AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT	1. CONTRACT ID CODE: U	PAGE OF PAGES: 1	2

2. AMENDMENT/MODIFICATION NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO. *(If applicable)*
06	06-Feb-2015	N/A	N/A

6. ISSUED BY	CODE	7. ADMINISTERED BY *(If other than Item 6)*	CODE
SPAWAR HQ 4301 Pacific Highway San Diego CA 9211 [redacted] 619-524-3526	N00039	DCMA Manassas 14501 George Carter Way Chantilly VA 20151	S2404A

8. NAME AND ADDRESS OF CONTRACTOR *(No., street, county, State, and Zip Code)*		9A. AMENDMENT OF SOLICITATION NO.
BOOZ ALLEN HAMILTON INC 8283 Greensboro Drive McLean VA 22102		9B. DATED *(SEE ITEM 11)*
	[X]	10A. MODIFICATION OF CONTRACT/ORDER NO. N00178-04-D-4024-NS44
CAGE CODE 17038 / FACILITY CODE		10B. DATED *(SEE ITEM 13)* 08-Dec-2014

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

[ ] The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers [ ] is extended, [ ] is not extended.
Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods:
(a) By completing Items 8 and 15, and returning one (1) copy of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGEMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA *(If required)*

13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS,
IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

(*)	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: *(Specify authority)* THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.
[ ]	
[X]	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES *(such as changes in paying office, appropriation date, etc)*SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
[ ]	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:
[ ]	D. OTHER *(Specify type of modification and authority)*

E. IMPORTANT: Contractor [X] is not, [ ] is required to sign this document and return __ copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION *(Organized by UCF section headings, including solicitation/contract subject matter where feasible)*
SEE PAGE 2

15A. NAME AND TITLE OF SIGNER *(Type or print)*		16A. NAME AND TITLE OF CONTRACTING OFFICER *(Type or print)*	
		[redacted], Contracting Officer	
15B. CONTRACTOR/OFFEROR	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA	16C. DATE SIGNED
		BY /s[redacted]	06-Feb-2015
(Signature of person authorized to sign)		*(Signature of Contracting Officer)*	

GENERAL INFORMATION

1. The purpose of this modification make a correction to the General Information section, paragraph 1 of modification 03. The change is to the Type of Funds column for 7001/03/AC and 9001/02/AC from O&MN,N to OPN.

The total amount of funds obligated to the task is hereby increased from $2,506,000.00 by $0.00 to $2,506,000.00.

The total value of the order is hereby increased from [redacted] by $0.00 to [redacted].

2. Section B has been modified accordingly.

3. A conformed copy of this Task Order is attached to this modification for informational purposes only.

SECTION B SUPPLIES OR SERVICES AND PRICES

CLIN - SUPPLIES OR SERVICES

For Cost Type Items:

Item	PSC	Supplies/Services	Qty	Unit	Est. Cost	Fixed Fee	CPFF
7001	R425	Base Year Labor (Fund Type - TBD)	0.0	LO	[redacted]	[redacted]	$13,858,699.92
700101	R425	Incremental Funding ACRN AA Cybersecurity Support (Deob $97,645 per Pr 1300469581 Mod 01) (RDT&E)					
700102	R425	Incremental Funding ACRN AB CRT/Cyber Risk Assessment (O&MN,N)					
700103	R425	Incremental Funding ACRN AC CND ORT L10 Sys Eng Mgmt (OPN)					
700104	R425	Incremental Funding ACRN AD PMW-160 IA-CA Cert Authority (OPN)					
700105	R425	Incremental Funding ACRN AE PMW-160 IA Cert Authority (O&MN,N)					
700106	R425	Incremental Funding ACRN AF PMW-170 PM Support (O&MN,N)					
700107	R425	Incremental Funding ACRN AG PMW-220 EPS Analytic Support (O&MN,N)					
7101	R425	Option Year 1 Labor (Fund Type - TBD)	1.0	LO	[redacted]	[redacted]	$12,495,951.02
		Option					
7201	R425	Option Year 2 Labor (Fund Type - TBD)	1.0	LO	[redacted]	[redacted]	$12,616,016.24
		Option					
7301	R425	Option Year 3 Labor (Fund Type - TBD)	1.0	LO	[redacted]	[redacted]	$12,738,298.95
		Option					
7401	R425	Option Year 4 Labor (Fund Type - TBD)	1.0	LO	[redacted]	[redacted]	$12,862,836.19
		Option					

For ODC Items:

Item	PSC	Supplies/Services	Qty	Unit	Est. Cost
9001	R425	Base Year - Other Direct Costs (ODC) and Travel (Fund Type - TBD)	1.0	LO	[redacted]
900101	R425	Incremental Funding ACRN AB CRT/Cyber Risk Assessment (O&MN,N)			
900102	R425	Incremental Funding ACRN AC CND ORT L10 Sys Eng Mgmt (OPN)			

Item	PSC	Supplies/Services	Qty	Unit	Est. Cost
900103	R425	Incremental Funding ACRN AD PMW-160 IA-CA Cert Authority (OPN)			
900104	R425	Incremental Funding ACRN AE PMW-160 IA Cert Authority (O&MN,N)			
9101	R425	Option Year 1 - Other Direct Costs (ODC) and Travel (Fund Type - TBD)	1.0	LO	[redacted]
		Option			
9201	R425	Option Year 2 - Other Direct Costs (ODC) and Travel (Fund Type - TBD)	1.0	LO	[redacted]
		Option			
9301	R425	Option Year 3 - Other Direct Costs (ODC) and Travel (Fund Type - TBD)	1.0	LO	[redacted]
		Option			
9401	R425	Option Year 4 - Other Direct Costs (ODC) and Travel (Fund Type - TBD)	1.0	LO	[redacted]
		Option			

B-1 ADDITIONAL SLINS

Additional SLINs will be unilaterally created by the Contracting Officer during performance of this Task Order to accommodate the multiple types of funds that will be used under this Order.

B-2 OTHER DIRECT COSTS

It is anticipated that ODC costs will consist mainly of travel and incidental material costs. The Government reserves the right to increase the Other Direct Costs CLINs to reflect increases for travel and other direct costs. Travel costs shall be reimbursed based on actual, reasonable costs in accordance with the Joint Travel Regulations or with FAR 31.205-46. Travel and Other Direct Costs (ODCs) will be non-fee bearing cost elements subject to Material Handling and G&A Rates only.

B-3 FEE DETERMINATION AND PAYMENT (LEVEL OF EFFORT)

(a) Total Estimated Hours.

The total number of hours of direct labor (including overtime and subcontract hours), but excluding holiday, sick leave, vacation and other excused absence hours) estimated to be expended under this task order is [redacted] hours. The [redacted] direct labor hours include zero uncompensated overtime labor hours.

(b) Computation of Fee.

The fee per direct labor hour is computed by dividing the fixed fee amount shown in Section B by the number of estimated hours.

(c) Modifications.

If the contracting officer determines, for any reason, to adjust the task order amount or the estimated total

hours set forth above, such adjustments shall be made by task order modification. Any additional hours will be fee bearing, and the additional negotiated fee will be divided by the additional estimated hours to determine a new fee (applicable to the additional hours only). If the fee for these additional hours is different from that of the original estimated hours, these hours shall be kept separate from the original estimated total hours.

The estimated cost of the task order may be increased by written modification, if required, due to cost overruns. This increase in cost is not fee bearing and no additional hours will be added.

(d) Payment of Fee.

The Government shall pay fixed fee to the contractor on each direct labor hour performed by the contractor or subcontractor, at the rate of SEE TABLE BELOW per labor hour invoiced by the contractor subject to the contract's "Fixed Fee" clause, provided that the total of all such payments shall not exceed eighty-five percent (85%) of the fixed fee specified under the task order. Any balance of fixed fee shall be paid to the contractor, or any overpayment of fixed fee shall be repaid by the contractor, at the time of final payment.

Nothing herein shall be construed to alter or waive any of the rights or obligations of either party pursuant to the FAR 52.232-20 "Limitation of Cost" or FAR 52.232-22 "Limitation of Funds" clauses, either of which is incorporated herein by reference.

TABLE	CLIN	FIXED FEE	HOURS	FEE PER DIRECT LABOR HOUR
BASE YEAR	7001	[redacted]		[redacted]
OPTION I	7101	[redacted]		[redacted]
OPTION II	7201	[redacted]		[redacted]
OPTION III	7301	[redacted]		[redacted]
OPTION IV	7401	[redacted]		[redacted]

The fee shall be paid to the prime contractor at the per hour rate specified in this paragraph regardless of whether the contractor or subcontractor is performing the work.

The Government reserves the right to transfer unused ceiling from one period to another as needed.

B-4 LIMITATION OF LIABILITY - INCREMENTAL FUNDING (5252.232-9210)

(a) This contract is incrementally funded with respect to both cost and fee.

(b) The amounts presently available and allotted to this contract for payment of cost and fee are as follows:

ITEM(S)	AMOUNT ALLOCATED (COST AND FEE)
7001	[redacted]
9001	[redacted]

(c) The parties contemplate that the Government will allot additional amounts to this contract from time to

time by unilateral contract modification, and any such modification shall state the total amounts allotted for cost and fee, and the CLINs covered thereby.

(d) Subject to the provisions of FAR 52.232-22 "Limitation of Funds" clause of this task order, no legal liability on the part of the Government for payment in excess of the amounts provided above shall arise unless additional funds are made available and are incorporated via modification to this task order.

B-5 OPTION EXTENSION COSTS

In the event the Government exercises its rights to extend the order by up to six additional months pursuant to clause at FAR 52.217-8, Option to Extend Services, such extension will be considered to have been evaluated, as its cost shall be at the rates specified for the period that is being extended.

SECTION C DESCRIPTIONS AND SPECIFICATIONS

C-1 SPECIFICATION/STATEMENT OF WORK (DEC 1998) (SPAWAR C-301)

Work under this task order shall be performed in accordance with Attachment 1 Performance Work Statement (PWS) and Attachment 5 Contract Data Requirements Lists (CDRLs).

C-2 QUALITY ASSURANCE SURVEILLANCE PLAN (QASP)

Objective: The purpose of this plan is to provide a quality assurance plan for the services contracted under this Task Order. This plan provides a basis for the Contracting Officer's Representative (COR) to evaluate the quality of the contractor's performance. The oversight provided for in this plan, and the remedy established, will help ensure that service levels are of high quality throughout the Task Order term. The Quality Assurance Surveillance Plan is provided as Attachment 3 to this solicitation and will be included in the Task Order award.

C-3 SECURITY REQUIREMENTS (DEC 1999) (5252.204-9200)

The work to be performed under this contract as delineated in the DD Form 254, Attachment 4, involves access to and handling of classified material up to and including TOP SECRET/SCI.

In addition to the requirements of the FAR 52.204-2 "Security Requirements" clause, the Contractor shall appoint a Security Officer, who shall (1) be responsible for all security aspects of the work performed under this contract, (2) assure compliance with the National Industry Security Program Operating Manual (DODINST 5220.22M), and (3) assure compliance with any written instructions from the SPAWARSYSCOM Security Officer.

C-4 WORKWEEK (APR 2012) (5252.222-9200)

(a) A portion of the effort under this contract will be performed on a Government installation. The normal workweek for Government employees at SPAWARSYSCOM is Monday – Friday 0800 to 1630 hours. Work at this Government installation, shall be performed by the contractor within the normal workweek unless differing hours are specified on the individual task orders. Following is a list of holidays observed by the Government:

Name of Holiday	Time of Observance
New Year's Day	1 January
Martin Luther King Jr. Day	Third Monday in January
President's Day	Third Monday in February
Memorial Day	Last Monday in May
Independence Day	4 July
Labor Day	First Monday in September
Columbus Day	Second Monday in October
Veteran's Day	11 November
Thanksgiving Day	Fourth Thursday in November
Christmas Day	25 December

(b) If any of the above holidays occur on a Saturday or a Sunday, then such holiday shall be

observed by the Contractor in accordance with the practice as observed by the assigned Government employees at the using activity.

(c) If the Contractor is prevented from performance as the result of an Executive Order or an administrative leave determination applying to the using activity, such time may be charged to the contract as direct cost provided such charges are consistent with the Contractor's accounting practices.

(d) This contract does not allow for payment of overtime during the normal workweek for employees who are not exempted from the Fair Labor Standards Act unless expressly authorized by the Ordering Officer. Under Federal regulations the payment of overtime is required only when an employee works more than 40 hours in a normal week period.

(e) Periodically the Government may conduct Anti-Terrorism Force Protection (AT/FP) and/or safety security exercises which may require the Contractor to adjust its work schedule and/or place of performance to accommodate execution of the exercise. The Contractor will be required to work with its Government point of contact to adjust work schedules and/or place of performance in the case of an exercise that causes disruption of normally scheduled work hours, or disruption of access to a government facility. The contract does not allow for payment of work if schedules cannot be adjusted and/or the work cannot be executed remotely (i.e., the contractor's facility or alternate non-impacted location), during an exercise when government facilities are inaccessible.

C-5 NOTICE TO CONTRACTOR OF CERTAIN DRUG DETECTION PROCEDURES

(a) Pursuant to Navy policy applicable to both Government and contractor personnel, measures will be taken to prevent the introduction and utilization of illegal drugs and related paraphernalia into Government Work areas.

(b) In furtherance of the Navy's drug control program, unannounced periodic inspections of the following nature may be conducted by installation security authorities:

(1) Routine inspection of contractor occupied work spaces.

(2) Random inspections of vehicles on entry or exit, with drug detection dog teams as available, to eliminate them as a safe haven for storage of or trafficking in illegal drugs.

(3) Random inspections of personnel possessions on entry or exit from the installation.

(c) When there is probable cause to believe that a contractor employee on board a naval installation has been engaged in use, possession or trafficking of drugs, the installation authorities may detain said employee until the employee can be removed from the installation, or can be released to the local authorities having jurisdiction.

(d) Trafficking in illegal drug and drug paraphernalia by contract employees while on a military vessel/installation may lead to possible withdrawal or downgrading of security clearance, and/or referral for prosecution by appropriate law enforcement authorities.

(e) The contractor is responsible for the conduct of employees performing work under this contract and is, therefore, responsible to assure that employees are notified of these provisions prior to assignment.

(f) The removal of contractor personnel from a Government vessel or installation as a result of the drug offenses shall not be cause for excusable delay, nor shall such action be deemed a basis for an equitable adjustment to price, delivery or other provisions of this contract.

C-6 LABOR CATEGORY IDENTIFICATION

Correspondence, Technical Instruction, Vouchers, Invoices, Status Reports, etc., shall utilize the Contractor's standard labor category terminology as established in its proposal at time of award. See **Attachment No. 2** for Desired Personnel Qualifications. For each category of labor specified by the Government, the Offeror shall identify the corresponding company labor category/categories table:

Labor Category	**Offeror Corresponding Labor Category**
Acquisition Management Specialist	[redacted]
Logistics/Configuration Specialist	[redacted]
Program Management/Acquisition/ Finance Specialist	[redacted]
Program Manager	[redacted]
Senior Cyber Security Engineer	[redacted]
	[redacted]
Junior Network Engineer	[redacted]
General Cyber Security Engineer	[redacted]
Computer Cyber Security Systems Specialist	[redacted]

C-7 LIABILITY INSURANCE--COST TYPE CONTRACTS (5252.228-9201) (OCT 2001)

(a) The following types of insurance are required in accordance with the FAR 52.228-7 "Insurance--Liability to Third Persons" clause and shall be maintained in the minimum amounts shown:

(1) Workers' compensation and employers' liability: minimum of $100,000
(2) Comprehensive general liability: $500,000 per occurrence
(3) Automobile liability: $200,000 per person $500,000 per occurrence
$20,000 per occurrence for property damage

(b) When requested by the contracting officer, the contractor shall furnish to the Contracting Officer a certificate or written statement of insurance. The written statement of insurance must contain the following information: policy number, policyholder, carrier, amount of coverage, dates of effectiveness (i.e., performance period), and contract number. The contract number shall be cited on the certificate of insurance.

