Performance Work Statement
SPAWAR 5.0 Experimentation and Project Management Support Services
25 January 2018

1 INTRODUCTION

The Department of the Navy (DON), Space and Naval Warfare Systems Command (SPAWAR) is acquiring Fleet Experimentation (Trident Warrior (TW), Allied and Coalition/Interoperability) and Project Management support services for the Office of the Chief Engineer (CHENG), SPAWAR 5.0.

2 BACKGROUND

According to the office of the Chief of Naval Operations (CNO), the Navy Information Warfare Community focuses on providing Naval and Joint warfighters the Assured Command and Control, Battlespace Awareness, and Integrated Fires capabilities they need to fight and win in this Information Age. This is true especially in Intelligence, Surveillance, and Reconnaissance (ISR), Command, Control, Communications, and Computers (C4), Information Operations (IO) and Cyber Warfare domains that are critical to the Navy's future success in operations at all levels of war and in all domains (afloat, aloft, ashore, subsurface, space and cyberspace). As the Navy's Information Warfare Lead systems command, SPAWAR's vision is to deliver knowledge superiority to the warfighter at the right time and for the right cost.

As the Technical Authority (TA) for Navy's Information Technology (IT) and Information Assurance, the SPAWAR CHENG, provides experimentation leadership in collaboration with other Navy commands, DoD agencies/laboratories, Science and Technology (S&T) activities, Allies and Coalition partners, academic organization and other experimentation stakeholder across a wide spectrum, ensuring development of innovative approaches and rapid development of products that solve problems and identify gaps for the Fleet.

3 SCOPE

This contract will provide a full spectrum of planning, design, execution, analysis and assessment, and reporting/product for fleet operational experimentation in Navy, joint, multi-service, and/or Allied environments for SPAWAR HQ CHENG. The scope includes the experimentation and testing of new and existing Fleet systems to reduce risk and lifecycle cost, alignment of Pacific Fleet warfighting capabilities development priorities with Coalition development activities and ensure interoperability of United States and Coalition capabilities prior to fielding. The Contractor shall perform the services identified in this PWS with minimal assistance from SPAWAR 5.0 personnel.

Knowledge, skill, and experience requirements will vary by task, from working level to senior engineers and analysts (program management, experimentation and information assurance) who will provide detailed analysis, strategic planning, concept development and execution in support

of experimentation and project management. The Contractor will be required to participate in meetings, support Fleet and Allied experimentation events to support the mission for the continued development, growth, and vision of Information Warfare. *The majority of the requirements within this PWS will be met at or below the SECRET level. The Contractor will be required to provide cleared staff for incidental access to TOP SECRET Sensitive Compartment Information (TS/SCI) data, information, and associated spaces to attend meetings, regional events and exercises (see paragraph 8.1.1 for further access information).*

3.1 Experimentation

Subject matter expertise for advanced C4I/C4I Information Warfare (IW) capabilities to support long term strategic planning for Naval Networks, Information Management/Collaboration, Knowledge Management, Command and Control, Human Systems Integration (HSI)/Intelligence Surveillance and Reconnaissance (ISR), Naval Fires and Information Operations and current and projected future Joint Integration, Coalition and Interagency IW capabilities are critical in support of SPAWAR HQ CHENG and fleet experimentation stakeholders. *The Contractor will be required to provide cleared staff for incidental access to TOP SECRET Sensitive Compartment Information (TS/SCI) data, information, and associated spaces to attend meetings, regional events and exercises (see paragraph 8.1.1 for further access information).*

Fleet Experimentation efforts in the following areas will be required by the contractor:

- Experimentation planning and design.
- Production of experiment planning products and development of post-experiment doctrine, organization changes, training process improvements, and material solution recommendations across Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities (DOTMLPF).
- Data collection planning, analysis, and assessment.
- Experiment execution/post-experiment briefings and support.
- Development of final experiment reports based on analytical rigor.
- General support for all experiment administrative requirements linked to the execution of the event.

4 APPLICABLE DOCUMENTS

The Contractor shall ensure all work accomplished on task utilizes the best commercial practices and current acceptable industry standards. The applicable references and standards invoked will vary within individual tasks and will be specifically referenced, if needed. In accordance with Defense Acquisition Policy changes, maximum utilization of non-government standards will be made wherever practical. Where backward compatibility with existing systems is required, selected interoperability standards will be invoked.

4.1 Required Documents

The following instructional documents are mandatory for use. Unless otherwise specified, the documents effective date of issue is the date on the request for proposal. Additional applicable documents may be included in specific task.

	Document Number	Title
a.	DFARS SUBPART 5239.71	Security and Privacy for Computer Systems dtd 21 Sep 15
b.	DoDI 5200.02	DoD Personnel Security Program (PSP) Reissues DoD Directive (DoDD) 5200.2 (Reference (a)) as a DoD Instruction (DoDI) in accordance with the authority in DoDD 5143.01 dtd 21 Mar 14
c.	DoDM 5200.01	DoD Manual – Information Security Program Manual dtd 24 Feb 12
d.	DoDD 5205.02E	DoD Directive – Operations Security (OPSEC) Program dtd 20 Jun 12
e.	DoD 5205.02-M	DoD Manual – Operations Security (OPSEC) Program Manual dtd 3 Nov 08
f.	DoD 5220.22-M	DoD Manual – National Industrial Security Program Operating Manual (NISPOM) dtd 28 Feb 06
g.	DoDI 5220.22	DoD Instruction – National Industrial Security Program dtd 18 Mar 11
h.	DoDI 6205.4	Department of Defense Instruction, Immunization of Other Than U.S. Forces (OTUSF) for Biological Warfare Defense dtd 14 Apr 00
i.	DoDI 8500.01	DoD Instruction – Cybersecurity dtd 14 Mar 14
j.	DoDI 8510.01	DoD Instruction – Risk Management Framework (RMF) for DoD Information Technology (IT) dtd 12 Mar 14
k.	DoD 8570.01-M	Information Assurance Workforce Improvement Program dtd 19 Dec 05 with Change 3 dtd 24 Jan 12
l.	DoDD 8140.01	Cyberspace Workforce Management dtd 11 Aug 15
m.	SECNAV M-5239.2	DON Cyberspace Information Technology and Cybersecurity Workforce Management and Qualification Manual dtd Jun 16
n.	SECNAV M-5510.30	Secretary of the Navy Manual – DoN Personnel Security Program dtd Jun 2006
o.	SECNAVINST 4440.34	Secretary of the Navy Instruction – Implementation of Item Unique Identification within the DoN, dtd 22 Dec 09
p.	SECNAVINST 5239.19	Department of the Navy Computer Network Incident Response and Reporting Requirements, dtd Mar 08
q.	SECNAVINST 5239.20A	DON Cyberspace IT and Cybersecurity dtd 10 Feb 16
r.	SECNAVINST 5239.3C	DON Cybersecurity Policy, dtd 2 May 16
s.	SECNAVINST 5510.30	DON Regulation – Personnel Security Program dtd 6 Oct 06
t.	DON CIO Memorandum	Acceptable Use of Department of the Navy Information Technology (IT) dtd 12 Feb 16

