluation and demonstration.

Research and development in advanced technology and special technical operations requires periodic contractor augmentation of a technical or scientific nature to meet technical as well as operational commitments and/or requirements. Contractor support is also required to supplement or provide personnel with specific expertise which is limited or not available at SSC PAC. Areas of expertise which may be required include, but are not limited to: Cyber Warfare doctrine/tactics, techniques and procedures (TTP), policy and strategy and operational planning analysis and intelligence assessment,

measures of effectiveness (MOE) and measures of performance (MOP) evaluation, electronic warfare, wargamming, modeling and simulation, systems engineering, systems analysis, computer hardware and software engineering and development, implementation and integration, operational research and analysis, communications and networking hardware, protocols, and security.

The work described below is representative of the type of requirements that currently exist or can reasonably be anticipated through fiscal year 2020. Because of the variety of tasks that may be required, specific work efforts will be initiated by means of delivery/task orders which will be issued in accordance with the provisions of this Statement of Work (SOW) and other provisions of the overarching support contract.

- Perform basic and applied research in Cyber Warfare, its enabling technologies, techniques, and theory.
- Design and develop network, system, services and application architectures that support the rapid development and implementation of new technologies and capabilities that reflect the rapidly evolving techniques which characterize cyber attacks.
- Analyze, design, develop, document, integrate, test, install and maintain Cyber Warfare and enabling capabilities.
- Develop, implement, and integrate solution sets that enable a holistic command and control capability, with appropriate underpinning technologies and capabilities, that provide for interagency communication and collaboration of cyber activities.
- Serve as the test site (via the SSC PAC labs and other Government facilities) for interoperability testing among Cyber Warfare systems, tools, technologies and processes (both existing and new) prior to their introduction to operational environments.
- Participate in Cyber technology forums.
- Provide operational support to assist in technical and programmatic oversight of Cyber Warfare and enabling systems, programs and functions.
- Provide Systems Engineering and Integration support to improve overall effectiveness of Cyber Warfare and enabling systems, services and functions.
- Demonstrate and evaluate the application of advanced software and hardware concepts and technology to Cyber Warfare and enabling systems and functions.
- Associate information posted in cyberspace to a physical identity and originating location.
- Conduct analyses and systems engineering to develop initiatives in support of emerging Cyber Warfare requirements.
- Develop capabilities to detect and identify complex, multi-dimensional attacks of an adversary, and to be able to correlate disparate events with their greater implications to the warfighter.
- Provide computer and network forensic capabilities.
- Perform analysis, algorithm development and implementation, and display for Cyber Warfare tools and data fusion drawn from various sources of information.
- Provide support for Cyber Warfare experiments, exercises, and other events.

- Perform analysis of adversarial cyber threat capabilities to develop courses-of-action and response options under a variety of hypothetical scenarios.
- Conduct Cyber Warfare Modeling and Simulation, wargaming and analysis.
- Perform risk assessment and mitigation planning.

1.3 REFERENCE DOCUMENTS

The following documents were used in the development of this SOW:

a. Cyberspace Policy Review, May 2009
b. Joint Doctrine for Information Operations, Joint Pub 3-13, 9 Oct 1998, Unclassified
c. Director of Central Intelligence Directive 7/3 Information Operations and Intelligence Community Related Activities (U)
d. Navy NetOps CONOPS, 2 Jun 09 (Draft)
e. The National Security Strategy, March 2006
f. National Military Strategy for Cyber Operations (NMS-CO), Dec 2006
g. National Strategy to Secure Cyberspace (National Security Presidential Directive 38 (NSPD-38)), 2004
h. Navy Warfare Pub 3-63 CNO Vol 1 and 2
i. NTTP 3.13.x series on Navy IO
j. Cyber Security and Monitoring (National Security Presidential Directive 54 (NSPD-54)/Homeland Security Presidential Directive 23 (HSPD-23)), 8 Jan 2008
k. DODD O-8530.1 (CND)
l. DODI O-8530.2 (CND)
m. CJCSM 6510.01 (DID: CND)
n. SECNAVINST 5239.19 (DON Incident Response/Reporting)
o. SECNAVINST 5000.2C, Implementation and Operation of the Defense Acquisition System and the Joint Capabilities Integration and Development System
p. NAVSEA Instruction 3900.8A, Human Systems Integration (HSI) Policy in Acquisition and Modernization, 20 May 2005

2.0 TECHNICAL REQUIREMENTS

The Contractor shall be required to provide a wide range of expertise supporting full spectrum Cyber Warfare and enabling activities.