C-8 INFORMATION ASSURANCE (IA)

The contractor must follow DOD instruction DFARS 252.239-7001 Information Assurance

Contractor Training and Certification, in solicitations and contracts involving contractor performance of information assurance functions as described in DoD 8570.01–M and DFARS 239.7102-3 Information Assurance Contractor Training and Certification.

The contractor shall follow SECNAVINST 5239.3A of 20 Dec 2004 & DoD 8500.2 of 6 Feb 2003 when performing IA tasks orders.

SECTION D PACKAGING AND MARKING

D-1 SHIP TO INFORMATION

See Section G – Contracting Officer's Representative

All Deliverables shall be packaged and marked IAW Best Commercial Practice.

SECTION E INSPECTION AND ACCEPTANCE

E-1 INSPECTION AND ACCEPTANCE -- DESTINATION (JAN 2002)

Inspection and acceptance of the services to be furnished hereunder shall be made at destination by the Contracting Officer's Representative or his/her duly authorized representative.

SECTION F DELIVERABLES OR PERFORMANCE

The periods of performance for the following Items are as follows:

7001	12/8/2014 - 12/7/2015
9001	12/8/2014 - 12/7/2015

CLIN - DELIVERIES OR PERFORMANCE

The periods of performance for the following Option Items are as follows:

7101	12/08/2015 - 12/07/2016
7201	12/08/2016 - 12/07/2017
7301	12/08/2017 - 12/07/2018
7401	12/08/2018 - 12/07/2019
9101	12/08/2015 - 12/07/2016
9201	12/08/2016 - 12/07/2017
9301	12/08/2017 - 12/07/2018
9401	12/08/2018 - 12/07/2019

The above period(s) of performance for the option(s) to extend the term of the task order shall apply only if the Government exercises the option(s) as stated in Section B in accordance with the basic contract clause at FAR 52.217-8 “Option to Extend Services” or FAR 52.217-9 “Option to Extend the Term of the Contract”.

Any option CLIN period of performance which extends past the current period of performance of the basic contract is only valid to the extent that the basic contract period of performance is extended.

SECTION G CONTRACT ADMINISTRATION DATA

G-1 TYPE OF CONTRACT

This is a Cost-Plus-Fixed-Fee (CPFF) level-of-effort Task Order.

G-2 INVOICING INSTRUCTIONS

(a) Consistent with Task Order clause H-1, Segregation of Costs, the contractor shall segregate and accumulate costs for the performance of this Task Order by the appropriate Accounting Classification Reference Number (ACRN) listed in the Accounting Data provided in Section G.

(b) Each ACRN under this contract is associated to a specific program, project, or PWS paragraph. Cross-reference information for invoicing is provided in Section G, "Accounting Data." Under each ACRN; the program, project, or PWS paragraph; appropriation funds type and appropriation year are identified.

Costs incurred under the referenced program, project, or PWS paragraph shall only be billed to the associated ACRN(s). The contractor is only authorized to invoice for work completed under the program, project, or PWS paragraph referenced within each ACRN. Within each program, project, or PWS paragraph, the Contractor shall invoice in the same proportion as the amount of funding currently unliquidated (for each ACRN within the same fiscal year), starting with the earliest appropriation year.

(c) The contractor's invoice shall identify the appropriate Contract and Task Order number. For the work performed, invoiced costs shall be associated to the Contract Line Item Number (CLIN), the Contract Subline Item Number (SLIN), and the specific ACRN. Invoices submitted to the paying office that do not comply with this requirement will be returned to the contractor for resubmission. The contractor shall provide an electronic copy of each invoice to the Contracting Officer's Representative at the time of submission to WAWF.

G-3 DFAS SPECIAL PAYMENT INSTRUCTION – OTHER (SEP 2009) (252.204-0012) (PGI 204.7108(d)(12))

The payment office shall make payment from each ACRN in accordance with the amounts invoiced by CLIN/SLIN/ACRN as referenced on the contractor's invoice.

Note:

This Task Order has multiple sources of funding. DFAS Special Payment Instructions (1)-(11) uses a first-in/first-out format that is not compatible with this multiple source funded Task order. Special Payment Instruction (12) must be used to facilitate the multiple source funding structure of this Task Order for which invoicing will be made by ACRN from each CLIN/SLIN/ACRN as referenced on the contractor's invoices.

G-4 252.232-7006 WIDE AREA WORKFLOW PAYMENT INSTRUCTIONS (JUN 2012)

(a) Definitions. As used in this clause--

Department of Defense Activity Address Code (DoDAAC) is a six position code that uniquely identifies a unit, activity, or organization.

Document type means the type of payment request or receiving report available for creation in Wide Area WorkFlow (WAWF).

Local processing office (LPO) is the office responsible for payment certification when payment certification is done external to the entitlement system.

(b) Electronic invoicing. The WAWF system is the method to electronically process vendor payment requests and receiving reports, as authorized by DFARS 252.232-7003, Electronic Submission of Payment Requests and Receiving Reports.

(c) WAWF access. To access WAWF, the Contractor shall--

(1) Have a designated electronic business point of contact in the Central Contractor Registration at https://www.acquisition.gov: and

(2) Be registered to use WAWF at https://wawf.eb.mil/ following the step-by-step procedures for self-registration available at this Web site.

(d) WAWF training. The Contractor should follow the training instructions of the WAWF Web-Based Training Course and use the Practice Training Site before submitting payment requests through WAWF. Both can be accessed by selecting the ``Web Based Training'' link on the WAWF home page at https://wawf.eb.mil/.

(e) WAWF methods of document submission. Document submissions may be via Web entry, Electronic Data Interchange, or File Transfer Protocol.

(3) Document routing. The Contractor shall use the information in the Routing Data Table below

(f) WAWF payment instructions. The Contractor must use the following information when submitting payment requests and receiving reports in WAWF for this contract/order:

(1) Document type. The Contractor shall use the following document type(s).

Cost Voucher

(2) Inspection/acceptance location. The Contractor shall select the following inspection/acceptance location(s) in WAWF, as specified by the contracting officer.

N/A

(3) Document routing. The Contractor shall use the information in the Routing Data Table below only to fill in applicable fields in WAWF when creating payment requests and receiving reports in the system.

Routing Data Table*

Field Name in WAWF	Data to be entered in WAWF
Pay Official DoDAAC	HQ0338
Issue By DoDAAC	N00039
Admin DoDAAC	S2404A
Inspect By DoDAAC	N00039
Service Approver (DoDAAC)	N00039
Service Acceptor (DoDAAC)	N00039
Accept at Other DoDAAC LPO	N/A

DoDAAC N/A
DCAA Auditor DoDAAC N/A
Other DoDAAC(s) N/A

---

(4) Payment request and supporting documentation. The Contractor shall ensure a payment request includes appropriate contract line item and subline item descriptions of the work performed or supplies delivered, unit price/cost per unit, fee (if applicable), and all relevant back-up documentation, as defined in DFARS Appendix F, (e.g. timesheets) in support of each payment request.

(5) WAWF email notifications. The Contractor shall enter the email address identified below in the ``Send Additional Email Notifications'' field of WAWF once a document is submitted in the system.

PCO: [redacted]
COR: [redacted]

(g) WAWF point of contact.

(1) The Contractor may obtain clarification regarding invoicing in WAWF from the following contracting activity's WAWF point of contact. N/A

(2) For technical WAWF help, contact the WAWF helpdesk at 866-618-5988.

G-5 ACTIVITY OMBUDSMAN

The SPAWAR Ombudsman for this Task Order is:

Name: [redacted]

Code: SPAWAR 2.0B

Address: 4301 Pacific Highway, San Diego, CA 92110

Phone: (619) 524-7598

G-6 CONTRACTING OFFICER REPRESENTATIVE

Name: [redacted]
Code: SPAWAR 5.0
Address: 4301 Pacific Highway, San Diego, CA 92110
E-mail: [redacted]
Phone: 858-537-0678

G-7 CONTRACTOR PERFORMANCE APPRAISAL REPORTING SYSTEM (CPARS)

(a) Past performance information will be collected and maintained under this contract using the Department of Defense Contractor Performance Appraisal Reporting System (CPARS). CPARS is a web-enabled application that collects and manages the contractor's performance information on a given contract during a specific period of time. Additional information is available at http://www.cpars.navy.mil/.

(b) After contract award, the contractor will be given access authorization by the respective SPAWAR Focal Point, to review and comment on any element of the proposed rating before that rating becomes final. Within 60 days after contract award, the contractor shall provide in writing (or via e-mail) to the contracting officer the name, title, e-mail address and telephone number of the company individual or individuals who will have the responsibility of reviewing and approving any Contractor Performance Appraisal Report (CPAR) Report developed under the contract. If, during the life of this contract these company individual(s) are replaced by the contractor, the name, title, e-mail address and telephone number of the substitute individuals will be provided to the contracting officer within 60 days of the replacement.

Accounting Data

SLINID	PR Number	Amount
700101	130046158900001	97645.00

LLA :
AA 1741319 55RE 255 00039 0 050120 2D 000000 COST CODE: A00002585861

BASE Funding 97645.00
Cumulative Funding 97645.00

MOD 01

700101	130046158900001	(97645.00)

LLA :
AA 1741319 55RE 255 00039 0 050120 2D 000000 COST CODE: A00002585861
Cybersecurity support
(Deob $97,645 per PR 1300469581 Mod 01)

700102	1300461589-0001	270000.00

LLA :
AB 1751804 5U2N 252 00039 0 050120 2D 000000 COST CODE: A10002585861
CRT/Cyber Risk Assessment
CIN 130046158900002: $275,000.00

900101	1300461589-0001	5000.00

LLA :
AB 1751804 5U2N 252 00039 0 050120 2D 000000 COST CODE: A10002585861
CRT/Cyber Risk Assessment
CIN 130046158900002: $275,000.00

MOD 01 Funding 177355.00
Cumulative Funding 275000.00

MOD 02 Funding 0.00
Cumulative Funding 275000.00

MOD 03

700103	1300461589-0002	250000.00

LLA :
AC 1741810 M2DA 252 00039 0 050120 2D 000000 COST CODE: A20002585861
CND ORT L10 Sys Eng Mgmt
CIN 130046158900003

900102	1300461589-0002	10000.00

LLA :
AC 1741810 M2DA 252 00039 0 050120 2D 000000 COST CODE: A20002585861
CND ORT L10 Sys Eng Mgmt
CIN 130046158900003

MOD 03 Funding 260000.00
Cumulative Funding 535000.00

MOD 04 Funding 0.00
Cumulative Funding 535000.00

MOD 05

700104 1300461589-0003 430000.00
LLA :
AD 1751810 M25F 252 00039 0 050120 2D 000000 COST CODE: A30002585861
PMW-160 IA-CA Cert Authority
CIN 130046158900004

700105 1300461589-0003 405000.00
LLA :
AE 1751804 5B2B 252 00039 0 050120 2D 000000 COST CODE: A40002585861
PMW-160 IA Cert Authority
CIN 130046158900005

700106 1300461589-0003 1000000.00
LLA :
AF 1751804 5C1C 252 00039 0 050120 2D 000000 COST CODE: A50002585861
PMW-170 PM Support
CIN 130046158900006

700107 1300461589-0003 96000.00
LLA :
AG 1751804 5FIT 252 00039 0 050120 2D 000000 COST CODE: A60002585861
PMW-220 EPS Analytic Support
CIN 130046158900007

900103 1300461589-0003 20000.00
LLA :
AD 1751810 M25F 252 00039 0 050120 2D 000000 COST CODE: A30002585861
PMW-160 IA-CA Cert Authority
CIN 130046158900004

900104 1300461589-0003 20000.00
LLA :
AE 1751804 5B2B 252 00039 0 050120 2D 000000 COST CODE: A40002585861
PMW-160 IA Cert Authority
CIN 130046158900005

MOD 05 Funding 1971000.00
Cumulative Funding 2506000.00

MOD 06 Funding 0.00
Cumulative Funding 2506000.00

SECTION H SPECIAL CONTRACT REQUIREMENTS

H-1 SEGREGATION OF COSTS (DEC 2003) (5252.232-9206)

(a) The Contractor agrees to segregate costs incurred under this Task Order at the lowest level of performance, either task or subtask, rather than on a total Task Order basis, and to submit invoices reflecting costs incurred at that level. Invoices shall contain summaries of work charged during the period covered, as well as overall cumulative summaries by labor category for all work invoiced to date, by line item, task or subtask.

(b) Where multiple lines of accounting are present, the ACRN preceding the accounting citation will be found in Section B and/or Section G of the contract or in the task or delivery order that authorizes work. Payment of Contractor invoices shall be accomplished only by charging the ACRN that corresponds to the work invoiced.

H-2 DATA RIGHTS

The Data Rights clause in the basic contract is invoked for this Task Order.

H-3 CONTRACTOR PICTURE BADGE (JUL 2013) (5252.204-9202)

(a) A contractor picture badge may be issued to contractor personnel by the SPAWARSYSCOM Security Office upon receipt of a valid visit request from the Contractor and a picture badge request from the COR. A list of personnel requiring picture badges must be provided to the COR to verify that the contract or delivery/task order authorizes performance at SPAWARSYSCOM prior to completion of the picture badge request.

(b) The contractor assumes full responsibility for the proper use of the identification badge and shall be responsible for the return of the badge upon termination of personnel or expiration or completion of the contract.

(c) At the completion of the contract, the contractor shall forward to SPAWARSYSCOM Security Office a list of all unreturned badges with a written explanation of any missing badges.

(End of clause)

H-4 CONTRACTOR IDENTIFICATION (MAY 2004) (5252.237-9602)

(a) Contractor employees must be clearly identifiable while on Government property by wearing appropriate badges.

(b) Contractor employees are required to clearly identify themselves and the company they work for whenever making contact with Government personnel by telephone or other electronic means.

H-5 LIMITED RELEASE OF CONTRACTOR CONFIDENTIAL BUSINESS INFORMATION (5252.227-9207) (APRIL 2010)

(a) Definition.

"Confidential Business Information," (Information) as used in this clause, is defined as all forms and types of financial, business, economic or other types of information other than technical data or computer software/computer software documentation, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if -- (1) the owner thereof has taken reasonable measures to keep such Information secret, and (2) the Information derives independent economic value, actual or potential from not being generally known to, and not being readily ascertainable through proper means by, the public. Information does not include technical data, as that term is defined in DFARS 252.227-7013(a)(14), 252.227-7015(a)(4), and 252.227-7018(a)(19). Similarly, Information does not include computer software/computer software documentation, as those terms are defined in DFARS 252.227-7014(a)(4) and 252.227-7018(a)(4).

(b) The Space and Naval Warfare Systems Command (SPAWAR) may release to individuals employed by SPAWAR support contractors and their subcontractors Information submitted by the contractor or its subcontractors pursuant to the provisions of this contract. Information that would ordinarily be entitled to confidential treatment may be included in the Information released to these individuals. Accordingly, by submission of a proposal or execution of this contract, the Offeror or contractor and its subcontractors consent to a limited release of its Information, but only for purposes as described in paragraph (c) of this clause.

(c) Circumstances where SPAWAR may release the contractor's or subcontractors' Information include the following:

(1) To other SPAWAR contractors and subcontractors, and their employees tasked with assisting SPAWAR in handling and processing Information and documents in the administration of SPAWAR contracts, such as file room management and contract closeout; and,

(2) To SPAWAR contractors and subcontractors, and their employees tasked with assisting SPAWAR in accounting support services, including access to cost-reimbursement vouchers.