	Document Number	Title
u.	SPAWARINST 3432.1	SPAWAR Instruction – Operations Security (OPSEC) Policy dtd 2 Feb 05
v.	SPAWARINST 4440.12	Management of Operating Materials and Supplies (OM&S), Government Furnished Property (GFP), Contractor Acquired Property (CAP), Property, Plant and Equipment (PP&E), and Inventory
w.	SPAWARINST 5721.1B	SPAWAR Section 508 Implementation Policy, 17 Nov 09
x.	SPAWARSYSCENLANT INST 12910.1A	Space and Naval Warfare Systems Center Atlantic Instruction – Deployment of Personnel and Contractor Employees to Specific Mission Destinations, of 28 Dec 09
y.	COMUSFLTFORCOM/C OMPACFLTINST 6320.3B	Commander US Fleet Forces Command/Commander US Pacific Fleet Instruction, Medical Screening For US Govt Civilian Employees, Contractor Personnel, and Guests prior to embarking Fleet Units, of 7 April 14
z.	OPNAV 5239/14 (Rev 9/2011)	System Authorization Access Request (SAAR) - Navy
aa.	SPAWARINST 4130.3	SPAWAR Life Cycle Configuration Management (CM) Policy dtd 28 Mar 13
bb.	EIA-649-1	Configuration Management Requirements for Defense Contracts
cc.	DoDI 6205.4	Department of Defense Instruction, Immunization of Other Than U.S. Forces (OTUSF) for Biological Warfare Defense

4.2 Guidance Documents

The following documents are to be used as guidance. Unless otherwise specified, the documents effective date of issue is the date on the request for proposal. Additional applicable documents may be included in a specific task.

	Document Number	Title
a.	AI CONOPS V1.0	CONOPS Application Integration dtd Dec 09
b.	ANSI/EIA-748A	America National Standards Institute/Electronic Industries Alliance Standard – Earned Value Management (EVM) Systems
c.	CJCSI 3170.01I(ser)	Joint Capabilities Integration and Development System
d.	CJCSI 6212.01(ser)	Interoperability and Supportability of Information Technology and National Security Systems
e.	DODD 5000.01	Defense Acquisition System
f.	DoDI 3020.41	DoD Instruction – Operational Contract Support (OCS), 20 Dec 11
g.	DoDI 4151.19	DoD Instruction – Serialized Item Management (SIM) for Life-Cycle Management of Materiel, 9 Jan 14

	Document Number	Title
h.	DoDI 4161.02	DoD Instruction – Accountability and Management of Government Contract Property, 27 Apr 12
i.	DoDI 5000.02	DoD Instruction – Operation of the Defense Acquisition System
j.	DoDI 5000.2E	DON Defense Acquisition and Joint Capabilities Integration and Development
k.	DoDI 5000.61	DoD Modeling and Simulation Verification, Validation, and Accreditation
l.	DoDI 8320.04	DoD Instruction – Item Unique Identification (IUID) Standards for Tangible Personal Property, 3 Sep 15
m.	DoDM-1000.13-M-V1	DoD Manual – DoD Identification Cards: ID card Life-Cycle dtd 23 Jan 14
n.	DoN EA Memo V5 (ser)	Fiscal Year 2016 Annual Review Process with DoN Enterprise Architecture ver 5.0, 23 Dec 2015
o.	DoN CNO Ltr 3800	Navy Information Technology Enterprise Architecture Development to Support Joint Information Environment Transition Planning dtd 5 Aug 13
p.	FIPS PUB 201-2	Federal Information Processing Standards Publication 201-2 – Personal Identity Verification (PIV) of Federal Employees and Contractors, August 2013
q.	Form I-9, OMB No. 1615-0047	US Department of Justice, Immigration and Naturalization Services, Form I-9, OMB No. 1615-0047 – Employment Eligibility Verification
r.	Defense Acquisition Guidebook	Defense Acquisition Guidebook
s.	Naval Systems Engineering Guide	Naval Systems Engineering Guide
t.	HSPD-12	Homeland Security Presidential Directive – Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004 https://hspd12.usda.gov/
u.	IEEE Std 12207-2008	Systems and Software Engineering – Software Life Cycle Processes
v.	ISO 9001 (ANSI/ASQ Q9001)	International Organization for Standardization (American National Standard Institute/American Society for Quality) – Quality Management Systems, Requirements
w.	ISO/IEC 12207	International Organization for Standardization/ International Electrotechnical Commission: Systems and Software Engineering – Software Life Cycle Processes
x.	ISO/IEC 15288	International Organization for Standardization/ International Electrotechnical Commission: Systems and Software Engineering – System Life Cycle Processes

	Document Number	Title
y.	GEIA-HB-649A	Configuration Management Standard Implementation Guide
z.	MIL-STD-130N	DoD Standard Practice – Identification Marking of US Military Property
aa.	MIL-STD-1916	DoD Test Method Standard – DoD Preferred Methods for Acceptance Of Product
ab.	MIL-STD-881C	Work Breakdown Structure for Defense Materiel Items
ac.	OPNAVINST 3050.25	Alignment and Responsibility of Navy Requirements Generation and Resource Planning DOD Architectural Framework OPNAVINST 3050.23 (Alignment and Responsibility of Navy Requirements Generation and Resource Planning DOD Architectural Framework) This instruction was not listed in the Navy Issuances page; apparently it was cancelled by OPNAVINST 3050.25, see attached.
ad.	SECNAVINST 5200.38	DON Modeling and Simulation Management
ae.	SECNAVINST 5200.40	DON VV&A of Models and Simulations
af.	SPAWARINST 3058.1	Naval SYSCOM Risk Management Policy dtd Apr 08
ag.	SPAWARINST 5400.1A	Virtual SYSCOM Engineering and Technical Authority Policy
ah.	ANSI/EIA-649B	Configuration Management Standard
ai.	SPAWARINST 5400.3	Systems Engineering Technical Review Process
aj.	SPAWARINST 5401.3	Enterprise Architecture Policy dtd 5 Feb 16
ak.	Technical Warrant Holder CONOPS	Technical Warrant Holder CONOPS 22 April 15
al.	Strategic_Plan_2015-17	SPAWAR 5.0 Strategic Plan 2015-2017
am.	SPAWARINST 5238.2B	Science and Technology Forecasting, Investment, and Transition Concept of Operations Implementation
an.	SPAWAR EA ADM	SPAWAR Enterprise Architecture Data Model v2 Approved July 2017
ao.	SPAWAR EA ID	SPAWAR Enterprise Architecture Integrated Dictionary Approved June 2017
ap.	DoDI 5000.75	Defense Business Systems Instruction

5 PERFORMANCE REQUIREMENTS

The following paragraphs list all support tasks required throughout the life of the task order. The Contractor shall provide necessary resources and knowledge to support the listed tasks. The Contractor shall complete all required tasks while controlling and tracking performance and goals in terms of cost, schedule, and resources.