2.1 GENERAL

The Contractor shall provide technical and management services to support SSC PAC in establishing and maintaining Cyber Warfare and enabling product lines, programs and projects. The Contractor shall provide experienced personnel to engage in identifying, and developing core technical and functional services in support of full spectrum Cyber Warfare and enablers. The Contractor shall provide technical and management services that enable rapid development and deployment of new capabilities to attack, defend, and exploit networks, systems and services in response to emerging requirements.

2.2 TECHNOLOGY ASSESSMENT, DEVELOPMENT AND TRANSITION

The Contractor shall identify and perform research, analysis, analysis of alternatives (AoA), evaluation, development and test of technologies from Industry, Academia, and other Government organizations, to include Commercial Off-The-Shelf (COTS), Government Off-The-Shelf (GOTS), and open source technologies, for applicability to solving Cyber Warfare deficiencies, improving existing Cyber Warfare and enabling capabilities and/or generating new Cyber Warfare capabilities.

To address the timely challenges of Cyber Security deficiencies, the Contractor shall establish core technology evaluation criteria, metrics, datasets, and test protocols, and build a repository of technology to more easily automate the evaluation process for emerging technologies under consideration for use in cyber infrastructures. Unclassified laboratories with common synthetic data sets, representative of actual data, shall be constructed to enable proper systems engineering analysis and common criteria for comparison, concept refinement, and selection for more advanced analysis and study.

2.3 REQUIREMENTS ANALYSIS

The Contractor shall perform analyses of existing and emerging Operational and Functional Requirements at the force, theater, Combatant Commands (COCOM) and national levels to support the formulation, development and assessment of doctrine, strategy, plans, concepts of operations, and tactics, techniques and procedures in order to provide the full spectrum of Cyber Warfare and enabling capabilities to the warfighter. This shall include the analysis of Cyber Warfare organizations including tactics, techniques and procedures to develop new doctrine, operational methodologies and missions, identification of potential threats, vulnerabilities, risks, safeguards, performance indicators and countermeasures. The Contractor shall analyze social and cultural factors and attributes of potential adversaries and cognitive, behavioral, skill, and knowledge requirements derived form these considerations. The Contractor shall also perform feasibility analyses of systems or operational concepts, including a cost/benefit analysis as required. The Contractor shall research and develop technical analyses and assessment reports for integration of cyber requirements, capabilities and training. The Contractor shall research and develop reports, documents and assessments for mapping naval, theater and joint plans and programs to cyber capability requirements. The Contractor shall perform Cyber Military Utility Assessments (MUA)/Operational Utility Assessments (OUA), to include assessments of cyber warfighting capability and the utility of new and or/emerging technologies.

2.4 SYSTEMS ENGINEERING

The Contractor shall perform system analysis, architecture, engineering, and integration services at the system, intra/inter-node, force, theater and national levels. The Contractor shall perform analyses of current Cyber Warfare and enabling capabilities and deficiencies, identify system requirements and associated architectures and perform all aspects of systems engineering support required to implement the full spectrum of Cyber Warfare capabilities and systems. The Contractor shall perform technical trade studies which shall lead to the development of new Cyber Warfare architectures and detailed engineering designs.

2.5 OPERATIONAL AND TECHNICAL SUPPORT

The Contractor shall provide operational and technical support to SSC PAC Cyber Warfare and enabling efforts by reviewing and analyzing national security policy and military strategy, including defense transformation and planning guidance, intelligence estimates, threat projections, vulnerability assessments, forensics and other relevant material and activities. The Contractor shall support the production and implementation of comprehensive, long-term, fully-integrated DoD strategies for the application of innovative approaches that supports national security and theater specific operations plans. Incorporating the results of prior planning and strategy development, the Contractor shall support the development of theater focused strategies, concepts of operations, standard operating procedures, rules of engagement, pre-planned responses, and supporting Annexes/Tabs to Combatant Commanders/Joint Task Force (JTF) Commanders' Operational/Contingency Plans (OPLAN/CONPLAN). Additionally, the Contractor shall provide technical recommendations that support the development of Memorandums of Understanding/Memorandums of Agreement (MOU/MOA) between theater, national, and global stakeholders.

The Contractor shall provide theater focused full spectrum security test and evaluation activities, to include Blue, Green, White, and Red Team support to provide training, as well as assess vulnerabilities and/or deficiencies of Cyber Warfare capabilities to the latest threats emanating from adversaries and other malicious sources, identifying solutions and/or trade offs to correct any deficiencies.