(d) SPAWAR recognizes its obligation to protect the contractor and its subcontractors from competitive harm that could result from the release of such Information. SPAWAR will permit the limited release of information under paragraphs (c)(1) and (c)(2) only under the following conditions:

(1) SPAWAR determines that access is required by other SPAWAR contractors and their subcontractors to perform the tasks described in paragraphs (c)(1) and (c)(2);

(2) Access to Information is restricted to individuals with a bona fide need to possess;

(3) Contractors and their subcontractors having access to Information have agreed under their contract or a separate corporate non-disclosure agreement to provide the same level of protection to the Information that would be provided by SPAWAR employees. Such contract terms or separate corporate non-disclosure agreement shall require the contractors and subcontractors to train their employees on how to properly handle the Information to which they will have access, and to have their employees sign company non-disclosure agreements certifying that they understand the sensitive nature of the Information and that unauthorized use of the Information could expose their company to significant liability. Copies of such employee non-disclosure agreements shall be provided to the Government;

(4) SPAWAR contractors and their subcontractors performing the tasks described in paragraphs (c)(1) or (c)(2) have agreed under their contract or a separate non-disclosure agreement to not use the Information for any purpose other than performing the tasks described in paragraphs (c)(1) and (c)(2); and,

(5) Before releasing the Information to a non-Government person to perform the tasks described in paragraphs (c)(1) and (c)(2), SPAWAR shall provide the contractor a list of the company names to which access is being granted, along with a Point of Contact for those entities.

(e) SPAWAR's responsibilities under the Freedom of Information Act are not affected by this clause.

(f) If SPAWAR satisfies the conditions listed in paragraph (d), the contractor and its subcontractors agree to indemnify and hold harmless the Government, its agents, and employees from every claim or liability, including attorney's fees, court costs, and expenses, arising out of, or in any way related to, the misuse or unauthorized modification, reproduction, release, display, or disclosure of Information provided by the contractor to the Government.

(g) The Contractor agrees to include, and require inclusion of, this clause in all subcontracts at any tier that requires the furnishing of Information.

(h) The Prime Contractor will submit a signed copy of the Information Access Agreement - Company, see Section J, Attachment 10.

H-6 REQUIRED INFORMATION ASSURANCE AND PERSONNEL SECURITY REQUIREMENTS FOR ACCESSING GOVERNMENT INFORMATION SYSTEMS AND NONPUBLIC INFORMATION (5252.237-9603) (AUG 2011)

(a) Definition. As used in this clause, "sensitive information" includes:

(i) All types and forms of confidential business information, including financial information relating to a contractor's pricing, rates, or costs, and program information relating to current or estimated budgets or schedules;

(ii) Source selection information, including bid and proposal information as defined in FAR 2.101 and FAR 3.104-4, and other information prohibited from disclosure by the Procurement Integrity Act (41 USC 423);

(iii) Information properly marked as "business confidential," "proprietary," "procurement sensitive," "source selection sensitive," or other similar markings;

(iv) Other information designated as sensitive by the Space and Naval Warfare Systems Command (SPAWAR).

(b) In the performance of the contract, the Contractor may receive or have access to information, including information in Government Information Systems and secure websites. Accessed information may include "sensitive information" or other information not previously made available to the public that would be competitively useful on current or future related procurements.

(c) Contractors are obligated to protect and safeguard from unauthorized disclosure all sensitive information to which they receive access in the performance of the contract, whether the information comes from the Government or from third parties. The Contractor shall—

(i) Utilize accessed information and limit access to authorized users only for the purposes of performing the services as required by the contract, and not for any other purpose unless authorized;

(ii) Safeguard accessed information from unauthorized use and disclosure, and not discuss, divulge, or disclose any accessed information to any person or entity except those persons authorized to receive the information as required by the contract or as authorized by Federal

statute, law, or regulation;

(iii) Inform authorized users requiring access in the performance of the contract regarding their obligation to utilize information only for the purposes specified in the contact and to safeguard information from unauthorized use and disclosure.

(iv) Execute a "Contractor Access to Information Non-Disclosure Agreement," and obtain and submit to the Contracting Officer a signed "Contractor Employee Access to Information Non-Disclosure Agreement" for each employee prior to assignment;

(v) Notify the Contracting Officer in writing of any violation of the requirements in (i) through (iv) above as soon as the violation is identified, no later than 24 hours. The notice shall include a description of the violation and the proposed actions to be taken, and shall include the business organization, other entity, or individual to whom the information was divulged.

(d) In the event that the Contractor inadvertently accesses or receives any information marked as "proprietary," "procurement sensitive," or "source selection sensitive," or that, even if not properly marked otherwise indicates the Contractor may not be authorized to access such information, the Contractor shall (i) Notify the Contracting Officer; and (ii) Refrain from any further access until authorized in writing by the Contracting Officer.

(e) The requirements of this clause are in addition to any existing or subsequent Organizational Conflicts of Interest (OCI) requirements which may also be included in the contract, and are in addition to any personnel security or Information Assurance requirements, including Systems Authorization Access Request (SAAR-N), DD Form 2875, Annual Information Assurance (IA) training certificate, SF85P, or other forms that may be required for access to Government Information Systems.

(f) Subcontracts. The Contractor shall insert paragraphs (a) through (f) of this clause in all subcontracts that may require access to sensitive information in the performance of the contract.

Mitigation Plan. If requested by the Contracting Officer, the contractor shall submit, within 45 calendar days following execution of the "Contractor Non-Disclosure Agreement," a mitigation plan for Government approval, which shall be incorporated into the contract. At a minimum, the mitigation plan shall identify the Contractor's plan to implement the requirements of paragraph (c) above and shall include the use of a firewall to separate Contractor personnel requiring access to information in the performance of the contract from other Contractor personnel to ensure that the Contractor does not obtain any unfair competitive advantage with respect to any future Government requirements due to unequal access to information. A "firewall" may consist of organizational and physical separation; facility and workspace access restrictions; information system access restrictions; and other data security measures identified, as appropriate. The Contractor shall respond promptly to all inquiries regarding the mitigation plan. Failure to resolve any outstanding issues or obtain approval of the mitigation plan within 45 calendar days of its submission may result, at a minimum, in rejection of the plan and removal of any system access.

H-7 TECHNICAL DIRECTION (COST TYPE CONTRACTS) (5252.242-9202) (APR 1992)

(a) Technical Direction may be provided to the Contractor from time to time by the Contracting Officer or Contracting Officer's Representative, if authorized, during the term (term is defined as the period of performance for the basic contract and any options that may be exercised) of this contract. Technical Direction will provide specific information relating to the tasks contained in the Statement of Work and will be provided to the contractor in writing. Any Technical Direction

issued hereunder will be subject to the terms and conditions of the contract. The contract shall take precedence if there is any conflict with any Technical Direction issued hereunder, and cannot be modified by any Technical Direction.

(b) As stated, Technical Direction shall be issued in writing and shall include, but not be limited to, the following information:

(1) date of issuance of Technical Direction;
(2) applicable contract number;
(3) technical direction identification number;
(4) description of Technical Direction;
(5) estimated cost;
(6) estimated level of effort by labor category; and
(7) signature of the PCO/COR.

(c) If the contractor does not agree with the estimated cost specified on the technical direction, or considers the technical direction to be outside the scope of the contract, he shall notify the PCO or COR immediately and, in the case of the estimated cost, arrive at a general agreement to the cost of the task. In the case of the direction requiring work that is out of the scope of the contract, the contractor shall not proceed with the effort unless and until the PCO executes a contract modification to include the change in scope.

H-8 ORGANIZATIONAL CONFLICT OF INTEREST

The Organizational Conflict of Interest clause in the Contractor's basic Seaport IDIQ Contract is incorporated in this Task Order by reference.

H-9 ORGANIZATIONAL CONFLICT OF INTEREST

(a) *Definitions.*

"Support Services" are services provided to support and assist a program office or staff code with their acquisition responsibilities, including but not limited to, program management support services, preparing program budget submissions, business financial reporting or accounting services, data collection and reporting, general administration, performance and earned value monitoring; or advisory and assistance services including but not limited to consultant services, requirements analysis and planning, contract management, systems engineering and technical direction, logistics management, information technology management, test and evaluation, production and installation management.

"Prime Mission Products" are the primary product(s) for which the program office or competency has acquisition responsibility and for which they may obtain support services to assist in acquiring, including but not limited to the design, development, production or sustainment of hardware, software or firmware related to acquisition programs of record or other projects.

(b) The Contracting Officer has determined that potentially significant Organizational Conflicts of Interest (OCIs) may arise due to the nature of the work the Contractor will perform under this contract that may preclude the Contractor from being awarded future SPAWAR contracts in a related area. Whereas the Contractor has agreed to undertake this contract to provide "support

services," it is agreed that the Contractor shall be ineligible to act as a prime contractor, consultant, or subcontractor to any prime contractor or subcontractor at any tier who is to supply the "prime mission products" related to, or arising from the "support services" provided by the Contractor. Specifically, the Contractor shall be ineligible to act as a prime contractor, consultant, or subcontractor to any prime contractor or subcontractor at any tier for task orders awarded under the SPAWAR Sea Enterprise II Global C4ISR Installation Multiple Award Contract as well the follow-on SPAWAR C4ISR Installation contract(s). Additionally, should the Contractor's performance under this task order give rise to OCI issues with respect to future SPAWAR "support services" procurements, the Contractor shall be similarly ineligible.

(d) These restrictions shall apply the prime awardee of this task order. This clause shall remain in effect during the life of this task order (including option periods, if exercised) and for one (1) year after completion of this task order. This restriction does not apply to any recompetition for equipment or services furnished pursuant to this task order.

(e) The Contractor shall flow down this clause to any subcontractors or consultants that have access to information, participate in the development of data, or perform any other efforts which are subject to terms of this clause at the prime contractor level.

H-10 NOTIFICATION CONCERNING DETERMINATION OF SMALL BUSINESS SIZE STATUS

For the purposes of FAR clauses 52.219-6, NOTICE OF TOTAL SMALL BUSINESS SET-ASIDE, 52.219-3, NOTICE OF TOTAL HUBZONE SET-ASIDE, 52.219-18, NOTIFICATION OF COMPETITION LIMITED TO ELIGIBLE 8(A) CONCERNS, and 52.219-27 NOTICE OF TOTAL SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS SET-ASIDE, the determination of whether a small business concern is independently owned and operated, not dominant in the field of operation in which it is bidding on Government contracts, and qualified as a small business under the size standards in this solicitation, and further, meets the definition of a HUBZone small business concern, a small business concern certified by the SBA for participation in the SBA's 8(a) program, or a service disabled veteran-owned small business concern, as applicable, shall be based on the status of said concern at the time of award of the SeaPort-e MACs and as further determined in accordance with Special Contract Requirement H-19.

H-11 REIMBURSEMENT OF TRAVEL COSTS (JAN 2006) (5252.231-9200)

(a) Contractor Request and Government Approval of Travel

Any travel under this contract must be specifically requested in writing, by the contractor prior to incurring any travel costs. If this contract is a definite or indefinite delivery contract, then the written Government authorization will be by task/delivery orders issued by the Ordering Officer or by a modification to an issued task/delivery order. If this contract is not a definite or indefinite delivery contract, then the written Government authorization will be by written notice of

approval from the Contracting Officer's Representative (COR). The request shall include as a minimum, the following:

(1) Contract number
(2) Date, time, and place of proposed travel
(3) Purpose of travel and how it relates to the contract
(4) Contractor's estimated cost of travel
(5) Name(s) of individual(s) traveling and;
(6) A breakdown of estimated travel and per diem charges.

(b) General

(1) The costs for travel, subsistence, and lodging shall be reimbursed to the contractor only to the extent that it is necessary and authorized for performance of the work under this contract. The costs for travel, subsistence, and lodging shall be reimbursed to the contractor in accordance with the Federal Acquisition Regulation (FAR) 31.205-46, which is incorporated by reference into this contract. As specified in FAR 31.205-46(a) (2), reimbursement for the costs incurred for lodging, meals and incidental expenses (as defined in the travel regulations cited subparagraphs (b)(1)(i) through (b)(1)(iii) below) shall be considered to be reasonable and allowable only to the extent that they do not exceed on a daily basis the maximum per diem rates in effect at the time of travel as set forth in the following:

(i) Federal Travel Regulation prescribed by the General Services Administration for travel in the contiguous 48 United States;

(ii) Joint Travel Regulation, Volume 2, DoD Civilian Personnel, Appendix A, prescribed by the Department of Defense for travel in Alaska, Hawaii, The Commonwealth of Puerto Rico, and the territories and possessions of the United States; or

(iii) Standardized Regulations, (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances in Foreign Areas" prescribed by the Department of State, for travel in areas not covered in the travel regulations cited in subparagraphs (b)(1)(i) and (b)(1)(ii) above.

(2) Personnel in travel status from and to the contractor's place of business and designated work site or vice versa, shall be considered to be performing work under the contract, and contractor shall bill such travel time at the straight (regular) time rate; however, such billing shall not exceed eight hours per person for any one person while in travel status during one calendar day.

(c) Per Diem

(1) The contractor shall not be paid per diem for contractor personnel who reside in the metropolitan area in which the tasks are being performed. Per diem shall not be paid on services performed at contractor's home facility and at any facility required by the contract, or at any location within a radius of 50 miles from the contractor's home facility and any facility required by this contract.

(2) Costs for subsistence and lodging shall be paid to the contractor only to the extent that overnight stay is necessary and authorized in writing by the Government for performance of the work under this contract per paragraph (a). When authorized, per diem shall be paid by the contractor to its employees at a rate not to exceed the rate specified in the travel regulations cited in FAR 31.205-46(a)(2) and authorized in writing by the Government. The authorized per diem rate shall be the same as the prevailing locality per diem rate.

(3) Reimbursement to the contractor for per diem shall be limited to payments to employees not

to exceed the authorized per diem and as authorized in writing by the Government per paragraph (a). Fractional parts of a day shall be payable on a prorated basis for purposes of billing for per diem charges attributed to subsistence on days of travel. The departure day from the Permanent Duty Station (PDS) and return day to the PDS shall be 75% of the applicable per diem rate. The contractor shall retain supporting documentation for per diem paid to employees as evidence of actual payments, as required by the FAR 52.216-7 "Allowable Cost and Payment" clause of the contract.

(d) Transportation

(1) The contractor shall be paid on the basis of actual amounts paid to the extent that such transportation is necessary for the performance of work under the contract and is authorized in writing by the Government per paragraph (a).

(2) The contractor agrees, in the performance of necessary travel, to use the lowest cost mode commensurate with the requirements of the mission and in accordance with good traffic management principles. When it is necessary to use air or rail travel, the contractor agrees to use coach, tourist class or similar accommodations to the extent consistent with the successful and economical accomplishment of the mission for which the travel is being performed.

Documentation must be provided to substantiate non-availability of coach or tourist if business or first class is proposed to accomplish travel requirements.

(3) When transportation by privately owned conveyance (POC) is authorized, the contractor shall be paid on a mileage basis not to exceed the applicable Government transportation rate specified in the travel regulations cited in FAR 31.205-46(a)(2) and is authorized in writing by the Government per paragraph (a).

(4) When transportation by privately owned (motor) vehicle (POV) is authorized, required travel of contractor personnel, that is not commuting travel, may be paid to the extent that it exceeds the normal commuting mileage of such employee. When an employee's POV is used for travel between an employee's residence or the Permanent Duty Station and one or more alternate work sites within the local area, the employee shall be paid mileage for the distance that exceeds the employee's commuting distance.

(5) When transportation by a rental automobile, other special conveyance or public conveyance is authorized, the contractor shall be paid the rental and/or hiring charge and operating expenses incurred on official business (if not included in the rental or hiring charge). When the operating expenses are included in the rental or hiring charge, there should be a record of those expenses available to submit with the receipt. Examples of such operating expenses include: hiring charge (bus, streetcar or subway fares), gasoline and oil, parking, and tunnel tolls.

(6) Definitions:

(i) "Permanent Duty Station" (PDS) is the location of the employee's permanent work assignment (i.e., the building or other place where the employee regularly reports for work.