5.1 Project Management Support Services

5.1.1 Project Management Support Services (RDT&E)

5.1.1.1 The Contractor shall design, develop, test, implement and document the Microsoft SharePoint Site Collection hosted on the Naval Systems Engineering Resource Center (NSERC) and network/web based collaboration tools/platforms for all Technical Authority, engineering, and business operations efforts (CDRL A002).

5.1.1.2 The Contractor shall investigate, research, verify and validate services for NMCI in support of the SPAWAR 5.0 mission, including technical refresh and communicate NMCI guidance (CDRL A002).

5.1.2 Project Management Support Services (O&M,N)

5.1.2.1 The Contractor shall assist with the operation and maintenance of NSERC and/or network/web based collaboration tools for all Technical Authority, engineering, and business operations efforts (CDRL A002).

5.1.2.2 The Contractor shall prepare reports, plans, summaries and/or briefings with associated data (CDRL A002) that describe the topics described above. The Contractor shall ensure reports demonstrate the applicability and effectiveness of the criteria. Unacceptable solutions shall be identified as to how and why each solution failed to satisfy the specified criteria and shall be discussed. The report shall include a list of solutions that satisfied the criteria and a recommended course of action. The remainder of the report shall clearly show the correlation between each solution and the technical requirements (CDRL A0002). Unless otherwise specified, the Contractor's format is acceptable.

5.1.2.3 The Contractor shall modify and track services for NMCI in support of the SPAWAR 5.0's mission, including IT maintenance, technical refresh, day-to-day issues and communicate NMCI guidance.

5.2 Experimentation

5.2.1 Trident Warrior (TW) Experiment Concept Development and Strategic Planning (RDT&E)

Incidental access up to TS/SCI is required for research of background data to characterize analytical/task scenarios and to support regional events and exercises (see paragraph 8.1.1 for further access information).

5.2.1.1 The Contractor shall develop a long-term strategy for delivery of Information Warfare (IW) capabilities to the warfighter, including providing technical and program management services to accurately assess current Navy/Joint/Coalition C4I/C5I capabilities, and future requirements. Develop a strategic experimentation plan to identify and validate potential technology solutions to known capability gaps. Coordinate with other organizations such as

OPNAV, NWDC, NWC, SPAWAR, NAVAIR, NAVSEA, USFFC, Industry, Allies (ex. AUSCANNZUKUS) and Coalition.

5.2.1.2 The Contractor shall define timelines for achieving specific future IW capabilities based on integration with non-naval organizations C4ISR/C4I systems and provide recommendations on prioritization of future capabilities.

5.2.1.3 The Contractor shall identify potential experimentation venues and opportunities for IW capabilities and provide recommendations for inclusion in operational experimentation plans.

5.2.1.4 The Contractor shall provide experiment initiative management and technical services to include: (1) experiment design, planning, and execution; (2) management, systems engineering, test/experiment and evaluation; (3) integration engineering and data collection and analysis (4) Architecture artifact generation.

5.2.1.5 The Contractor shall provide technical continuity and coordination to ensure selected experiment proposals are technically feasible, compatible, and interoperable with other Naval, Joint, Coalition and national programs, operational experiment objectives and related projects.

5.2.1.6 The Contractor shall assess proposed technologies for potential to provide solutions to gaps in operational capability, including reviewing and updating of Fleet Experimentation Management System, and/or follow on systems as appropriate.

5.2.1.7 The Contractor shall assess experimentation proposals for changes to, or creation of new Concepts of Operation (CONOPS) or Tactics, Techniques and Procedures (TTPs) for potential to provide solutions to gaps in operational capability, including CONOPS or TTPs arising from introduction of new technologies.

5.2.1.8 The Contractor shall coordinate the participation and integration of technologies from different providers in specific experiment events and establish relevant and measurable metrics for specific experiments.

5.2.1.9 The Contractor shall liaison with numerous Fleet afloat schedulers to identify specific platforms for use in underway experimentation venues to ensure selected platforms will support achievement of experiment objectives.

5.2.1.10 The Contractor shall develop event Scenario and Mission Scenario Event List (MSEL) documentation, including manning and training plans for the overall experiment and/or individual initiatives (CDRL A002).

5.2.1.11 The Contractor shall coordinate with technology providers to assess risk to operational platform systems from installation of experiment systems.

5.2.1.12 The Contractor shall coordinate with technology providers to ensure that all applications, networks, servers, or associated devices procured and/or connected to a Navy network have completed DADMS registration and received Functional Area Management

(FAM) approval.

5.2.1.13 The Contractor shall develop and brief detailed experimentation event specific C4I architecture and installation plans to Destroyer Squadrons (DESRONS), Amphibious Squadrons (PHIBRONS), Strike Group Staffs, Type Commanders (Air, Surface, Subsurface), Numbered Fleet Commanders, Fleet Commanders, surface platforms and submarines, Naval Communications and Telecommunications Area Master Stations and East, West Coast Network Operations Centers (NOC's) and other commands as necessary (CDRL A002).

5.2.1.14 The Contractor shall coordinate rigorous ship and shore installation processes including Ship Change Documents for the Entitled Process, IT-21 Certification, Security Accreditation and Fleet Readiness Certification Board (FRCB) processes for shore installations, including Installation (Navy Modernization Process), Certification and Accreditation (C&A), Assessment and Authorization (A&A), and Human Systems Integration (HSI) processes (CDRL A002).

5.2.1.15 The Contractor shall coordinate with SPAWAR, and other organizations as appropriate, to develop and refine complex IW experimentation architectures and to identify/track all process milestones to meet fleet defined installation windows.

5.2.1.16 The Contractor shall create experimentation plans and provide schedules for testing of all participating initiatives and the conditions required for each test sequence, including platform positioning and network/system condition requirements for each experiment.

5.2.1.17 The Contractor shall coordinate execution of experiments to ensure that technologies follow the experiment plan and record required data for the evaluation of experiment objectives.

5.2.1.18 The Contractor shall provide technical and engineering expertise to monitor and maintain data collection systems during the experiment events.