The Contractor shall participate in Cyber focused forums, boards, conferences, seminars, exercises, and planning sessions as required.

The Contractor shall provide forensics support of compromised systems as well as captured systems. This support shall include analysis of software, firmware, hardware (analog and digital sections), as well as protective measures including tamper prevention/evidence systems.

2.6 EXERCISE AND EXPERIMENTATION SUPPORT

The Contractor shall propose and participate in Exercise and Experimentation (including war gaming) to support the development and assessment of Cyber Warfare and enabling capabilities and their utility, to identify new tactics, techniques and procedures for the full spectrum of Cyber Warfare. This shall include all planning, logistics and scheduling and manning requirements of exercises and experiments. Additional requirements include, but are not limited to:

a) Detailed exercise and experiment design, planning and scheduling, including specification of equipment, platforms, systems (including their configuration,) exercise code/scripts, and personnel.
b) Develop simulation capabilities and/or models for validation of functional operation of Cyber Warfare and enabling capabilities or activities.

c) Logistics support, including configuration management, quality assurance, reliability/maintainability analysis, material/data control and classification / information security oversight.
d) Participation in exercise and experiments, including subject matter experts, being an observer of a system or activity as well as being a data collector.
e) Analysis and reconstruction of exercise and experiment data from actual collected information.
f) Develop Cyber Warfare training objectives to stimulate training audiences, assess capability shortfalls, and develop Plans of Action and Milestones.
g) Research, gather data, analyze and develop intelligence and IO concept development and experimentation planning documents and execution planning.

2.7 SOFTWARE DEVELOPMENT AND PROTOTYPING

The Contractor shall specify, design, develop, code, test, integrate and document software modules systems and subsystems to provide new functional capabilities and improve existing Cyber Warfare and enabling systems. The Contractor shall perform reverse engineering of software components and systems to support vulnerability and exploitation analysis. The functions to be implemented include the full spectrum of Cyber Warfare. The Contractor shall adhere to open standards and modern software development methodologies, including what is considered ‘best’ practices by the industry. This also includes rapid prototyping to meet time critical requirements.

2.8 HARDWARE DEVELOPMENT AND PROTOTYPING

The Contractor shall provide hardware engineering support to development, prototype and implementation, test, integrate and document hardware based solutions to the full spectrum of Cyber Warfare and enabling capabilities. The Contractor shall perform reverse engineering of hardware components and systems to support vulnerability and exploitation analysis. This includes mixed signal integrated circuit design and development. The Contractor shall adhere to modern hardware development and fabrication methodologies, including what is considered ‘best’ practices by the industry. This also includes rapid prototyping to meet time critical requirements.

2.9 MODELING AND SIMULATION

The Contractor shall architect, design and develop Modeling and Simulating (M&S) infrastructure and capabilities to investigate systems and their interdependencies, enhance preparedness, protection, response, mitigation, and recovery activities of Cyber Warfare offensive and defensive measures. The M&S capabilities shall address network contingency analysis, cyber-attack analysis, situation assessment, course-of-action analysis and optimization. The M&S shall also support the integration of multiple pre-existing M&S capabilities and the creation of new capabilities.

2.10 TRAINING SUPPORT

The Contractor shall plan, develop, and implement Cyber Warfare training plans, educational and training courses, and formal Cyber exercises that enable the attack, defense, and exploitation capabilities of Cyber Warfare within the cyber domain.

2.11 SECURITY ENGINEERING

The Contractor shall execute all phases of the US Department of Defense's Information Technology Security Certification and Accreditation Process (DITSCAP)/ Defense Information Assurance Certifications and Accreditation Process (DIACAP) process, all security tests and evaluations and provide a comprehensive risk assessment as part of their individual delivery/task order fulfillment. The Contractor shall support the certification and accreditation of programs using DITSCAP/DIACAP, Secret and Below Interoperability (SABI), Director of Central Intelligence Directives (DCID) 6/3 processes. The Contractor shall also perform analysis related to the development of security test plans, procedures, reports, and assessments as appropriate.

3.0 REPORTS, DATA AND DELIVERABLES

Technical data and computer software deliverables shall be provided in accordance with the Contract Data Requirements List, DD Form 1423, as specified in individual delivery/task orders. All deliverables are subject to SSC PAC review and approval before final acceptance.

All classified deliverables shall be protected and handled in accordance with standard security practices and procedures.

4.0 SECURITY

The nature of this task requires access to Secret information. The work performed by the Contractor will include access to unclassified and up to Secret data, information, and spaces. The Contractor will be required to attend meetings classified up to Secret level.

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.