(ii) "Privately Owned Conveyance" (POC) is any transportation mode used for the movement of persons from place to place, other than a Government conveyance or common carrier, including a conveyance loaned for a charge to, or rented at personal expense by, an employee for transportation while on travel when such rental conveyance has not been authorized/approved as a Special Conveyance.

(iii) "Privately Owned (Motor) Vehicle (POV)" is any motor vehicle (including an automobile, light truck, van or pickup truck) owned by, or on a long-term lease (12 or more months) to, an employee or that employee's dependent for the primary purpose of providing personal transportation, that:

(a) is self-propelled and licensed to travel on the public highways;

(b) is designed to carry passengers or goods; and

(c) has four or more wheels or is a motorcycle or moped.

(iv) "Special Conveyance" is commercially rented or hired vehicles other than a POC and other than those owned or under contract to an agency.

(v) "Public Conveyance" is local public transportation (e.g., bus, streetcar, subway, etc) or taxicab.

(iv) "Residence" is the fixed or permanent domicile of a person that can be reasonably justified as a bona fide residence.

EXAMPLE 1: Employee's one way commuting distance to regular place of work is 7 miles. Employee drives from residence to an alternate work site, a distance of 18 miles. Upon completion of work, employee returns to residence, a distance of 18 miles.

In this case, the employee is entitled to be reimbursed for the distance that exceeds the normal round trip commuting distance (14 miles). The employee is reimbursed for 22 miles (18 + 18 -14 = 22).

EXAMPLE 2: Employee's one way commuting distance to regular place of work is 15 miles. Employee drives from residence to an alternate work site, a distance of 5 miles. Upon completion of work, employee returns to residence, a distance of 5 miles.

In this case, the employee is not entitled to be reimbursed for the travel performed (10 miles), since the distance traveled is less than the commuting distance (30 miles) to the regular place of work.

EXAMPLE 3: Employee's one way commuting distance to regular place of work is 15 miles. Employee drives to regular place of work. Employee is required to travel to an alternate work site, a distance of 30 miles. Upon completion of work, employee returns to residence, a distance of 15 miles.

In this case, the employee is entitled to be reimbursed for the distance that exceeds the normal round trip commuting distance (30 miles). The employee is reimbursed for 30 miles (15 + 30 + 15 - 30 = 30).

EXAMPLE 4: Employee's one way commuting distance to regular place of work is 12 miles. In the morning the employee drives to an alternate work site (45 miles). In the afternoon the employee returns to the regular place of work (67 miles). After completion of work, employee returns to residence, a distance of 12 miles.

In this case, the employee is entitled to be reimbursed for the distance that exceeds the normal round trip commuting distance (24 miles). The employee is reimbursed for 100 miles (45 + 67 + 12 - 24 = 100).

EXAMPLE 5: Employee's one way commuting distance to regular place of work is 35 miles. Employee drives to the regular place of work (35 miles). Later, the employee drives to alternate work site #1 (50 miles) and then to alternate work site #2 (25 miles). Employee then drives to residence (10 miles).

In this case, the employee is entitled to be reimbursed for the distance that exceeds the normal commuting distance (70 miles). The employee is reimbursed for 50 miles (35 + 50 + 25 + 10 - 70 = 50).

EXAMPLE 6: Employee's one way commuting distance to regular place of work is 20 miles. Employee drives to the regular place of work (20 miles). Later, the employee drives to alternate

work site #1 (10 miles) and then to alternate work site #2 (5 miles). Employee then drives to residence (2 miles).

In this case, the employee is not entitled to be reimbursed for the travel performed (37 miles), since the distance traveled is less than the commuting distance (40 miles) to the regular place of work.

H-12 AUTHORIZED CHANGES ONLY BY THE CONTRACTING OFFICER (5252.243-9600) (JAN 1992)

(a) Except as specified in paragraph (b) below, no order, statement, or conduct of Government personnel who visit the Contractor's facilities or in any other manner communicates with Contractor personnel during the performance of this contract shall constitute a change under the Changes clause of this contract.

(b) The Contractor shall not comply with any order, direction or request of Government personnel unless it is issued in writing and signed by the Contracting Officer, or is pursuant to specific authority otherwise included as a part of this contract.

(c) The Contracting Officer is the only person authorized to approve changes in any of the requirements of this contract and notwithstanding provisions contained elsewhere in this contract, the said authority remains solely the Contracting Officer's. In the event the contractor effects any change at the direction of any person other than the Contracting Officer, the change will be considered to have been made without authority and no adjustment will be made in the contract price to cover any increase in charges incurred as a result thereof. The address and telephone number of the Contracting Officer is:

NAME: Patrick Dimla
ADDRESS: 4301 Pacific Highway, San Diego, CA 92110
TELEPHONE: (619) 524-7179
E-MAIL: patrick.dimla@navy.mil

H-13 EMPLOYMENT OF NAVY PERSONNEL RESTRICTED (5252.209-9206) (DEC 1999)

In performing this contract, the Contractor will not use as a consultant or employ (on either a full or part-time basis) any active duty Navy personnel (civilian or military) without the prior approval of the Contracting Officer. Such approval may be given only in circumstances where it is clear that no law and no DOD or Navy instructions, regulations, or policies might possibly be contravened and no appearance of a conflict of interest will result.

H-14 ENTERPRISE CONTRACTOR MANPOWER REPORTING APPLICATION (ECMRA)

The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the Space and Naval Warfare Systems Command (SPAWAR) via a secure data collection site. The contractor is required to completely fill in all required data fields using the following web address https://doncmra.nmci.navy.mil.

Reporting inputs (from contractors) will be for the labor executed during the period of performance during each Government fiscal year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year. Contractors may direct questions to the help desk, linked at https://doncmra.nmci.navy.mil.

SECTION I CONTRACT CLAUSES

I-1 OPTION TO EXTEND SERVICES (52.217-8) (NOV 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor.

I-2 OPTION TO EXTEND THE TERM OF THE CONTRACT (52.217-9) (MAR 2008)

(a) The Government may extend the term of this contract by written notice to the Contractor on or before the expiration date of the Task Order.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed five years, six months.

I-3 SUBCONTRACTS (OCT 2010) - ALTERNATE I (FAR 52.244-2) (OCT 2010)

(a) *Definitions.* As used in this clause—

"Approved purchasing system" means a Contractor's purchasing system that has been reviewed and approved in accordance with Part 44 of the Federal Acquisition Regulation (FAR)

"Consent to subcontract" means the Contracting Officer's written consent for the Contractor to enter into a particular subcontract.

"Subcontract" means any contract, as defined in FAR Subpart 2.1, entered into by a subcontractor to furnish supplies or services for performance of the prime contractor a subcontract. It includes, but is not limited to, purchase orders, and changes and modifications to purchase orders.

(b) When this clause is included in a fixed-price type contract, consent to subcontract is required only on unpriced contract actions (including unpriced modifications or unpriced delivery orders), and only if required in accordance with paragraph (c) or (d) of this clause.

(c) If the Contractor does not have an approved purchasing system, consent to subcontract is required for any subcontract that-

(1) Is of the cost-reimbursement, time-and-materials, or labor-hour type; or

(2) Is fixed-price and exceeds—

(i) For a contract awarded by the Department of Defense, the Coast Guard, or the National Aeronautics and Space Administration, the greater of the simplified acquisition threshold or 5 percent of the total estimated cost of the contract; or

(ii) For a contract awarded by a civilian agency other than the Coast Guard and the National Aeronautics and Space Administration, either the simplified acquisition threshold or 5 percent of the total estimated cost of the contract.

(d) If the Contractor has an approved purchasing system, the Contractor nevertheless shall obtain the Contracting Officer's written consent before entering into *any* subcontract over the Simplified Acquisition Threshold (SAT) that was not initially proposed regardless of whether the potential subcontractor(s) have an approved accounting system and before placing the following subcontracts:

(e)(1) The Contractor shall notify the Contracting Officer reasonably in advance of placing any subcontract or modification thereof for which consent is required under paragraph (b), (c), or (d) of this clause, including the following information:

(i) A description of the supplies or services to be subcontracted.

(ii) Identification of the type of subcontract to be used.

(iii) Identification of the proposed subcontractor.

(iv) The proposed subcontract price.

(v) The subcontractor's current, complete, and accurate cost or pricing data and Certificate of Current Cost or Pricing Data, if required by other contract provisions.

(vi) The subcontractor's Disclosure Statement or Certificate relating to Cost Accounting Standards when such data are required by other provisions of this contract.

(vii) A negotiation memorandum reflecting -

(A) The principal elements of the subcontract price negotiations;

(B) The most significant considerations controlling establishment of initial or revised prices;

(C) The reason cost or pricing data were or were not required;

(D) The extent, if any, to which the Contractor did not rely on the subcontractor's cost or pricing data in determining the price objective and in negotiating the final price;

(E) The extent to which it was recognized in the negotiation that the subcontractor's cost or pricing data were not accurate, complete, or current; the action taken by the Contractor and the subcontractor; and the effect of any such defective data on the total price negotiated;

(F) The reasons for any significant difference between the Contractor's price objective and the price negotiated; and

(G) A complete explanation of the incentive fee or profit plan when incentives are used. The explanation shall identify each critical performance element, management decisions used to quantify each incentive element, reasons for the incentives, and a summary of all trade-off possibilities considered.

(2) If the Contractor has an approved purchasing system and consent is not required under paragraph (c) or (d) of this clause, the Contractor nevertheless shall notify the Contracting Officer reasonably in advance of entering into any (i) cost-plus-fixed-fee subcontract, or (ii) fixed-price subcontract that exceeds either the simplified acquisition threshold or 5 percent of the total estimated cost of this contract. The notification shall include the information required by paragraphs (e)(1)(i) through (e)(1)(iv) of this clause.

(f) Unless the consent or approval specifically provides otherwise, neither consent by the Contracting Officer to any subcontract nor approval of the Contractor's purchasing system shall constitute a determination -

(1) Of the acceptability of any subcontract terms or conditions;

(2) Of the allowability of any cost under this contract; or

(3) To relieve the Contractor of any responsibility for performing this contract.

(g) No subcontract or modification thereof placed under this contract shall provide for payment on a cost-plus-a-percentage-of-cost basis, and any fee payable under cost-reimbursement type subcontracts shall not exceed the fee limitations in FAR 15.404-4(c)(4)(i).

(h) The Contractor shall give the Contracting Officer immediate written notice of any action or suit filed and prompt notice of any claim made against the Contractor by any subcontractor or vendor that, in the opinion of the Contractor, may result in litigation related in any way to this contract, with respect to which the Contractor may be entitled to reimbursement from the Government.

(i) The Government reserves the right to review the Contractor's purchasing system as set forth in FAR Subpart 44.3.

(j) Paragraphs (c) and (e) of this clause do not apply to the following subcontracts, which were evaluated during negotiations:

[redacted]

I-4 RESTRICTIONS ON THE USE OF MANDATORY ARBITRATION AGREEMENTS (252.222-7006) (DEC 2010)

(a) *Definitions.* As used in this clause–

"Covered subcontractor" means any entity that has a subcontract valued in excess of $1 million, except a subcontract for the acquisition of commercial items, including commercially available off-the-shelf items.

"Subcontract" means any contract, as defined in Federal Acquisition Regulation subpart 2.1, to furnish supplies or services for performance of this contract or a higher-tier subcontract thereunder.

(b) The Contractor—

(1) Agrees not to–

(i) Enter into any agreement with any of its employees or independent contractors that requires, as a condition of

employment, that the employee or independent contractor agree to resolve through arbitration

(A) Any claim under title VII of the Civil Rights Act of 1964; or

(B) Any tort related to or arising out of sexual assault or harassment, including assault and battery, intentional infliction of emotional distress, false imprisonment, or negligent hiring, supervision, or retention; or (ii) Take any action to enforce any provision of an existing agreement with an employee or independent contractor that mandates that the employee or independent contractor resolve through arbitration–

(A) Any claim under title VII of the Civil Rights Act of 1964; or

(B) Any tort related to or arising out of sexual assault or harassment, including assault and battery, intentional infliction of emotional distress, false imprisonment, or negligent hiring, supervision, or retention; and

(2) Certifies, by signature of the contract, that it requires each covered subcontractor to agree not to enter into, and not to take any action to enforce, any provision of any existing agreements, as described in paragraph (b)(1) of this clause, with respect to any employee or independent contractor performing work related to such subcontract.

(c) The prohibitions of this clause do not apply with respect to a contractor's or subcontractor's agreements with employees or independent contractors that may not be enforced in a court of the United States.

(d) The Secretary of Defense may waive the applicability of the restrictions of paragraph (b) of this clause in accordance with Defense Federal Acquisition Regulation Supplement 222.7404.

I-5 CLAUSES INCORPORATED BY REFERENCE (FAR 52.252-2) (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be

accessed electronically at this/these address(es):

http://farsite.hill.af.mil/
http://www.arnet.gov/far/

The following clauses are incorporated into this task order in addition to the clauses included in the Basic Seaport Contract, Section I.

FAR SOURCE	TITLE	DATE
52.203-16	Preventing Personal Conflicts of Interest	DEC 2011
52.204-10	Reporting Executive Compensation and First-Tier Subcontract Awards	FEB 2012
252.242-7005	Contractor Business Systems	FEB 2012
252.242-7006	Accounting System Administration	FEB 2012

I-6 252.204-7012 Safeguarding of Unclassified Controlled Technical Information.

SAFEGUARDING OF UNCLASSIFIED CONTROLLED TECHNICAL INFORMATION (NOV 2013)

(a) *Definitions*. As used in this clause—

"Adequate security" means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.

"Attribution information" means information that identifies the Contractor, whether directly or indirectly, by the grouping of information that can be traced back to the Contractor (e.g., program description or facility locations).

"Compromise" means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

"Contractor information system" means an information system belonging to, or operated by or for, the Contractor.

"Controlled technical information" means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information is to be marked with one of the distribution statements B-through-F, in accordance with DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

"Cyber incident" means actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein.

"Exfiltration" means any unauthorized release of data from within an information system. This includes copying the data through covert network channels or the copying of data to unauthorized media.

"Media" means physical devices or writing surfaces including, but is not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which information is recorded, stored, or printed within an information system.

"Technical information" means technical data or computer software, as those terms are defined in the clause at DFARS 252.227-7013, Rights in Technical Data-Non Commercial Items, regardless of whether or not the clause is incorporated in this solicitation or contract. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

(b) *Safeguarding requirements and procedures for unclassified controlled technical information*. The Contractor shall provide adequate security to safeguard unclassified controlled technical information from compromise. To provide adequate security, the Contractor shall—

(1) Implement information systems security in its project, enterprise, or company-wide unclassified information technology system(s) th have unclassified controlled technical information resident on or transiting through them. The information systems security program sha implement, at a minimum—

(i) The specified National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 security con following table; or

(ii) If a NIST control is not implemented, the Contractor shall submit to the Contracting Officer a written explanation

(A) The required security control identified in the following table is not applicable; or

(B) An alternative control or protective measure is used to achieve equivalent protection.

(2) Apply other information systems security requirements when the Contractor reasonably determines that information systems security measures, in addition to those identified in paragraph (b)(1) of this clause, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability.

Table 1 -- Minimum Security Controls for Safeguarding

Minimum required security controls for unclassified controlled technical information requiring safeguarding in accordance with paragraph (d) of this clause. (A description of the security controls is in the NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations" (http://csrc.nist.gov/publications/PubsSPs.html).)