5.2.1.19 The Contractor shall coordinate with technology providers and Trident Warrior leadership to perform analysis of experiment data and provide reports (CDRL A002) with observation and recommendations.

5.2.1.20 The Contractor shall verify accreditation for all hardware, software, network or site to ensure successful execute experimentation demonstrations and provide input to demonstration assessment and lessons learned.

5.2.1.21 The Contractor shall provide systems/network engineering expertise at all related conferences and meetings as required.

5.2.2 Allied, Strategic Planning, Vision, Experiment Support (O&M,N)

Incidental access up to TS/SCI is required for research of background data to characterize analytical/task scenarios and to support regional/allied events and exercises (see paragraph 8.1.1 for further access information).

5.2.2.1 The Contractor shall liaison with resource sponsor OPNAV N2/N6 and the executing agency SPAWAR 5.0, SSC-PACIFIC as well as with other SPAWAR activities and stakeholders.

5.2.2.2 The Contractor shall provide expertise in AUSCANNZUKUS Experimentation Working Group and Report writing and initiative review for current exercises and scenarios, and criteria evaluation for other exercises and scenarios.

5.2.2.3 The Contractor shall plan, and participate in, all Allied Experimentation events – to include hardware/software integration, generation of necessary documentation (unclassified and classified networks) and coordination to track progress of selected trials for experimentation scenarios; Certification and Accreditation (C&A)/Assessment and Authorization (A&A) event assessment, and report writing.

5.2.2.4 The Contractor shall identify issues related to capability gaps, various coalition operations, and IA/CND scenarios and participate in S&T activities that address the Gaps/Limitations within the selected scenarios.

5.2.2.5 The Contractor shall attend all applicable international meetings and planning conferences and participate in working groups and provide reasonable and beneficial inputs in support of the Allied goals and objectives.

5.2.3 Allied, Coalition/Interoperability Strategic Planning, Vision Support, Experiment Concept Development (RDT&E)

Incidental access up to TS/SCI is required for research of background data to characterize analytical/task scenarios and to support regional/allied events and exercises (see paragraph 8.1.1 for further access information).

5.2.3.1 The Contractor shall liaison with resource sponsor OPNAV N2/N6 and the executing agency SPAWAR 5.0, SSC-PACIFIC as well as with other SPAWAR activities and stakeholders.

5.2.3.2 The Contractor shall provide expertise in AUSCANNZUKUS Experimentation Working Group and Trident Warrior (TW) Report writing and initiative development for current exercises and scenarios, and criteria evaluation for other exercises and scenarios.

5.2.3.3 The Contractor shall plan, participate in, and execute Coalition Interoperability Experimentation events to include Coalition Warrior Interoperability Demonstration (CWIX) and Coalition Interoperability Assurance and Validation (CIAV), Combined Coalition Interoperability Board (CCIB), and Interoperability Management Board (IMB), and other venues as appropriate – to include hardware/software integration, generation of necessary documentation (unclassified and classified networks) and coordination to track progress of selected trials for experimentation scenarios; Certification and Accreditation (C&A)/Assessment and Authorization (A&A) event assessment, and report writing (CDRL A002).

5.2.3.4 The Contractor shall plan for the installation and operation of classified and unclassified networks within the space designated as the Navy site, including outdoor installations and vehicles. Perform Information Assurance (IA) testing to ensure compliance within the network for all equipment utilized in support of Coalition Interoperability Experimentation. Prepare supporting documentation to identify equipment on the network and network test results.

5.2.3.5 The Contractor shall identify issues related to capability gaps, various coalition operations, and IA/CND scenarios and participate in S&T activities that address the Gaps/Limitations within the selected scenarios.

5.2.3.6 The Contractor shall attend all applicable international meetings and planning conferences and participate in working groups and provide reasonable and beneficial inputs in support of the Coalition Interoperability goals and objectives.

6 CONTRACT MONITORING

6.1 Cybersecurity Workforce (CSWF) Report

IAW clause DFARS 252.239-7001, if cybersecurity support is provided, the Contractor shall provide a Cybersecurity Workforce (CSWF) list that identifies those individuals who are IA trained and certified (CDRL A001). The prime Contractor shall be responsible for collecting, integrating, and reporting all subcontractor personnel. See applicable DD Form 1423 for additional reporting details and distribution instructions. Contractor shall verify with the COR or other government representative the proper labor category cybersecurity designation and certification requirements.

6.2 Enterprise-wide Contractor Manpower Reporting Application

The Contractor shall report all contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the DoD via a secure data collection website – Enterprise-wide Contractor Manpower Reporting Application (eCMRA). Contracted services excluded from reporting are based on Product Service Codes (PSCs). The excluded PSCs are:

(1) W, Lease/Rental of Equipment;
(2) X, Lease/Rental of Facilities;
(3) Y, Construction of Structures and Facilities;
(4) S, Utilities ONLY;
(5) V, Freight and Shipping ONLY.

The Contractor shall completely fill-in all required data fields using the following web address: https:// doncmra.nmci.navy.mil/.

Reporting inputs consists of labor hours executed during the contract/TO period of performance within each Government fiscal year (FY) which runs from October 1 through September 30.

While inputs may be reported any time during the FY, the Contractor shall report all data no later than October 31 of each calendar year. Contractors may direct questions to the help desk at https://doncmra.nmci.navy.mil.

6.3 Labor Rate Limitation Notification

For all Level of Effort (LOE) cost type, labor-hour, fixed-price LOE services contracts above the Simplified Acquisition Procedures (SAP) threshold, the Contractor shall monitor labor rates as part of the monthly Contract Status Report (CDRL A001). The Contractor shall initiate required notification (CDRL A004) where the value exceeds the threshold values specified in SPAWARNOTE 4200. The Contractor's ability to monitor labor rates effectively will be included in the contract Quality Assurance Surveillance Plan (QASP).

6.4 QUALITY ASSURANCE SURVEILLANCE PLAN (QASP)

The Task Order QASP will be used to monitor performance. Inspection and acceptance is performed by the COR on all services, data, and non-data deliverables in accordance with the Quality Assurance Surveillance Plan (QASP), Attachment 2_QASP for N00039-17-R-3068.

7 DOCUMENTATION AND DELIVERABLES

7.1 Contract Data Requirement Listings (CDRLS)

The following CDRL listing identifies the data item deliverables required under this contract and the applicable section of the PWS for which they are required. The Contractor shall establish a practical and cost-effective system for developing and tracking the required CDRLs generated under each task.

CDRL#	Description	PWS Paragraph
A001	Contract Status Report (CSR)*	6.3, 7.1.2
A002	Technical/Analysis Reports, General	5.1.1.1, 5.1.1.2, 5.1.2.1, 5.1.2.2, 5.2.1.10, 5.2.1.13, 5.2.1.14, 5.2.3.3, 5.3.1.2, 5.3.2.2, 5.3.2.3
A003	Invoice Support Documentation	As soon as Contractor submits invoice
A004	Limitation Notification & Rationale	6.3
A005	Subcontracting Status Report	FAR 52.219-14

**Note: The Contractor shall develop and submit CDRL A001 to the customer within 30 days after contract award and by the 15th of each month throughout the period of performance thereafter. The prime shall be responsible for collecting, integrating, and reporting all*

subcontractor reports. The Contractor shall report on various contract functions: performance, schedule, financial, business relations, and staffing plan. See applicable DD Form 1423 for additional reporting details and distribution instructions.

7.2 Electronic Format

At a minimum, the Contractor shall provide deliverables electronically by e-mail; hard copies are only required if requested by the Government. To ensure information compatibility, the Contractor shall guarantee all deliverables (i.e., CDRLs), data, and correspondences are provided in a format approved by the receiving government representative. The Contractor shall provide all data in an editable format compatible with customer(s) corporate standard software configuration as specified below. Contractor shall conform to the customer(s) corporate standards within 30 days of task order award unless otherwise specified. *The initial or future upgrade costs of the listed computer programs are not chargeable as a direct cost to the government*.

	Deliverable	**Format/Software to be used**
a.	Word Processing	Microsoft Word
b.	Technical Publishing	PageMaker/Interleaf/SGML/ MS Publisher
c.	Spreadsheet/Graphics	Microsoft Excel
d.	Presentations	Microsoft PowerPoint
e.	2-D Drawings/ Graphics/Schematics (new data products)	CGM/SVG, CALS Type I, TIFF/BMP, JPEG, PNG
f.	Scheduling	Microsoft Project
g.	Computer Aid Design (CAD) Drawings	AutoCAD/Visio
h.	Geographic Information System (GIS)	ArcInfo/ArcView
i.	DoDAF Architecture products	SYSCOM Architecture Diagram Interactive Explorer (SADIE), Magic Draw, PDF, Visio, TIFF/BMP, JPEG, PNG, XML, PPT

7.3 Information System

7.3.1 Electronic Communication

The Contractor shall have broadband Internet connectivity and an industry standard email system for communication with the Government. The Contractor shall be capable of Public Key Infrastructure client side authentication to DoD private web servers.

7.3.2 Information Security

Pursuant to DoDM 5200.01, the Contractor shall provide adequate security for all unclassified DoD information passing through non-DoD information systems including all subcontractor information systems utilized on the task order. The Contractor shall disseminate unclassified

DoD information within the scope of assigned duties and with a clear expectation that confidentiality is preserved. Examples of such information include the following: non-public information provided to the Contractor, information developed during the course of the task order, and privileged contract information (e.g., program schedules, contract-related tracking).

7.3.3 Safeguards

The Contractor shall protect Government information and shall provide compliance documentation validating they are meeting this requirement in accordance with DFARS Clause 252.204-7012. The Contractor and all utilized subcontractors shall abide by the following safeguards:

(a) Do not process DoD information on public computers (e.g., those available for use by the general public in kiosks or hotel business centers) or computers that do not have access control.

(b) Protect information by at least one physical or electronic barrier (e.g., locked container or room, login and password) when not under direct individual control.

(c) Sanitize media (e.g., overwrite) before external release or disposal.

(d) Encrypt all information that has been identified as controlled unclassified information (CUI) when it is stored on mobile computing devices such as laptops and personal digital assistants, or removable storage media such as portable hard drives and digital optical disks, using DoD Authorized Data-at-Rest encryption technology. NOTE: Thumb drives are not authorized for DoD work, storage, or transfer. Use GSA Awarded DAR solutions (GSA # 10359) complying with ASD-NII/DOD-CIO Memorandum, "Encryption of Sensitive Unclassified Data-at-Rest on Mobile Computing Devices and Removable Storage." The Contractor shall ensure all solutions meet FIPS 140-2 compliance requirements.

(e) Limit information transfer to subcontractors or teaming partners with a need to know and a commitment to at least the same level of protection.

(f) Transmit e-mail, text messages, and similar communications using technology and processes that provide the highest level of privacy available, given facilities, conditions, and environment. Examples of recommended technologies or processes include closed networks, virtual private networks, public key-enabled encryption, and Transport Layer Security (TLS). Encrypt organizational wireless connections and use encrypted wireless connection where available when traveling. If encrypted wireless is not available, encrypt application files (e.g., spreadsheet and word processing files), using at least application-provided password protection level encryption.

(g) Transmit voice and fax transmissions only when there is a reasonable assurance that access is limited to authorized recipients.

(h) Do not post DoD information to Web site pages that are publicly available or have access limited only by domain or Internet protocol restriction. Such information may be posted to Web

site pages that control access by user identification or password, user certificates, or other technical means and provide protection via use of TLS or other equivalent technologies. Access control may be provided by the intranet (vice the Web site itself or the application it hosts).

(i) Provide protection against computer network intrusions and data exfiltration, minimally including the following:

1. Current and regularly updated malware protection services, e.g., anti-virus, anti-spyware.

2. Monitoring and control of inbound and outbound network traffic as appropriate (e.g., at the external boundary, sub-networks, individual hosts) including blocking unauthorized ingress, egress, and exfiltration through technologies such as firewalls and router policies, intrusion prevention or detection services, and host-based security services.

3. Prompt application of security-relevant software patches, service packs, and hot fixes.

(j) As applicable, comply with other current Federal and DoD information protection and reporting requirements for specified categories of information (e.g., medical, critical program information (CPI), personally identifiable information, export controlled).

(k) Report loss or unauthorized disclosure of information in accordance with contract or agreement requirements and mechanisms.

7.3.4 Compliance

Pursuant to DoDM 5200.01, the Contractor shall include in their quality processes procedures that are compliant with information security requirements.

8 SECURITY

8.1 Organization

8.1.1 Security Classification

In accordance with clause 5252.204-9200 and the DoD Contract Security Classification Specification, DD Form 254, classified work is performed under this contract. Prior to commencement of classified work, a TOP SECRET facility clearance (FCL) shall be obtained.

The majority of the requirements of this PWS will be met at or below the SECRET level with incidental access to TOP SECRET (TS) or TOP SECRET with Sensitive Compartment Information (SCI) access requiring Joint Worldwide Intelligence Communications System (JWICS) accounts.

Incidental access to TS/SCI shall be required for research of background data to characterize analytical/task scenarios. To conduct the research, there's a requirement for access to data, meetings, discussion and entrance to SCIFs.