Access	Audit &	Identification	Media	System &

Control	Accountability	and Authentication	Protection	Comm Protection
AC-2	AU-2	IA-2	MP-4	SC-2
AC-3(4)	AU-3	IA-4	MP-6	SC-4
AC-4	AU-6(1)	IA-5(1)		SC-7
AC-6	AU-7		Physical and Environmental Protection	SC-8(1)
AC-7	AU-8	Incident Response	PE-2	SC-13
AC-11(1)	AU-9	IR-2	PE-3	
AC-17(2)		IR-4	PE-5	SC-15
AC-18(1)	Configuration Management	IR-5		SC-28
AC-19	CM-2	IR-6	Program Management	
AC-20(1)	CM-6		PM-10	System & Information Integrity
AC-20(2)	CM-7	Maintenance		SI-2
AC-22	CM-8	MA-4(6)	Risk Assessment	SI-3
		MA-5	RA-5	SI-4
Awareness & Training	Contingency Planning	MA-6		
AT-2	CP-9			

Legend:

AC: Access Control MA: Maintenance

AT: Awareness and Training MP: Media Protection

AU: Auditing and Accountability PE: Physical & Environmental Protection

CM: Configuration Management PM: Program Management

CP: Contingency Planning RA: Risk Assessment

IA: Identification and Authentication SC: System & Communications Protection

IR: Incident Response SI: System & Information Integrity

(c) *Other requirements*. This clause does not relieve the Contractor of the requirements specified by applicable statutes or other Federal and DoD safeguarding requirements for Controlled Unclassified Information (CUI) as established by Executive Order 13556, as well as regulations and

guidance established pursuant thereto.

(d) *Cyber incident and compromise reporting.*

(1) *Reporting requirement.* The Contractor shall report as much of the following information as can be obtained to the Department of De (http://dibnet.dod.mil/) within 72 hours of discovery of any cyber incident, as described in paragraph (d)(2) of this clause, that affects unc controlled technical information resident on or transiting through the Contractor's unclassified information systems:

(i) Data Universal Numbering System (DUNS).

(ii) Contract numbers affected unless all contracts by the company are affected.

(iii) Facility CAGE code if the location of the event is different than the prime Contractor location.

(iv) Point of contact if different than the POC recorded in the System for Award Management (address, position, teleph

(v) Contracting Officer point of contact (address, position, telephone, email).

(vi) Contract clearance level.

(vii) Name of subcontractor and CAGE code if this was an incident on a Sub-contractor network.

(viii) DoD programs, platforms or systems involved.

(ix) Location(s) of compromise.

(x) Date incident discovered.

(xi) Type of compromise (e.g., unauthorized access, inadvertent release, other).

(xii) Description of technical information compromised.

(xiii) Any additional information relevant to the information compromise.

(2) *Reportable cyber incidents.* Reportable cyber incidents include the following:

(i) A cyber incident involving possible exfiltration, manipulation, or other loss or compromise of any unclassified con information resident on or transiting through Contractor's, or its subcontractors', unclassified information systems.

(ii) Any other activities not included in paragraph (d)(2)(i) of this clause that allow unauthorized access to the Contrac information system on which unclassified controlled technical information is resident on or transiting.

(3) *Other reporting requirements.* This reporting in no way abrogates the Contractor's responsibility for additional safeguarding and cyb incident reporting requirements pertaining to its unclassified information systems under other clauses that may apply to its contract, or a result of other U.S. Government legislative and regulatory requirements that may apply (e.g., as cited in paragraph (c) of this clause).

(4) *Contractor actions to support DoD damage assessment.* In response to the reported cyber incident, the Contractor shall—

(i) Conduct further review of its unclassified network for evidence of compromise resulting from a cyber incident to in to, identifying compromised computers, servers, specific data and users accounts. This includes analyzing information the compromise, as well as other information systems on the network that were accessed as a result of the compromise

(ii) Review the data accessed during the cyber incident to identify specific unclassified controlled technical information programs, systems or contracts, including military programs, systems and technology; and

(iii) Preserve and protect images of known affected information systems and all relevant monitoring/packet capture data the cyber incident to allow DoD to request information or decline interest.

(5) *DoD damage assessment activities.* If DoD elects to conduct a damage assessment, the Contracting Officer will request that the Cont point of contact identified in the incident report at (d)(1) of this clause provide all of the damage assessment information gathered in acco with paragraph (d)(4) of this clause. The Contractor shall comply with damage assessment information requests. The requirement to sha and images exists unless there are legal restrictions that limit a company's ability to share digital media. The Contractor shall inform th Contracting Officer of the source, nature, and prescription of such limitations and the authority responsible.

(e) *Protection of reported information.* Except to the extent that such information is lawfully publicly available without restrictions, the Government will protect information reported or otherwise provided to DoD under this clause in accordance with applicable statutes, regulations, and policies. The Contractor shall identify and mark attribution information reported or otherwise provided to the DoD. The Government may use information, including attribution information and disclose it only to authorized persons for purposes and activities consistent with this clause.

(f) Nothing in this clause limits the Government's ability to conduct law enforcement or counterintelligence activities, or other lawful activities

in the interest of homeland security and national security. The results of the activities described in this clause may be used to support an investigation and prosecution of any person or entity, including those attempting to infiltrate or compromise information on a contractor information system in violation of any statute.

(g) *Subcontracts*. The Contractor shall include the substance of this clause, including this paragraph (g), in all subcontracts, including subcontracts for commercial items.

(End of clause)

SECTION J LIST OF ATTACHMENTS

Attachment 1 - Performance Work Statement (PWS)

Attachment 2 - Personnel Qualifications

Attachment 3 - Quality Assurance Surveillance Plan (QASP)

Attachment 4 - DD254

Attachment 5 - Monthly Status Report (MSR) CDRL A001

Attachment 5(a) - CDRL A001 MSR Attachment 1

Attachment 5(b) - CDRL A001 MSR Attachment 2

Performance Work Statement (PWS)
For Official Use Only

Cyber Security, Information Assurance and Technical Authority Support Services for the SPAWAR CHENG

1.0 INTRODUCTION

The Department of the Navy (DoN), Space and Naval Warfare System Command (SPAWAR) is acquiring Cyber Security (CS), Information Assurance (IA) and Technical Authority (TA) support services for the Office of the Chief Engineer (CHENG) (SPAWAR 5.0) and various C4ISR programs in the specific area of Information Assurance/Cyber Security.

2.0 BACKGROUND

Information is a vital source of power for the United States Navy (USN). Per Chief of Naval Operations (CNO) guidance, the ability to achieve Decision Superiority through Information Dominance (ID), especially in Intelligence, Surveillance, and Reconnaissance (ISR), Command, Control, Communications, and Computers (C4), Information Operations (IO) and Cyber Warfare, is critical to the Navy's future success. Information Assurance ensures confidentiality, integrity and availability to Navy information systems identifying, monitoring, and restricting unauthorized accesses. As the Navy continues toward a net-centric information sharing environment, IA is an operational necessity to ensure risks are identified, evaluated, and countered in a reliable and timely manner.

The SPAWAR Chief Engineer (CHENG) is the Navy's Information Dominance engineering authority and will establish and exercise Technical Leadership across the engineering lifecycle to define, develop, deliver and sustain the Navy's assured Information warfighting platforms. The CHENG will execute Technical Authority (TA) to ensure systems are interoperable and meet the Cyber needs of today's operations as follows:

(a) SYSCOM Technical Authority: Provide an operational mission based system-of-systems engineering approach for Major Acquisition Programs such as Consolidated Afloat Networks & Enterprise Services (CANES); Automated Digital Network System (ADNS); Next Generation Enterprise Network (NGEN); and Mobile User Objective System (MUOS)
(b) Information Technology Technical Authority (IT TA): CNO and ASN/RDA Joint Letter NAVY INFORMATION TECHNOLOGY TECHNICAL AUTHORITY 3800 Ser N00/100068, dtd 9 Oct 12…development, configuration management, and certification of Navy system compliance with architectures (As Is & To Be), technical standards, tools, and policies for the Navy's IT enterprise both afloat and ashore
(c) Information Assurance Technical Authority (IA TA): OPNAVINST 5239.1C and Virtual Systems Command (SYSCOM) Joint Instruction - VS-JI-22A of 31 January 2007.
    a. Execute TA, which is the authority, responsibility and accountability to establish, monitor and approve technical standards, tools and processes in conformance to higher authority policy, requirements, architectures and standards, in accordance with Virtual Systems Command (SYSCOM) Joint Instruction - VS-JI-22A of 31 January 2007.
    b. Provide high-level oversight and standardization for information system C&A

processes for all IT systems, sites, and networks requiring C&A under the DON IA policy.

c. In coordination with the ODAA, provide procedural guidance on the C&A process.
d. Serve as technical support agent to the FLTCYBERCOM representative on the United States Strategic Command Enterprise-wide Solutions Steering Group.
e. Provide technical and non-technical system security evaluations and identification of operational risk to Navy networks.
f. Provide IT system security engineering and other technical expertise to the virtual SYSCOM supporting SYSCOMs, PEOs, and other Navy development, acquisition, and operational activities for all Service, joint, and coalition programs.
g. Serve as the Navy's Technical Area Expert for the development and maintenance of IT risk management programs.
h. Support Navy's IA Research and Development activities.
i. Lead engineering efforts for emerging concepts such as Joint Information Environment (JIE), Legacy Network, Navy Data Center Consolidation, and Cloud Computing.

SPAWAR 5.0 serves as the Information Assurance (IA) and Information Technology (IT) Technical Authority for the Navy to include Navy Cyber Security. SPAWAR is responsible for Cyber Security architecture, systems engineering, standards, processes, procedures, and specifications to ensure the Navy has secure command and control of Cyberspace and to assure superiority for the warfighter 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." Cyberspace Operations encompasses Computer Network Operations (e.g. Attack, Defend and Exploit), IA, 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.

Key elements of the Enterprise IA strategy include:

- Transactional Information Protection: Granular end-to-end security controls to enable protected information exchange within the trust net-centric environment
- Defense Against an Adversary from Within: Persistently monitor, track, search for, and respond to insider activity and misuse within the enterprise
- Integrated Security Management: Dynamic and automated net-centric security management seamlessly integrated with operations management
- Enhanced Integrity and Trust of Net-Centric Systems: Robust information assurance embedded within enterprise components and maintained over their life cycle

The security disciplines required to adequately address these operational capabilities and key elements include:

- Computer Network Defense (CND)
- IA Readiness

- Cross Domain Solutions (CDS)
- IA Architecture and Engineering (A&E)
- Risk Management

3.0 SCOPE

This task provides a full spectrum of Architecture, analysis, interoperability assessments, engineering, and technical management services in support of SPAWAR's Information Assurance (IA) /Cyber Security (CS), Technical Authority (TA), including:

- System and Security Engineering and Technical Assistance
    - Threat, Vulnerability, and Risk Analysis
    - Information Technology (IT) Enterprise Training and Knowledge Management
    - Automated Information Systems Engineering, Certification and Accreditation
    - System Engineering and Requirements Analysis
    - Service Oriented/Enterprise Architecture Services
    - Test and Evaluation Support (including Early Operational Assessments, Developmental, Operational, and Integrated Testing)
    - Emerging Science and Technologies
    - Configuration Data Management
    - Program Policy and Standards Interpretation and Analysis
- Program Management
    - Modernization and Installation Planning/Management Support
    - Schedule Management
    - Planning, Design and Architectural Support
    - Risk Management
- Administrative and Management Support

Knowledge, skill, and experience requirements will vary by task and will range from working level system and Cyber Security architects and engineers, to senior analysts who will present detailed analysis of Cyber Security technology, systems, tools, standards, policy, procedures and products used to protect the United States' information resources; detect vulnerabilities, and react to threats regardless of the information medium (e.g., data, voice, video, and imagery) with the Navy's operational context to Flag level military and SES level civilian personnel.

Information Assurance and Cyber Security

The contractor will participate in meetings and the development of task related deliverables as they relate to the continued development, growth, and use of the technology, systems, tools, standards, policy, procedures and products for IA and Cyber Security. The contractor may also support engineering events and certification related functions required by SPAWAR's IA TA mission. Related activities include functions such as Acquisition support (IA strategy, Critical Program Information (CPI), Program Protection Plan (PPP), and Anti-Tamper requirements),

Security Engineering to include IA Engineering and Architecture, Engineering Change Request (ECR) support, IA testing, and Certification and Accreditation.

Software Engineering Support

The Contractor will be required to perform review and analysis of software requirements, documentation, plans, and schedules developed or acquired to support SPAWAR 5.0 programs, projects, development efforts, SETR events, SoS compatibility issues, Standard Processes, Software Safety Program Plan/ Programmatic Environment, Safety and Occupational Health (ESOH) Evaluation, Configuration Control and Technical Authority responsibilities. Develop risk management plans to ensure management and mitigation plans are in place.

Configuration Management

The Contractor will be required to provide Configuration Management (CM) support for various programs to include ADNS, CANES, Legacy Programs, OE, and JHSV programs. Implementation and maintenance of CM program plans and processes. Tasks include reviewing change control documents (EPRs and ECRs) and assigning them to the correct work flow along with the release of approved documents in CMPRO. Working with System Engineers and Logistics personnel to identify Configuration Items in order to establish and maintain baselines. Assist in the facilitation of Configuration Control Board (CCB) meetings, preparing agendas and minutes, keeping track of action items generated, and making recommendations as to whether a particular ECR has met the criteria to move to the next step in the process. Support the program office acquisition milestone events and various technical reviews such as SETR and CDR. Provide program office personnel training as to the use of CMPRO. Provide Tier 1 and Tier 2 help in resolving issue with CMPRO, generate reports in response to data calls, and assist programs in enabling the different modules in CMPRO. Participate in various program CM related Integrated Process Team evolutions. Provide support in implementing the main principles of CM in programs: configuration management planning, configuration identification, configuration control, configuration status accounting, and configuration verification and audit.

Computer Network Defense (CND)

The Contractor will be required to provide services related to Computer Network Defense (CND). CND provides for engineering of next generation IA equipment with computer network defense in depth security, active security monitoring and security defense management. The CND product/service area includes a wide range of tasking associated with securing naval shore and shipboard and joint networks. Critical to the CND product/service area is the definition and standardization of network security architecture. The CND product/service area includes the procurement and fielding of Network Security Suites (NSS) for ashore sites and afloat platforms. A suite of products consists of: host/embedded firewalls, high assurance guards, network/host based intrusion detection systems, virus scanning, and VPNs. CND also includes the acquisition, integration, and implementation of products and services to support enclave boundary protection, Intrusion Detection Systems (IDS), Defense Message System (DMS) and other major initiatives currently being developed by the National Security Agency (NSA) and other In-Line Network Encryptor (INE) developers. NSS includes the development and production of the Embeddable

Information Security (INFOSEC) Products (EIP), and the assessment of Cross Domain Solution (CDS) technologies such as trusted software applications (e.g., databases and operating systems). The CND product/service area also covers the tasking associated with planning, executing and deploying intrusion detection capabilities, implementing Defense in Depth (DID) concepts, providing security engineering to promote shore/afloat interoperability, and integrating of next generation CND products and capabilities. These include Intelligent Agent Security Module (IASM), Vulnerability Assessment Tools, Security Asset Accounting Tools and Computer Network Management Tools. In addition, CND encompasses the procurement, installation and integration of Outside the Continental United States (OCONUS) Navy Enterprise Network (ONE-Net) IDS management components and the associated infrastructure to enable a fully operational CND system within the ONE-Net OCONUS environment.

IA Readiness

The Contractor will be required to perform tasks related to IA Readiness. The core effort of IA Readiness is to ensure naval IT systems are designed, installed and operated in compliance with DoD and DoN system security requirements. IA Readiness includes IA dissemination, training, awareness and Fleet support through computer network vulnerability assists. In addition, IA Readiness provides technical review/recommendations for IA policy.

Cross Domain Solutions (CDS)

The Contractor will be required to perform tasks related to CDS. CDS capability is intended to provide a reconfigurable, enabling architecture that supports data transfer services at multiple security levels. CDS will support data exchanges between entities that have varying levels of access control and rules of releasability.