U.S. Government security clearance eligibility is required for incidental access and handling classified and certain controlled unclassified information (CUI), attend program meetings, and/or work within restricted areas unescorted. Access to SCI is limited to U.S. Government Facilities or other U.S. Government sponsored SCI Facilities (SCIFs) authorized on the DD254.

NATO information: This means information/documents belonging to, and circulated by, the North Atlantic Treaty Organization (NATO). Access to NATO classified information requires a final U.S. government clearance at the appropriate level and a special briefing. Contractors working on this contract may be required to access up to the NATO Secret (NS) level. The special briefing is provided by the contracting company's facility security officer (FSO). The company's FSO shall make an entry into the Joint Personnel Adjudication System (JPAS) upon personnel being "read-on" (granted access) up the NS level. Prior approval from the Government Contracting Activity's NATO Control Officer (NCO)/alternate NCO (code 83310, (619) 553-3005/3191) is required before a subcontractor can be NATO read-on; no exceptions. This contract only authorizes the prime contractor to be "read-on" up to NS level when IT personnel are working on BICES related testing.

Per Naval Intelligence Security Policy Directive 17-008 those contractors cleared SCI with SIPRnet or JWICS accounts shall be NATO read-on and complete the derivative classification training prior to being granted access to SIPRnet/JWICS; training is provided by the facility security officer. Note: there are no systems at SPAWAR Headquarters or SSCLANT that is authorized for NATO Restricted up to NATO Secret data. Specific requirements shall be identified in the DD254.

Contractors performing tasks at the TS or below level without SCI access are only received to have the NATO awareness brief and complete the derivative classification training prior to being granted access to SIPRnet; training is provided by the facility security officer.

8.1.2 Security Officer

The Contractor shall appoint a Facility Security Officer (FSO) to support those Contractor personnel requiring access to Government facility/installation and/or access to information technology systems under this task order. The FSO shall have a U.S. Government security clearance equal to or higher than the FCL requires on this task order. The FSO shall be responsible for tracking the security requirements for all personnel (subcontractors included) utilized on this task order. Responsibilities include entering and updating the personnel security related and mandatory training information within the Staffing Plan document, which is an attachment to the Contract Status Report (CDRL A001).

8.2 Personnel

The Contractor shall conform to the security provisions of DoDI 5220.22/DoD 5220.22-M – National Industrial Security Program Operating Manual (NISPOM), SECNAVINST 5510.30,

DoD 8570.01-M, and the Privacy Act of 1974. Prior to any labor hours being charged on the task order, the Contractor shall ensure all personnel (including administrative and subcontractor personnel) have obtained and can maintain favorable background investigations at the appropriate level(s) for access required for the task order and if applicable, are certified/credentialed for the Cybersecurity Workforce (CSWF). A favorable background determination is determined by either a National Agency Check with Inquiries (NACI), National Agency Check with Law and Credit (NACLC), or Single Scope Background Investigation (SSBI) and favorable Federal Bureau of Investigation (FBI) fingerprint checks. Investigations are not necessarily required for personnel performing unclassified work who do not require access to Government installations/facilities, government IT systems and IT resources, or SPAWAR/SSC Atlantic/SSC Pacific information

NOTE: If a final determination is made that an individual does not meet or cannot maintain the minimum fitness standard, the Contractor shall permanently remove the individual from customer(s) facilities and task. If an individual who has been submitted for a fitness determination or security clearance is "denied" or receives an "Interim Declination," the Contractor shall remove the individual from the customer(s) facilities and task until such time as the investigation is fully adjudicated or the individual is resubmitted and is approved. All contractor and subcontractor personnel removed from facilities or task shall cease charging labor hours directly or indirectly on task and the task order.

8.2.1 Personnel Clearance

Personnel associated with this task order shall possess a SECRET personnel security clearance (PCL). Some of the tasks issued against this task order require personnel to possess higher clearance levels such as TOP SECRET with SSBI. At the Government's request, on a case-by case basis, Top Secret (TS) clearances that consist of a Single Scope Background Investigation (SSBI) are eligible for access to Sensitive Compartmented Information (SCI). These tasks include, as a minimum, Contractor personnel having the appropriate clearances required for access to classified data as applicable. Prior to starting work on the task, Contractor personnel shall have the required clearance granted by the Department of Defense Consolidated Adjudications Facility (DoD CAF) and shall comply with IT access authorization requirements. In addition, Contractor personnel shall possess the appropriate IT level of access for the respective task and position assignment as applicable per DoDI 8500.01, DoD Instruction for Cybersecurity. Any future revision to the respective directive and instruction will be applied at the task level. Contractor personnel shall handle and safeguard any Controlled Unclassified Information (CUI) and/or classified information in accordance with appropriate Department of Defense, Navy, and customer (s) security regulations. The Contractor shall immediately report any security violation to the customer(s) Security Management Office, the COR, and Government Project Manager.

8.2.2 Access Control of Contractor Personnel

8.2.2.1 Physical Access to Government Facilities and Installations

Contractor personnel shall physically access Government facilities and installations for purposes of site visitation, supervisory and quality evaluation, work performed within Government spaces (either temporary or permanent), or meeting attendance. Individuals supporting these efforts shall comply with the latest security regulations applicable to the Government facility/installation.

(a) The majority of Government facilities require Contractor personnel to have an approved visit request on file at the facility/installation security office prior to access. The Contractor shall initiate and submit a request for visit authorization to the COR in accordance with DoD 5220.22-M (NISPOM) not later than one (1) week prior to visit. Note that timeframes may vary at each facility/installation. For admission to SPAWAR/SSC Atlantic/SSC Pacific facilities/installations, the Contractor shall forward a visit request to Joint Personnel Adjudication System (JPAS) /SMO 652366; faxed to 843-218-4045 or mailed to Space and Naval Warfare Systems Center Atlantic, P.O. Box 190022, North Charleston, SC 29419-9022, Attn: Security Office, for certification of need to know by the specified COR. For visitation to all other Government locations, the Contractor shall forward visit request documentation directly to the on-site facility/installation security office (to be identified at the task level) via approval by the COR.

(b) Depending on the facility/installation regulations, Contractor personnel shall present a proper form of identification(s) and vehicle proof of insurance or vehicle rental agreement. NOTE: SPAWARSYSCEN Atlantic facilities located on Joint Base Charleston require a Common Access Card (CAC) each time physical installation access is requested. Contractor shall contact SPAWAR/SSC Atlantic/SSC Pacific Security Office directly for latest policy.

(c) All Contractor persons engaged in work while on Government property shall be subject to inspection of their vehicles at any time by the Government, and shall report any known or suspected security violations to the Security Department at that location.

8.2.2.2 Identification and Disclosure Requirements

Pursuant to DFARS clause 211.106, Contractors shall take all means necessary to <u>not</u> represent themselves as Government employees. All Contractor personnel shall follow the identification and disclosure requirement as specified in local clause 5252.237-9602. In addition, Contractor and subcontractors shall identify themselves and their company name on attendance meeting list/minutes, documentation reviews, and their electronic digital signature.

8.2.2.3 Government Badge Requirements

As specified in contract clause 5252.204-9202, some Contract personnel shall require a Government issued picture badge. While on Government installations/facilities, Contractors shall abide by each site's security badge requirements. Various Government installations are continually updating their security requirements to meet Homeland Security Presidential Directive (HSPD-12) identification standards. Contractors are responsible for obtaining and complying with the latest security identification requirements for their personnel. Contractors shall submit valid paper work (e.g., site visit request, request for picture badge, and/or DD form

1172-2 for Common Access Card (CAC)) to the applicable Government security office via the contract COR. The Contractor's appointed Security Officer, as required in clause 5252.204-9200, shall track all personnel holding local government badges at the contract level.

8.2.2.4 Common Access Card (CAC) Requirements

Some Government facilities/installations (e.g., SPAWARSYSCEN) require Contractor personnel to have a Common Access Card (CAC) for physical access to the facilities or installations. Contractors supporting work that requires access to NMCI also requires a CAC. Granting of logical and physical access privileges remains a local policy and business operation function of the local facility. The Contractor is responsible for obtaining the latest facility/installation and IT CAC requirements from the applicable local Security Office. When a CAC is required to perform work, Contractor personnel shall be able to meet all of the following security requirements prior to work being performed:

(a) Pursuant to DoD Manual (DoDM-1000.13-M-V1), issuance of a CAC is based on the following four criteria:

1. Eligibility for a CAC - to be eligible for a CAC, Contractor personnel's access requirement shall meet one of the following three criteria: (a) individual requires access to multiple DoD facilities or access to multiple non-DoD Federal facilities on behalf of the Government on a recurring bases for a period of 6 months or more, (b) individual requires both access to a DoD facility and access to DoD network on site or remotely, or (c) individual requires remote access to DoD networks that use only the CAC logon for user identification.

2. Verification of DoD affiliation from an authoritative data source - CAC eligible personnel must be registered in the Defense Enrollment Eligibility Reporting Systems (DEERS) through either an authoritative personnel data feed from the appropriate Service or Agency or Trusted Associated Sponsorship System (TASS) (formally Contractor Verification System (CVS)).

3. Completion of background vetting requirements according to FIPS PUB 201-2 and DoD Regulation 5200.2-R - at a minimum, the completion of Federal Bureau of Investigation (FBI) fingerprint check with favorable results and submission of a National Agency Check with Inquiries (NACI) investigation to the Office of Personnel Management (OPM), or a DoD-determined equivalent investigation. NOTE: Contractor personnel requiring logical access shall obtain and maintain a favorable National Agency Check with Law and Credit (NACLC) investigation. Contractor personnel shall contact the SPAWAR/SSC Atlantic/SSC Pacific Security Office to obtain the latest CAC requirements and procedures.

4. Verification of a claimed identity - all Contractor personnel shall present two forms of identification in its original form to verify a claimed identity. The identity source documents must come from the list of acceptable documents included in Form I-9, OMB No. 115-0136, Employment Eligibility Verification. Consistent with applicable law, at least one document from the Form I-9 list must be a valid (unexpired) State or Federal Government-issued picture identification (ID). The identity documents will be inspected for authenticity, scanned, and stored in the DEERS.

(b) When a Contractor requires logical access to a Government IT system or resource (directly or indirectly), the required CAC will have a Public Key Infrastructure (PKI). A hardware solution and software (e.g., ActiveGold) is required to securely read the card via a personal computer. Pursuant to DoDM 1000.13-M-V1, CAC PKI certificates will be associated with an official Government issued e-mail address (e.g. .mil, .gov, .edu). Prior to receipt of a CAC with PKI, Contractor personnel shall complete the mandatory Cybersecurity Awareness training and submit a signed System Authorization Access Request Navy (SAAR-N) form to the contract specified COR, via the Contract Program Manager. Note: In order for personnel to maintain a CAC with PKI, each Contractor employee shall complete annual cybersecurity training. The following guidance for training and form submittal is provided; however, Contractors shall seek latest guidance from their appointed company Security Officer and the SPAWAR/SSC Atlantic/SSC Pacific Information Assurance Management (IAM) office:

1. For annual DoD Cybersecurity/IA Awareness training, Contractors shall use this site: https://twms.nmci.navy.mil/. For those Contractors requiring initial training and do not have a CAC, contact the SPAWAR/SSC Atlantic/SSC Pacific IAM office at phone number [insert applicable contract information] (843)218-6152 or e-mail questions to ssc_lant_iam_office.fcm@navy.mil for additional instructions. Training can be taken at the IAM office or online at http://iase.disa.mil/index2.html.

2. For SAAR-N form, the Contractor shall use OPNAV 5239/14 (Rev 9/2011). Contractors can obtain a form from the SPAWAR/SSC Atlantic/SSC Pacific IAM office at or from the website: https://navalforms.documentservices.dla.mil/. Digitally signed forms will be routed to the IAM office via encrypted e-mail to ssclant_it_secmtg@navy.mil.

8.2.2.5 Contractor Check-in and Check-out Procedures

All Contractor personnel requiring or possessing a government badge and/or CAC for facility and/or IT access shall have a SPAWAR/SSC Atlantic/SSC Pacific Government sponsor and be in compliance with the most current version of the Contractor Check-in and Check-out process. At task order award throughout task order completion, the Contractor shall provide necessary employee information and documentation for employees hired, transferred, and/or terminated in support of this task order within the required timeframe as cited in the Check-in and Check-out instructions. Contractor's Security Officer shall ensure all Contractor employees whose services are no longer required on contract return all applicable government documents/badges to a Government representative or the COR. NOTE: If the Contractor does not have access to the Check-In/ Check-Out website, the Contractor shall get all necessary instruction and forms from the COR.

8.2.3 Security Training

Regardless of the task order security level required, the Contractor shall be responsible for verifying applicable personnel (including subcontractors) receive all required training. At a minimum, the Contractor’s designated Security Officer shall track the following information: security clearance information; dates possessing Common Access Cards; issued & expired dates; Cybersecurity training; Privacy Act training; Personally Identifiable Information (PII) training;

Cybersecurity Workforce (CSWF) certifications and other training, as required by the customer. The Contractor shall educate employees on the procedures for the handling and production of classified material and documents, and other security measures as described in the PWS and in accordance with DoD 5220.22-M.