Information Assurance Architecture and Engineering (A&E)

The Contractor will be required to perform tasks related to Information Assurance Architecture and Engineering. This area includes the efforts necessary to integrate network security, key management, secure voice, and other architectures into an overarching IA architecture. One initiative is to facilitate the transition and application of new technology to DoN IA challenges. Emphasis will be placed on providing R&D support for the programs that are identified within the seven GIG IA ICD operational capabilities as their highest priorities, and emphasis will be placed on increasing the speed of delivery of useful IA capability to Fleet users. This includes the security architecture development for each discipline/area, and the coordination with other organizations and functional areas to develop the overarching IA architecture. The A&E area also includes the development of system engineering tools, specific engineering processes, and the implementation of defense-in-depth concepts in support of the following areas:

- Security Analysis & Engineering
- Software Engineering and Software Assurance
- Test and Evaluation
- Technology Development

New Ship Construction Support

New construction ships include the CVN, DDG 1000, LCS, LHA, LHD, LPD, JHSV, DDG 51, T-AKE, MPF (F) and USCG Deepwater. Specific hulls to be supported will be identified with each funding increment.

4.0 APPLICABLE DIRECTIVES/DOCUMENTS

The Contractor shall adhere to the following documents in accordance with paragraph 5.0, Performance Requirements:

Document Type	No./Version	Title	Date
CNSS	No. 6	National Policy on Certification and Accreditation of National Security Systems	Oct 05
DoD	8570.01-M	Information Assurance Workforce	19 Dec 05
Naval	(ser)	Navy Enterprise Architecture	Current
Naval	(ser)	Department of the Navy Enterprise Architecture	Current
DOD	(ser)	DoD Architecture Framework	Current
DOD	CJCSI 6212.01(ser)	Interoperability and Supportability of Information Technology and National Security Systems	Current
DOD	CJCSI 3170.01(ser)	Joint Capabilities Integration and Development System	Current
DOD Directive	5000.01	Acquisition System	Current
Instruction	5000.2D	Secretary of the Navy	October 2008
DODINST	5000.02	Operation of the Defense Acquisition System	Current
OMB Circular	A-11	Preparation, Submission and Execution of the Budget	30 Jun 06
DoN CIO Guidance		Department of the Navy IM/IT Cyberspace Campaign Plan	5 May 11
Federal Regulation	Title 48 CFR, Chapter 1	Federal Acquisition Regulation	Current Month
Federal Regulation	Title 48, CFR Chapter 2	Defense Acquisition Regulations System	Current Month
CJCSI	6510.0D	Information Assurance (IA) and Computer Network Defense (CND)	15 Oct 10
SPAWARINST	5400.3	Systems Engineering Technical Review Process	Current
SPAWARINST	3058.1	Naval SYSCOM Risk Management Policy	April 2008
SPAWARINST	4130.2	SPAWAR Configuration Management (CM) for C4ISR Systems	
DoN CIO Memo	(ser)	DoN Enterprise Architecture ver 1.0	Current

SPAWAR Process SOP	(ser)	Executable Architecture Requirements Model (ExARM) Process SOP	1 October 2013
OPNAVINST	3500.38 (ser)	Universal Naval Task List	Current
OPNAVINST	3050.23 (ser)	Alignment and Responsibility of Navy Requirements Generation and Resource Planning DOD Architectural Framework	Current
SPAWAR 5.0D Policy		Technical Authority Execution Plan	
		DoD Business Enterprise Architecture (BEA)	
SPAWARNOTE	5400	Technical Warrant Holder Memo	June 2010
		Navy's Information Dominance Enterprise Architecture (IDEA). (IDEA)	
Guidebook		Defense Acquisition Guidebook	Current
Guidebook		Naval Systems Engineering Guide	Current
AI CONOPS	Version 1.0	CONOPS Application Integration	October 2009
Document	Version 1.5	SPAWAR 5.0 CONOPS	Current
Plan	Version 1.0	Configuration and Data Management	June 2008
Manual	Version 1.0	Lifecycle CM Implementation Manual	February 2007
DODI	8500.01	Information Assurance	Current
DODI	8500.02	Information Assurance Implementation	Current
DODI	8510.01	DOD Risk Management Framework	Current
Office of Naval Intelligence	DCID 6/3	Director of Central Intelligence Directives (DCID) 6/3	Current
IATA Standard	DFIA	Defense in Depth Functional Implementation Architecture Guide	Current
CNSSI	1253	Security Categorization and Control Selection for National Security Systems	Current
Virtual Systems Command (VSYSCOM) Join Joint Instruction	VS-JI-22A	Virtual SYSCOM Engineering and Technical Authority Policy	January 2007
OPNAVINST	5239.1	Navy Information Assurance (IA) Program	Current

5.0 PERFORMANCE REQUIREMENTS

The Contractor shall provide high technical competence and exemplary IA Technical and Program Management skills described in the following paragraphs. The Contractor shall coordinate with other internal and external stakeholders and provide feedback to their SPAWAR

5.0 client. The Contractor shall work collaboratively with Government personnel and other Contractors internal and external to SPAWAR.

The Contractor shall prepare and deliver products in accordance with the requirements stated in this PWS and in accordance with Contract Data Requirements Lists (CDRLs), when identified and in accordance with applicable directives/documents identified in Section 4.0 above. The Contractor shall provide methods, processes, and tools to strive for cost, schedule, and performance efficiencies. The Contractor shall provide the necessary timely assistance to meet program emergent requirements as requested by the IA TA or other properly designated authority.

Contractor personnel shall be proficient with advanced knowledge in the use of Microsoft Office (Excel, Word, Access, PowerPoint, and Project) applications and their analytical tools, Primavera in a Microsoft Windows and Web environment, intranets, servers, NSERC, SharePoint's System Engineering Environment (SE2), iRAPS, PBIS, NTIRA, SPIDER, SNaP-IT, SharePoint, SMARTS and Total Records and Information Maintenance (TRIM) .

The Contractor shall participate in Government sponsored training, as assigned. Government sponsored training is defined as training required to allow and maintain access to Government databases to perform duties as assigned such as NMCI and Acquisition Metrics Management System (AMMS), but does not include training that would incur additional Government cost.

The Contractor shall implement cost saving and cost control initiatives throughout the life of the contract (e.g. overhead and G&A rate reduction strategies, mentoring of junior employees to replace higher-cost employees, etc.). The Contractor shall measure their performance against the Quality Assurance Surveillance Plan (QASP).

The Contractor shall comply with all security regulations and instructions concerning handling and storage of classified material under their control. Classified material will be inventoried annually by government authority, with no inventory discrepancies allowed.

The Contractor shall prepare and deliver the Contractor's Monthly Status Report which indicates the performance, schedule, cost, personnel and travel and other direct cost status.

5.1 Requirements Definitions and Analysis

5.1.1 The Contractor shall identify viable approaches for the research, development, testing, and support of information systems and equipment to satisfy IA requirements. (RDT&E)

5.1.2 The Contractor shall evaluate and create changes to the DoN and DoD IA goals and initiatives and revisions to IA systems. (RDT&E)

5.1.3 The Contractor shall develop and present alternatives, scope, cost/schedule analysis and associated risks/benefits for all project phases. (RDT&E)

5.1.4 The Contractor shall provide support in the identification of requirements, cost, schedule and performance criteria to support the Navy's IA goals and initiatives in order to develop and defend existing and future IA budgets, program plans and policies. Requirements may result from existing IA product lines, integration of IA solutions into legacy systems, integration of IA into developing systems, and development of new IA technology and solutions. (RDT&E)

5.1.5 The Contractor shall develop and maintain a current list of communication systems deployed and in development requiring potential IA support. (RDT&E)

5.1.6 The Contractor shall evaluate and quantify system criticality and risk, perform triage when requested, and provide recommendations concerning priorities for IA initiatives, and assess all IA technical approaches to ensure consistency with GIG IA performance objectives and key elements. When approaches are determined to be ineffective, inconsistent or incompatible, the Contractor shall provide recommendations concerning technical and programmatic changes through point papers, status reports, program briefings, or other means to provide sufficient information to SPAWAR 5.0 Cyber Security for evaluation. (RDT&E)

5.1.7 The Contractor shall support the management of individual tasks such as the development and tracking of Work Breakdown Structures (WBS), Integrated Master Schedules (IMS), and task tracking and reporting. (RDT&E)

5.1.8 The Contractor shall evaluate and make recommendations on technical information for Integrated Product Teams (IPTs), both internal and external to SPAWAR. (RDT&E)

5.1.9 The Contractor shall develop and execute technical management processes such as Requirements Management, Risk Management, or Configuration Management. (RDT&E)

5.1.10 The Contractor shall participate in the development and execution governance processes, and in the development and management of SPAWAR's analytic agenda for implementation of the decisions of the governance process. (RDT&E)

5.1.11 The Contractor shall perform Cyberspace Operations Mission Assurance and Mission Planning. (OM&N)

5.1.12 The contractor shall review emergent hardware products and technologies (Commercial and Government-owned) and provide recommendations for candidate solutions to satisfy Afloat user requirements to support new ship construction. (SCN)

5.2 Threat, Vulnerability and Risk Analysis

5.2.1 Threat, Vulnerability and Risk Analysis (RDT&E)

5.2.1.1 The Contractor shall investigate and evaluate system concepts and operational and functional requirements of new, developing, and existing systems in order to develop the system security approach which includes defining security environments, potential threats, vulnerabilities, safeguards, security performance indicators, and risk factors.

5.2.1.2 The Contractor shall investigate alternative operational or performance approaches and security measures and compare alternatives by applying decision criteria.

5.2.1.3 The Contractor shall investigate and evaluate threat, vulnerability, and risk analysis of developing systems as directed by the Government.

5.2.1.4 The Contractor shall document results of evaluations and recommend corrective action, contingencies, and other issues appropriate to each specific evaluation.

5.2.1.5 The Contractor shall serve as the SPAWAR 5.0 Cyber Security Risk Management Coordinator (RMC). Specific duties of the RMC are:

- Evaluate and improve the Risk Management process in SPAWAR 5.0 Cyber Security.
- Develop a risk review schedule that complements the submission of required reports.
- Establish portfolio and program Risk Review Boards.
- Establish the SPAWAR 5.0 Cyber Security Risk Watch List and the monthly SPAWAR 5.0 Cyber Security Top 5 Risks.
- Evaluate and validate the SPAWAR 5.0 Cyber Security process in the identification of cross-program/enterprise-level risks
- Develop and conduct Risk Management training.
- Establish processes to assist in the identification and reduction of program risks.
- Participate in SPAWAR 5.0 Cyber Security Risk Review Council and relevant Risk Management Councils and Working Groups.

5.2.1.6 The Contractor shall prepare applicable risk management plans.

5.2.1.7 The Contractor shall also serve as the Risk Management Administrator (RMA). The RMA shall be responsible for day to day Risk Exchange management efforts, including registration of new users.

5.2.1.8 The Contractor shall quantify risk in hours, days, or weeks of delay and provide realistic (whether optimistic or pessimistic) timelines for each major activity and event.

5.2.1.9 The Contractor shall support data collection, and subsequently generate technical drawings to support development of platform specific Navy Risk Management Framework (RMF) that is consistent with the DOD RMF.

5.2.1.10 The Contractor shall support the development, documentation, and governance of DOD-mandated RMF standards, as well as in the coordination of USN positions on RMF standards to include support for determination and evaluation of the USN instantiation of RMF.

5.2.1.11 The Contractor shall support the development and documentation of Computer Network Operations measures report and briefing.

5.2.1.12 The Contractor shall support the development and documentation of Computer Network Attack (CNA) and Computer Network Exploitation (CNE) measures report and briefing.

5.2.1.13 The Contractor shall support the development and documentation for reports and briefing on Information Assurance (IA) and Computer Network Defense (CND) measures.

5.2.1.14 The Contractor shall support the development of Cyberspace Operations Mission Assurance and Mission Plans.

5.2.1.15 The Contractor shall support the development of Information Assurance (IA) and Computer Network Defense (CND) System Lists, Process & Procedures documents, and briefings.

5.2.1.16 The Contractor shall support the development of Computer Network Attack (CNA) and Computer Network Exploitation (CNE) System Lists, Process & Procedures documents, and briefings.

5.2.1.17 The Contractor shall support the development of Computer Network Operations (e.g. Attack, Defend and Exploit functions) System Lists, Process & Procedures documents, and briefings.

5.2.1.18 The Contractor shall prepare Cyber Security/IA Systems and Systems-of-Systems engineering technical reports, analysis, briefings, meeting minutes, etc.

5.2.1.19 The Contractor shall identify systems and develop monitoring processes and procedures for the automated, continuous monitoring of Information Assurance (IA) and Computer Network Defense (CND) status.

5.2.1.20 The Contractor shall identify systems and develop monitoring processes and procedures for the automated, continuous monitoring of Computer Network Attack (CNA) and Computer Network Exploitation (CNE) status.

5.2.1.21 The Contractor shall identify systems and develop monitoring processes and procedures for the automated, continuous monitoring of Computer Network Operations (e.g. Attack, Defend and Exploit functions) status.

5.2.1.22 The Contractor shall perform assessment of Cyber Security metrics (data collection, monitoring, analysis, and reporting).

5.2.2 Threat, Vulnerability and Risk Analysis (OM&N)

5.2.2.1 The Contractor shall perform monitoring, analyzing and reporting on Computer Network Operations.

5.2.2.2 The Contractor shall perform monitoring, analyzing and reporting on Computer Network Attack (CNA) and Computer Network Exploitation (CNE).

5.2.2.3 The Contractor shall perform monitoring, and reporting on Information Assurance (IA) and Computer Network Defense (CND).

5.2.2.4 The Contractor shall perform monitoring and mitigating of Operations Security (OPSEC) vulnerabilities.

5.2.2.5 The Contractor shall perform IA Certification and Accreditation.

5.2.2.6 The Contractor shall perform Cyber Risk assessment.

5.2.2.7 The Contractor shall provide Cyber Security/IA Systems and Systems-of-Systems engineering support.

5.2.2.8 The Contractor shall prepare and maintain Information Assurance (IA) and Computer Network Defense (CND) weekly status reports.

5.2.2.9 The Contractor shall prepare and maintain IA Certification and Accreditation documentation.

5.2.3 Threat, Vulnerability and Risk Analysis (OPN)

5.2.3.1 The Contractor shall perform monitoring, analyzing and reporting on Computer Network Operations.

5.2.3.2 The Contractor shall perform monitoring, analyzing and reporting on Computer Network Attack (CNA) and Computer Network Exploitation (CNE).

5.2.3.3 The Contractor shall perform monitoring, analyzing and reporting on Information Assurance (IA) and Computer Network Defense (CND).

5.2.3.4 The Contractor shall perform monitoring, analyzing and mitigating Operations Security (OPSEC) vulnerabilities.

5.2.3.5 The Contractor shall perform IA Certification and Accreditation.

5.2.3.6 The Contractor shall perform assessment of Cyber Security metrics (data collection, monitoring, analysis, and reporting).

5.2.3.7 The Contractor shall perform Cyber Risk assessment.

5.2.3.8 The Contractor shall provide Cyber Security/IA Systems and Systems-of-Systems engineering support.

5.2.4 Threat, Vulnerability and Risk Analysis (SCN)

5.2.4.1 The Contractor shall perform monitoring and mitigating of Operations Security (OPSEC) vulnerabilities.

5.2.4.2 The Contractor shall perform IA Certification and Accreditation.

5.2.4.3 The Contractor shall perform Cyber Risk assessment.

5.2.4.4 The Contractor shall provide Cyber Security/IA Systems and Systems-of-Systems engineering support.

5.2.4.5 The Contractor shall prepare and maintain IA Certification and Accreditation documentation.

5.3 Security Engineering

5.3.1 Security Engineering (RDT&E)

5.3.1.1 The Contractor shall assist SPAWAR 5.0 Cyber Security personnel in providing security engineering support to developing systems.