8.2.4 Disclosure of Information

In support of DFARS Clause 252.204-7000, Contractor employees shall not discuss or disclose any information provided to them in the performance of their duties to parties other than authorized Government and Contractor personnel who have a "need to know". The Contractor shall not use any information or documentation developed by the Contractor under direction of the Government for other purposes without the consent of the Government Contracting Officer.

8.2.5 Handling of Personally Identifiable Information (PII)

When a Contractor, including any subcontractor, is authorized access to Personally Identifiable Information (PII), the Contractor shall complete annual PII training requirements and comply with all privacy protections under the Privacy Act (Clause 52.224-1 and 52.224-2). The Contractor shall safeguard PII from theft, loss, and compromise. The Contractor shall transmit and dispose of PII in accordance with the latest DON policies. The Contractor shall not store any Government PII on their personal computers. The Contractor shall mark all developed documentation containing PII information accordingly in either the header or footer of the document: “FOUO – Privacy Sensitive. Any misuse or unauthorized disclosure may result in both criminal and civil penalties.” Any unauthorized disclosure of privacy sensitive information through negligence or misconduct can lead to Contractor removal or contract termination depending on the severity of the disclosure. Upon discovery of a PII breach, the Contractor shall immediately notify the Contracting Officer and COR. Contractors responsible for the unauthorized disclosure of PII shall be held accountable for any costs associated with breach mitigation, including those incurred as a result of having to notify personnel.

8.3 Operations Security (OPSEC) Requirements

Security programs are oriented towards protection of classified information and material. Operations Security (OPSEC) is an operations function which involves the protection of any critical information – focusing on unclassified information that may be susceptible to adversary exploitation. Pursuant to DoDD 5205.02E and SPAWARINST 3432.1, SPAWAR/SSC Atlantic/SSC Pacific’s OPSEC program implements requirements in DoD 5205.02-M – OPSEC Program Manual. Note: OPSEC requirements are applicable when contract personnel have access to classified information or unclassified Critical Program Information (CPI)/sensitive information.

8.3.1 Local and Internal OPSEC Requirement

Contractor personnel, including subcontractors if applicable, shall adhere to the OPSEC program policies and practices as cited in the SPAWARINST 3432.1 and existing local site OPSEC procedures. The Contractor shall development their own internal OPSEC program specific to the

contract and based on SPAWAR/SSC Atlantic/SSC Pacific OPSEC requirements. At a minimum, the Contractor's program shall identify the current SPAWAR/SSC Atlantic/SSC Pacific site OPSEC Officer/Coordinator.

8.3.2 OPSEC Training

Contractor shall track and ensure applicable personnel receive initial and annual OPSEC awareness training. Training may be provided by the government or a contractor's OPSEC Manager. Contractor training shall, as a minimum, cover OPSEC as it relates to contract work, discuss the Critical Information applicable in the contract and review OPSEC requirements if working at a government facilities. The Contractor shall ensure any training materials developed by the Contractor shall be reviewed by the SPAWAR/SSC Atlantic/SSC Pacific OPSEC Officer, who will ensure it is consistent with SPAWAR/SSC Atlantic/SSC Pacific OPSEC policies. OPSEC training requirements are applicable for personnel during their entire term supporting SPAWAR contracts.

8.3.3 SPAWAR/SSC Atlantic/SSC Pacific OPSEC Program

If required, the Contractor shall participate in SPAWAR OPSEC program briefings and working meetings. The Contractor shall complete any required OPSEC survey or data call within the timeframe specified.

8.3.4 Classified Contracts

OPSEC requirements identified under a classified contract shall have specific OPSEC requirements listed on the DD Form 254.

8.4 Data Handling and User Controls

8.4.1 Data Handling

At a minimum, the Contractor shall handle all data received or generated under this contract as For Official Use Only (FOUO) material. The Contractor shall handle all classified information received or generated Pursuant to the attached DD Form 254 and be in compliance with all applicable PWS references and other applicable Government policies and procedures that include DOD/Navy/SPAWAR.

8.4.2 Effective Use of Controls

The Contractor shall screen all electronic deliverables or electronically provided information for malicious code using DoD approved anti-virus software prior to delivery to the Government. The Contractor shall utilize appropriate controls (firewalls, password protection, encryption, digital certificates, etc.) at all times to protect contract related information processed, stored or transmitted on the Contractor's and Government's computers/servers to ensure confidentiality, integrity, availability, authentication and non-repudiation. The Contractor shall ensure provisions are in place to safeguard all aspects of information operations pertaining to this

contract in compliance with all applicable PWS references. In compliance with Para 6.3.3, the Contractor shall ensure Data-at-Rest is required on all portable electronic devices including storage of all types. Encryption/digital signing of communications is required for authentication and non-repudiation.

9 GOVERNMENT FACILITIES

As specified in each task, Government facilities (i.e., office space, computer hardware/software, or lab space) will be provided where required. Contractor personnel with supplied Government facilities shall be located at the location identified on each task.

10 CONTRACTOR FACILITIES

A significant portion of tasks issued under this contract require close liaison with the Government. The Contractor shall already have, or be prepared to establish, a local facility within a thirty (30)-mile radius of SPAWAR HQ, San Diego. Close proximity allows for proper contract administration duties. The Contractor's local facility shall include sufficient physical security to protect Government assets. The Contractor's facility shall meet all location to perform work requirements within 30 days after task order award. Facility space shall include offices, conference rooms, lab work, and a staging area for materials and equipment.

11 GOVERNMENT FURNISHED PROPERTY

No contract property (i.e., Government Furnished Information (GFI), Government-furnished property (GFP), or Contractor-acquired Property (CAP)) will be provided or acquired on this task order.

12 TRAVEL

The Contractor shall ensure all travel is performed pursuant to clause 5252.231-9200. If travel is required, the Contractor shall be prepared to travel, at a minimum, to the following locations:

a) Washington D.C. area
b) Norfolk, VA
c) Charleston, SC area
d) Other locations may be identified during the performance of this contract.
e) Incidental travel to locations outside the Continental limits of the United States (OCONUS) both shore and afloat will be required. Contractor employees who deploy to locations that require immunizations shall do so pursuant to DoDI 6205.4, Department of the Navy (DON)

13 PLACE OF PERFORMANCE

TS/SCI incidental tasking shall be performed at Government facilities as prescribed in the DD254. Work will be performed at the Contractor's facilities (offsite), on-site at the SPAWAR Old Town Campus (4301 Pacific Highway, San Diego, CA) and other locations as indicated below:

a) San Diego, CA. Area
b) Washington D.C. Area
c) Norfolk, VA Area
d) Other locations may be identified during the performance of this contract.

14 DATA RIGHTS

The Government shall own all data rights to the developed and collected information.