5.3.1.2 The Contractor shall provide security inputs into system architectures.

5.3.1.3 The Contractor shall provide recommendations of IA network security tools to be implemented.

5.3.1.4 The Contractor shall provide IA technical expertise at interchange meetings/design reviews, and assist in the development of security policies/procedures.

5.3.1.5 The Contractor shall provide IA engineering and technical support to DoN IA systems engineering and product analyses.

5.3.1.6 The Contractor shall investigate system operational requirements and assist in the development of security functional and performance requirements for new systems.

5.3.1.7 The Contractor shall provide support in the development of IA system concept specifications on systems and products under development.

5.3.1.8 The Contractor shall conduct continuing requirements analyses to identify and evaluate proposed changes to IA concepts and system specifications.

5.3.1.9 The Contractor shall perform security testing of systems as required during development to ensure security features are functioning properly.

5.3.1.10 The Contractor shall work with the Functional Area Team to identify and document information from each of the functional areas for incorporation into documentation of the Information Assurance Technical Authority Standards.

5.3.1.11 The Contractor shall assist in the development and presentation of IA TA documentation formats to include System Architect, MS Word documents, PowerPoint slides, excel spreadsheets, and schedules.

5.3.1.12 The Contractor shall establish Configuration Management of the Information Assurance Technical Authority Data Collection, Data Entry, and generation of fit-for-purpose views of architecture data using System Architect and other architecture tools.

5.3.1.13 The Contractor shall participate in the development of a Risk Management Framework based, top down Defense in Depth Information Assurance Functional Architecture (DFIA)

5.3.1.14 The Contractor shall participate in the development of target architectures for Information Assurance/Cyber Security and Information Dominance related systems.

5.3.1.15 The Contractor shall support development and implementation of system interface management control processes and products to document platform-based As-Programmed Platform Technical Baseline, interface standards, controlling parameters and interface agreements.

5.3.1.16 The Contractor shall prepare and maintain Cyber Security/IA Program engineering technical reports, analysis, briefings, meeting minutes, etc.

5.3.1.17 The Contractor shall support maintenance of SoS interface management control processes and products to document platform-based As-Programmed Platform Technical Baseline, interface standards, controlling parameters and interface agreements.

5.3.1.18 The Contractor shall develop the Cyber Defense-In-Depth architecture, processes, procedures, standards, and specifications.

5.3.1.19 The Contractor shall assist in the development of Cyber Defense-In-Depth architecture, Cyber Defense-In-Depth processes, Cyber Defense-In-Depth procedures, Cyber Defense-In-Depth Standards, and Cyber Defense-In-Depth Specifications.

5.3.1.20 The Contractor shall document Command and Control (C2) of Cyberspace Operational capabilities Architectures, Process, and Procedures.

5.3.1.21 The Contractor shall document Intelligence, Surveillance and Reconnaissance (ISR) aspects of Cyberspace Operations Architectures, Process, and Procedures.

5.3.1.22 The Contractor shall document Cyber Security Countermeasures, development capabilities, and development expertise reports and briefings.

5.3.1.23 The Contractor shall develop a network attack response operations model(s) and model documentation (including Verification and Validation methodology and results, operator's manual, etc.).

5.3.1.24 The Contractor shall evaluate Network Attack Response Modeling and Simulation results (raw and processed data) and Analysis of Model run results.

5.3.1.25 The Contractor shall prepare Cyberspace Operations briefings, doctrine manuals, and Tactics, Techniques & Procedures (TTP). The Contractor shall document Cloud Security Development capabilities and prepare Cloud Security development reports and briefings.

5.3.1.26 The Contractor shall prepare Trusted Security and Networks (TSN)/Supply Chain Risk Management (SCRM) engineering technical reports, analysis, briefings, meeting minutes, Tactics, Techniques & Procedures (TTP).

5.3.1.27 The Contractor shall prepare Insider Threat engineering technical reports, analysis, briefings, meeting minutes, Tactics, Techniques & Procedures (TTP).

5.3.1.28 The Contractor shall prepare Industrial Control System (ICS)/Supervisory Control and Data Acquisition (SCADA) engineering technical reports, analysis, briefings, meeting minutes, Tactics, Techniques & Procedures (TTP).

5.3.1.29 The contractor IA team shall develop and maintain information assurance strategy that is consistent with DoD policies, standards and architectures, and relevant standards. The IA strategy shall outline the program's approach to addressing IA requirements, the system's Mission Assurance Category (MAC) and Confidentiality Level (CL), perceived threats to information and information systems, IA shortfalls, an overview of C&A activities, as well as many other IA considerations. The program's IA strategy shall be maintained in the IA Acquisition folder on the Naval Systems Engineering Resource Center (NSERC) website.

5.3.2 Security Engineering (OM&N)

5.3.2.1 The contractor shall provide Security Architect services, working closely with each of the respective Engineering teams to ensure that all system designs and implementations are consistent with DoD policies, requirements, and directives. Newly developed solutions shall be reviewed for compliance with Defense Information Systems Agency (DISA) Security Technical Implementation Guidance (STIG), Checklists, and Security Requirements Guides (SRG) that shall also be assessed for threats and vulnerabilities not currently identified by published guidance. When compliance or vulnerability issues are identified, the IA contractor shall work closely with the engineering team to remediate existing issues and/or to develop compensating controls that minimize the impact, likelihood, and/or risk.

5.3.2.2 Contractor shall participate as members of respective Programs of Record Change Control Boards (CCB). In this role the IA contractor team shall review each proposed change to determine whether or not there is an associated IA impact. When a change is determined to

require IA support, the contractor shall coordinate with the respective Engineering teams to develop a schedule, execute engineering activities, and to develop the required deliverables. This might involve IA testing and documentation activities that include manual or automated reviews, and entry of those reviews in engineering and C&A documentation.

5.3.2.3 The Contractor shall provide security testing services in support of respective programs systems Engineering, change management, and certification and accreditation processes. As part of the security testing approach, the IA team shall coordinate the development of an IA Pre-Scan checklist with the Engineering team to ensure the scope and boundaries are adequately defined. The IA Pre-Scan checklist shall provide an overview of the test objectives, identify the hardware and software in scope for assessment, specify the tool or assessment methodology for each target, contain network diagrams for the systems under assessment, and document the associated access methodology required to assess each device.

5.3.2.4 The contractor shall provide Certification and Accreditation (C&A) support for all acquired systems within the respective programs. C&A services shall ensure that developed baselines are authorized to operate by the Operational Designated Accrediting Authority (ODAA). In the C&A role, the IA team shall validate systems accordance with DODI 8510.01 DoD Information Assurance Certification and Accreditation Process (DIACAP) for General Service (GENSER) systems and in accordance with the Director of Central Intelligence Directives (DCID) 6/3 for Sensitive Compartmented Information (SCI) systems. This will include preparation of C&A plans and System Security Authorization Agreements relevant to system certification and accreditation. All authoritative DIACAP documentation shall be stored in the Navy's eMASS instance under the respective package's artifact section. All authoritative SCI related documentation shall be stored in Xacta on the Joint Worldwide Intelligence Communications System (JWICS) per data classification requirements.

5.3.2.5 The Contractor shall develop and maintain information assurance strategy that is consistent with DoD policies, standards and architectures, and relevant standards. The IA strategy shall outline the program's approach to addressing IA requirements, the system's Mission Assurance Category (MAC) and Confidentiality Level (CL), perceived threats to information and information systems, IA shortfalls, an overview of C&A activities, as well as many other IA considerations. The program's IA strategy shall be maintained in the IA Acquisition folder on the Naval Systems Engineering Resource Center (NSERC) website.

5.3.2.6 The contractor shall maintain the Critical Program Information (CPI), Program Protection Plan (PPP), and Anti-Tamper requirements in accordance with the Department of Defense Instruction (DoDI) 5000.02.

5.3.2.7 The Contractor shall maintain Transformational Certification and Accreditation and Risk Management Framework using 800.53 security controls. CANES is the Navy pilot for Transformational C&A and all artifacts for the C&A of CANES must be developed in accordance with this agreement.

5.3.2.8 The Contractor shall maintain Host Based Security Services (HBSS) policy development and administration. Understanding of how HBSS works and how these policies affect the security of the system is required.

5.3.2.9 The Contractor shall provide Trusted Agents to perform/execute assessments on board Navy Vessels. Trusted Agents will be assessing CANES, Radiant Mercury, Trusted Thin Client (TTC) and ADNS. Experience performing Trusted Agent work and familiarity with these systems is required.

5.3.2.10 The Contractor shall: research, analyze, assemble, enter and complete the individual site SABI and TSABI packages for review and approval by the Navy Cross Domain Solutions Office (NCDSO) and the designated accreditation authority (DAA). The Contractor shall work with the CDS community to streamline the CDS certification process and liaison with the Navy Cross Domain Solutions Office (NCDSO). Contractor shall use the web based tools to complete this action. Anticipate developing Cross Domain Solution C&A packages for all SSC-PAC and US Ship sites.

5.3.2.11 The Contractor shall work with the Functional Area Team to update information from each of the functional areas for incorporation into documentation of the Information Assurance Technical Authority Standards.

5.3.2.12 The Contractor shall maintain Configuration Management of the IA TA Data Collection, Data Entry, and generation of fit-for-purpose views of architecture data using System Architect and other architecture tools.

5.3.2.13 The Contractor shall provide SoS Engineering and Architecture expertise in the maintenance and enhancement of the Defense in Depth Information Assurance Functional Architecture (DFIA).

5.3.2.14 The Contractor shall support maintenance of target architectures for Defense in Depth Functional Implementation Architecture (DFIA).

5.3.2.15 The Contractor shall provide specialized Information Technology (IT) systems support for development, deployment, and support of CDS systems. The scope of work shall include interfacing with the systems engineering personnel, system deployment planning, operations and maintenance support planning, customer services management (site modifications, upgrades, repairs, training); cost analysis; hardware and software evolution; develop end-to-end systems test cases; coordination and supervision of system installations; performing customer support activities; oversight of software development activities, system Change Requests (CR's), process and system configuration management, monitoring factory and certification testing, and project management. Customer support activities shall include articulating a clear definition of customer requirements and translation of those requirements into detailed guidance for the system developer to design and build a solution to satisfy customer-specific needs.

5.3.3 Security Engineering (OPN)

5.3.3.1 The Contractor shall provide Cyber Security/IA Program engineering support.

5.3.3.2 The Contractor shall provide Security Architect services, working closely with each of the respective Engineering teams to ensure that all system designs and implementations are consistent with DoD policies, requirements, and directives. Newly developed solutions shall be reviewed for compliance with Defense Information Systems Agency (DISA) Security Technical Implementation Guidance (STIG), Checklists, and Security Requirements Guides (SRG) that shall also be assessed for threats and vulnerabilities not currently identified by published guidance. When compliance or vulnerability issues are identified, the IA contractor shall work closely with the engineering team to remediate existing issues and/or to develop compensating controls that minimize the impact, likelihood, and/or risk.

5.3.3.3 The Contractor shall participate as members of respective Programs of Record Change Control Boards (CCB). In this role the IA contractor team shall review each proposed change to determine whether or not there is an associated IA impact. When a change is determined to require IA support, the contractor shall coordinate with the respective Engineering teams to develop a schedule, execute engineering activities, and to develop the required deliverables. This might involve IA testing and documentation activities that include manual or automated reviews, and entry of those reviews in engineering and C&A documentation.

5.3.3.4 The Contractor shall provide security testing services in support of respective programs systems Engineering, change management, and certification and accreditation processes. As part of the security testing approach, the IA team shall coordinate the development of an IA Pre-Scan checklist with the Engineering team to ensure the scope and boundaries are adequately defined. The IA Pre-Scan checklist shall provide an overview of the test objectives, identify the hardware and software in scope for assessment, specify the tool or assessment methodology for each target, contain network diagrams for the systems under assessment, and document the associated access methodology required to assess each device.

5.3.3.5 The Contractor shall provide Certification and Accreditation (C&A) support for all acquired systems within the respective programs. C&A services shall ensure that developed baselines are authorized to operate by the Operational Designated Accrediting Authority (ODAA). In the C&A role, the IA team shall validate systems accordance with DODI 8510.01 DoD Information Assurance Certification and Accreditation Process (DIACAP) for General Service (GENSER) systems and in accordance with the Director of Central Intelligence Directives (DCID) 6/3 for Sensitive Compartmented Information (SCI) systems. This will include preparation of C&A plans and System Security Authorization Agreements relevant to system certification and accreditation. All authoritative DIACAP documentation shall be stored in the Navy's eMASS instance under the respective package's artifact section. All authoritative SCI related documentation shall be stored in Xacta on the Joint Worldwide Intelligence Communications System (JWICS) per data classification requirements.

5.3.3.6 The Contractor shall develop and maintain information assurance strategy that is consistent with DoD policies, standards and architectures, and relevant standards

5.3.3.7 The Contractor shall review the Critical Program Information (CPI), Program Protection Plan (PPP), and Anti-Tamper requirements in accordance with the Department of Defense Instruction (DoDI) 5000.02.

5.3.3.8 The Contractor shall review the Transformational Certification and Accreditation and Risk Management Framework using 800.53 security controls. CANES is the Navy pilot for Transformational C&A and all artifacts for the C&A of CANES must be developed in accordance with this agreement.

5.3.3.9 The Contractor shall review the Host Based Security Services (HBSS) policy development and administration. An understanding of how HBSS works and how these policies affect the security of the system is required.

5.3.3.10 The Contractor shall provide Trusted Agents to perform/execute assessments on board Navy Vessels. Trusted Agents will be assessing CANES, Radiant Mercury, Trusted Thin Client (TTC) and ADNS. Experience performing Trusted Agent work and familiarity with these systems is required.

5.3.3.11 The Contractor shall: research, analyze, assemble, enter and complete the individual site SABI and TSABI packages for review and approval by the Navy Cross Domain Solutions Office (NCDSO) and the designated accreditation authority (DAA). The contractor shall work with the CDS community to streamline the CDS certification process and liaison with the Navy Cross Domain Solutions Office (NCDSO). The contractor shall use the web based tools to complete this action. Anticipate developing Cross Domain Solution C&A packages for all SSC-PAC and US Ship sites.

5.3.4 Security Engineering (SCN)

5.3.4.1 The Contractor shall provide IA technical expertise at interchange meetings/design reviews, and assist in the development of security policies/procedures.

5.3.4.2 The Contractor shall investigate system operational requirements and assist in the development of security functional and performance requirements for new systems.

5.3.4.3 The Contractor shall provide support in the development of IA system concept specifications on systems and products under development.

5.3.4.4 The Contractor shall perform security testing of systems as required during development to ensure security features are functioning properly.

5.3.4.5 The Contractor shall prepare and maintain Cyber Security/IA Program engineering technical reports, analysis, briefings, meeting minutes, etc.

5.3.4.6 The Contractor shall support maintenance of SoS interface management control processes and products to document platform-based As-Programmed Platform Technical Baseline, interface standards, controlling parameters and interface agreements.

5.3.4.7 The Contractor shall provide Cyber Security/IA Program engineering support.

5.3.4.8 The Contractor shall provide Security Architect services, working closely with each of the respective Engineering teams to ensure that all system designs and implementations are consistent with DoD policies, requirements, and directives. Newly developed solutions shall be reviewed for compliance with Defense Information Systems Agency (DISA) Security Technical Implementation Guidance (STIG), Checklists, and Security Requirements Guides (SRG) that shall also be assessed for threats and vulnerabilities not currently identified by published guidance. When compliance or vulnerability issues are identified, the IA contractor shall work closely with the engineering team to remediate existing issues and/or to develop compensating controls that minimize the impact, likelihood, and/or risk

5.3.4.9 The Contractor shall participate as members of respective Programs of Record Change Control Boards (CCB). In this role the IA contractor team shall review each proposed change to determine whether or not there is an associated IA impact. When a change is determined to require IA support, the contractor shall coordinate with the respective Engineering teams to develop a schedule, execute engineering activities, and to develop the required deliverables. This might involve IA testing and documentation activities that include manual or automated reviews, and entry of those reviews in engineering and C&A documentation.

5.3.4.10 The Contractor shall provide security testing services in support of respective programs systems Engineering, change management, and certification and accreditation processes. As part of the security testing approach, the IA team shall coordinate the development of an IA Pre-Scan checklist with the Engineering team to ensure the scope and boundaries are adequately defined. The IA Pre-Scan checklist shall provide an overview of the test objectives, identify the hardware and software in scope for assessment, specify the tool or assessment methodology for each target, contain network diagrams for the systems under assessment, and document the associated access methodology required to assess each device.

5.3.4.11 The Contractor shall provide Certification and Accreditation (C&A) support for all acquired systems within the respective programs. C&A services shall ensure that developed baselines are authorized to operate by the Operational Designated Accrediting Authority (ODAA). In the C&A role, the IA team shall validate systems accordance with DODI 8510.01 DoD Information Assurance Certification and Accreditation Process (DIACAP) for General Service (GENSER) systems and in accordance with the Director of Central Intelligence Directives (DCID) 6/3 for Sensitive Compartmented Information (SCI) systems. This will include preparation of C&A plans and System Security Authorization Agreements relevant to system certification and accreditation. All authoritative DIACAP documentation shall be stored in the Navy's eMASS instance under the respective package's artifact section. All authoritative SCI related documentation shall be stored in Xacta on the Joint Worldwide Intelligence Communications System (JWICS) per data classification requirements.

5.3.4.12 The Contractor shall develop and maintain information assurance strategy that is consistent with DoD policies, standards and architectures, and relevant standards. The IA strategy shall outline the program's approach to addressing IA requirements, the system's Mission Assurance Category (MAC) and Confidentiality Level (CL), perceived threats to information and information systems, IA shortfalls, an overview of C&A activities, as well as many other IA considerations. The program's IA strategy shall be maintained in the IA Acquisition folder on the Naval Systems Engineering Resource Center (NSERC) website.

5.3.4.13 The Contractor shall review the Critical Program Information (CPI), Program Protection Plan (PPP), and Anti-Tamper requirements in accordance with the Department of Defense Instruction (DoDI) 5000.02.

5.3.4.14 The Contractor shall review the Transformational Certification and Accreditation and Risk Management Framework using 800.53 security controls. CANES is the Navy pilot for Transformational C&A and all artifacts for the C&A of CANES must be developed in accordance with this agreement.

5.3.4.15 The Contractor shall review the Host Based Security Services (HBSS) policy development and administration. An understanding of how HBSS works and how these policies affect the security of the system is required.

5.3.4.16 The Contractor shall support development and implementation of system interface management control processes and products to document platform-based As-Programmed Platform Technical Baseline, interface standards, controlling parameters and interface agreements.

5.3.4.17 The Contractor shall provide Trusted Agents to perform/execute assessments on board Navy Vessels. Trusted Agents will be assessing CANES, Radiant Mercury, Trusted Thin Client (TTC) and ADNS. Experience performing Trusted Agent work and familiarity with these systems is required.

5.3.4.18 The Contractor shall: research, analyze, assemble, enter and complete the individual site SABI and TSABI packages for review and approval by the Navy Cross Domain Solutions Office (NCDSO) and the designated accreditation authority (DAA). The contractor shall work with the CDS community to streamline the CDS certification process and liaison with the Navy Cross Domain Solutions Office (NCDSO). The contractor shall use the web based tools to complete this action. Anticipate developing Cross Domain Solution C&A packages for all SSC-PAC and US Ship sites.

5.4 Software Engineering /Assurance Support

5.4.1 Software Engineering /Assurance Support (RDT&E)

5.4.1.1 The Contractor shall evaluate System/Program software requirements, plans, processes, and artifacts, Fault Tree Analysis, Combinatorial Analysis, Event Tree Analysis, Cause-Consequence Analysis, briefs and briefing material, process definitions, test objectives, and technical papers.

5.4.2 Software Engineering/Assurance Support (OM&N)

5.4.2.1 The Contractor shall perform software quality assurance engineering in support of 5.0 technical authority and supporting PEO C4I, PEO Space, and PEO EIS programs/projects.

5.4.2.2 The Contractor shall update the Analysis of System/Program software requirements, plans, processes, and artifacts, Fault Tree Analysis, Combinatorial Analysis, Event Tree Analysis, Cause-Consequence Analysis, briefs and briefing material, process definitions, test objectives, and technical papers as program evolution dictates.

5.4.3 Software Engineering/Assurance Support (SCN)

5.4.3.1 The Contractor shall perform software quality assurance engineering in support of 5.0 technical authority and supporting PEO C4I, PEO Space, and PEO EIS programs/projects.

5.4.3.2 The Contractor shall update the Analysis of System/Program software requirements, plans, processes, and artifacts, Fault Tree Analysis, Combinatorial Analysis, Event Tree Analysis, Cause-Consequence Analysis, briefs and briefing material, process definitions, test objectives, and technical papers as program evolution dictates.

5.5 Test and Evaluation

5.5.1 Test and Evaluation (RDT&E)

5.5.1.1 The Contractor shall provide engineering and technical support for DoN laboratory testing of IA systems, software, tools and products.

5.5.1.2 The Contractor shall assist in the development of a Test and Evaluation Master Plan (TEMP) that describes test objectives, critical technical and operational test parameters, and test phases for various efforts.

5.5.1.3 The Contractor shall assist in the documentation of test results for conducted tests, including quick-look reports, final test reports and lessons learned reports.

5.5.1.4 The Contractor shall assist in the analysis of test data and reports for tests conducted by other developers or entities and present findings or conclusions.

5.5.1.5 The Contractor shall provide engineering and technical support for test and test related working groups, meetings, demonstrations and test events.

5.5.1.6 The Contractor shall prepare technical papers and briefings to support DoN test responsibilities.

5.5.1.7 The Contractor shall use approved written testing procedures for all software testing, including computer program test plan/software test plan, computer program test specification and generation of the computer program test report/software test report.

5.5.2 Test and Evaluation (OCF)

5.5.2.1 The Contractor shall provide engineering and technical support for DoN laboratory testing of IA systems, software, tools and products.

5.5.2.2 The Contractor shall assist in the development of a Test and Evaluation Master Plan (TEMP) that describes test objectives, critical technical and operational test parameters, and test phases for various efforts.

5.5.2.3 The Contractor shall assist in the documentation of test results for conducted tests, including quick-look reports, final test reports and lessons learned reports.

5.5.2.4 The Contractor shall assist in the analysis of test data and reports for tests conducted by other developers or entities and present findings or conclusions.

5.5.2.5 The Contractor shall provide engineering and technical support for test and test related working groups, meetings, demonstrations and test events.

5.5.2.6 The Contractor shall prepare technical papers and briefings to support DoN test responsibilities.

5.5.2.7 The Contractor shall use approved written testing procedures for all software testing, including computer program test plan/software test plan, computer program test specification and generation of the computer program test report/software test report.

5.5.3 Test and Evaluation (SCN)

5.5.3.1 The Contractor shall provide engineering and technical support for DoN laboratory testing of IA systems, software, tools and products.

5.5.3.2 The Contractor shall assist in the development of a Test and Evaluation Master Plan (TEMP) that describes test objectives, critical technical and operational test parameters, and test phases for various efforts.

5.5.3.3 The Contractor shall assist in the documentation of test results for conducted tests, including quick-look reports, final test reports and lessons learned reports.

5.5.3.4 The Contractor shall assist in the analysis of test data and reports for tests conducted by other developers or entities and present findings or conclusions.

5.5.3.5 The Contractor shall provide engineering and technical support for test and test related working groups, meetings, demonstrations and test events.

5.5.3.6 The Contractor shall prepare technical papers and briefings to support DoN test responsibilities.

5.5.3.7 The Contractor shall use approved written testing procedures for all software testing, including computer program test plan/software test plan, computer program test specification and generation of the computer program test report/software test report.

5.5.4 Test and Evaluation (OM&N)

5.5.4.1 The Contractor shall assist in the documentation of test results for conducted tests, including quick-look reports, final test reports and lessons learned reports.

5.5.4.2 The Contractor shall assist in the analysis of test data and reports for tests conducted by other developers or entities and present findings or conclusions.

5.5.4.3 The Contractor shall provide engineering and technical support for test and test related working groups, meetings, demonstrations and test events.

5.5.4.4 The Contractor shall prepare technical papers and briefings to support DoN test responsibilities.

5.5.4.5 The Contractor shall use approved written testing procedures for all software testing, including computer program test plan/software test plan, computer program test specification and generation of the computer program test report/software test report.

5.6 Technology Development

5.6.1 Technology Development (RDT&E)

5.6.1.1 The Contractor shall support SPAWAR 5.0 Cyber Security in development of the capability to understand, evaluate, develop, and apply technology to various DoN IA architecture problems, including IA applications; tools; equipment; processes; prototypes; and products/solutions testing, analysis, proof of concept testing, and new technology briefings and demonstrations.

5.6.1.2 The Contractor shall evaluate, and provide recommended areas of developing technology for more intensive exploration and development by the DoN IA program.

5.6.1.3 The Contractor shall develop approaches for extended exploration of developing technologies as directed by the Government. Such approaches may include focused research and development, identification of potential applications, utilization in new IA products, developing and conducting tests, feasibility assessment applications or systems, proof of concept scenarios

and pilot implementations. Proposed approaches should identify goals, schedules, resources, end products, and other issues.

5.6.1.4 The Contractor shall provide recommendations for the development and testing of IA technologies and security products, systems, tools and literature to improve IA tools, systems, products and management. The Contractor shall make recommendations to support continued evaluation and assessment of new technologies, new applications.

5.6.2 Technology Development (SCN)

5.6.2.1 The contractor shall perform analysis of emergent hardware products and technologies (Commercial and Government-owned) and provide recommendations for candidate solutions to satisfy Afloat user requirements to support new ship construction.

5.7 Configuration Management

5.7.1 Configuration Management (O&MN)

5.7.1.1 The Contractor shall provide support/participation for the implementation and/or maintenance of the following (O&MN):

- CM Policy and Process
- Configuration and Data Management Plan
- CM Work Instructions
- CDRL Management
- CM Data and Document Management
- As-Built Baseline
- Manages and tracks CDRL delivery items
- Facilities delivery item review between Government and Supplier
- Coordinates with CM Team on baseline tracking
- Supports APM/SE in identification and controlling configuration items and baselines
- Facilitates technical documentation reviews
- Process ECRs, ICRs, NCRs

5.7.1.2 The contractor shall identify impact/issues resulting from participation in the following events: CCB PTRB, CIB, SETRs, OIPT, WIPTs, POR IPTs, and POR/Product CCB. Make recommendations on results to government CM lead.

5.7.2 Configuration Management (OPN)

5.7.2.1 The Contractor shall provide support/participation for the implementation and/or maintenance of the following (OPN):

- CM Policy and Process
- Configuration and Data Management Plan
- CM Work Instructions
- CDRL Management
- CM Data and Document Management
- As-Built Baseline

- Manages and tracks CDRL delivery items
- Facilities delivery item review between Government and Supplier
- Coordinates with CM Team on baseline tracking
- Supports APM/SE in identification and controlling configuration items and baselines
- Facilitates technical documentation reviews
- Process ECRs, ICRs, NCRs

5.7.2.2 The contractor shall identify impact/issues resulting from participation in the following events: CCB PTRB, CIB, SETRs, OIPT, WIPTs, POR IPTs, and POR/Product CCB. Make recommendations on results to government CM lead.

5.7.3 Configuration Management (SCN)

5.7.3.1 The Contractor shall provide support/participation for the implementation and/or maintenance of the following (SCN):

- CM Policy and Process
- Configuration and Data Management Plan
- CM Work Instructions
- CDRL Management
- CM Data and Document Management
- As-Built Baseline
- Manages and tracks CDRL delivery items
- Facilities delivery item review between Government and Supplier
- Coordinates with CM Team on baseline tracking
- Supports APM/SE in identification and controlling configuration items and baselines
- Facilitates technical documentation reviews
- Process ECRs, ICRs, NCRs

5.7.3.2 The contractor shall identify impact/issues resulting from participation in the following events: CCB PTRB, CIB, SETRs, OIPT, WIPTs, POR IPTs, and POR/Product CCB. Make recommendations on results to government CM lead.

5.8 Management Support

5.8.1 The Contractor shall support the SPAWAR 5.0 Navy Cyber Security in managing day-to-day operations by tracking, coordinating, collecting, organizing and archiving information in accordance with SECNAVINST 5210.11 or local procedures as appropriate. The Contractor shall respond to data calls and compile statistics necessary to edit reports, correspondence, messages and other incidental documentation within the timeframe required to meet scheduled requirements. (O&MN)

5.8.2 The Contractor shall provide technical and planning support for meetings, conferences and working groups. This support shall include coordination of the meetings, drafting meeting agendas, setup, and operation of Video Tele-Conferencing (VTC) equipment and other audiovisual equipment and managing meeting minutes (finalizing and distributing). The

Contractor shall perform Business Case Analysis (BCA) using Computer Aided Software Engineering (CASE) tools to support recommendation using appropriate evaluation criteria of alternatives. Reports shall be updated and submitted on an ad hoc basis as necessary or requested to support program management. (O&MN)

5.8.3 The Contractor shall map SPAWAR, PEO C4I, PEO EIS, PEO SPACE, and NAVSEA advance planning processes and milestones to implementation timelines; coordinate and expedite implementation submissions, reviews, and approvals. The Contractor shall identify and recommend solutions to programmatic issues related to ashore, afloat, and submarine implementation; monitor compliance with implementation and advance planning processes and status; analyze implementation/advance planning timelines and acquisition/engineering timelines, identify implementation issues that may impact milestones and recommend solutions and recommend process improvements based on subject matter expertise with SPAWAR, PEO C4I, PEO EIS, PEO SPACE, NAVSEA, and fleet advance planning processes and databases. (O&MN)

5.8.4 Meeting Support **-** The contractor shall coordinate and provide support, including briefing materials and draft correspondence as applicable, for meetings, Integrated Product Teams (IPTs), working groups, including relevant working groups and reviews as applicable. (SCN)

6.0 DELIVERABLES

CDRL #	Deliverable	Frequency
A001	Contractor's Progress, Status and Management Report (MSR)	Monthly

The Contractor shall provide deliverables in accordance with the PWS.

Note: All work products generated from the PWS remain government property.

7.0 GOVERNMENT FURNISHED PROPERTY (N/A)

No Government Furnished Property will be required to perform this Task Order.

8.0 SECURITY REQUIREMENTS

The majority of the requirements of this PWS will be met at or below the SECRET level with incidental access to Top Secret Sensitive compartmented information (TS/SCI) which will result in a requirement for The Joint Worldwide Intelligence Communications System JWICS accounts.

The work performed by the Contractor will include access to unclassified, Secret and incidental access to TS/SCI data, information, spaces and meetings.

Incidental access to TS/SCI may be required for research of background data to characterize analytical/task scenarios.

The security classification of this procurement will be specified in the Contract Security Classification Specification, DD Form 254.

In addition to the requirements of the FAR 52.204-2 "Security Requirements" clause, the Contractor shall appoint a Security Officer, who shall (1) be responsible for all security aspects of the work performed under this contract, (2) assure compliance with the National Industry Security Program Operating Manual (DODINST 5220.22M), and (3) assure compliance with any written instructions from the SPAWARSYSCOM Security Officer.

9.0 FOREIGN TRAVEL

If foreign travel is required, all outgoing Country/Theater clearance message requests shall be submitted to the SSC Pacific Foreign Travel Team, OTC2, Room 1656 Code 8.3320, (619) 524-2285, SSC_fortrav@navy.mil 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 45 days in advance 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.

10.0 PLACE OF PERFORMANCE

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:

San Diego, CA
Washington D.C. Area
Norfolk, VA Area
Charleston, SC
Hawaii Area