AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

1. CONTRACT ID CODE	PAGE OF PAGES	
U	1	2

2. AMENDMENT/MODIFICATION NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO. *(If applicable)*
P00002	25-Jun-2019	N/A	N/A

6. ISSUED BY	CODE	7. ADMINISTERED BY *(If other than Item 6)*	CODE
	N65236		N65236

SCD: C

SPAWAR-NIWC Atlantic (CHRL)
P.O. BOX 190022
North Charleston SC 29419-9022
brett.bikowski@navy.mil 843-218-4512

SPAWAR-NIWC Atlantic (CHRL)
P.O. BOX 190022
North Charleston SC 29419-9022

8. NAME AND ADDRESS OF CONTRACTOR *(No., street, county, State, and Zip Code)*

Aermor LLC
207 Business Park Drive, Ste 100
Virginia Beach VA 23462

CAGE CODE: 5ZDW0
FACILITY CODE:

[X]

9A. AMENDMENT OF SOLICITATION NO.

9B. DATED *(SEE ITEM 11)*

10A. MODIFICATION OF CONTRACT/ORDER NO.
N00178-12-D-6753 / N6523619F3049

10B. DATED *(SEE ITEM 13)*
23-May-2019

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). 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)*	
		Brett T Bikowski, Contracting Officer	
15B. CONTRACTOR/OFFEROR	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA	16C. DATE SIGNED
		BY /s/Brett T Bikowski	25-Jun-2019
(Signature of person authorized to sign)		*(Signature of Contracting Officer)*	

GENERAL INFORMATION

The purposes of this modification are to: 1) Update Section G, DFARS clause 252.232-7006(f)(1) to revise the document type from "Invoice 2-n-1" to "Cost Voucher," and 2) Update Section I to include DFARS clause 252.229-7005 - Tax Exemptions (Spain) (Mar 2012).

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

The Line of Accounting information is hereby changed as follows:

The total amount of funds obligated to the task is hereby increased from $ by $ to $.

The total value of the order is hereby increased from $ by $ to $.

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	D310	Funding Source 1 - Base Year Labor (Fund Type - TBD)	13440.0	LH			
700101	D310	FY19 O&MN Labor Funding under CLIN 7001 (2410a Invoked) (O&MN,N)					
7002	D310	Funding Source 2 - Base Year Labor (Fund Type - TBD)	98560.0	LH			
700201	D310	FY19 O&MN Labor Funding under CLIN 7002 (2410a Invoked) (O&MN,N)					

For Cost Type / NSP Items

Item	PSC	Supplies/Services	Qty	Unit	Est. Cost	Fixed Fee	CPFF
7003		Not Separately Priced CDRLs IAW Section J, Exhibit A	1.0	LO			NSP

For Cost Type Items:

Item	PSC	Supplies/Services	Qty	Unit	Est. Cost	Fixed Fee	CPFF
7101	D310	Funding Source 1 - Option Year 1 Labor (Fund Type - TBD) Option	13440.0	LH			
7102	D310	Funding Source 2 - Option Year 1 Labor (Fund Type - TBD) Option	98560.0	LH			

For Cost Type / NSP Items

Item	PSC	Supplies/Services	Qty	Unit	Est. Cost	Fixed Fee	CPFF
7103		Not Separately Priced CDRLs IAW Section J Exhibit A	1.0	LO			NSP

For Cost Type Items:

Item	PSC	Supplies/Services	Qty	Unit	Est. Cost	Fixed Fee	CPFF
7201	D310	Funding Source 1 - Option Year 2 Labor (Fund Type - TBD) Option	13440.0	LH			
7202	D310	Funding Source 2 - Option Year 2 Labor (Fund Type - TBD) Option	98560.0	LH			

For Cost Type / NSP Items

Item	PSC	Supplies/Services	Qty	Unit	Est. Cost	Fixed Fee	CPFF
7203		Not Separately Priced CDRLs IAW Section J Exhibit A	1.0	LO			NSP

For Cost Type Items:

Item	PSC	Supplies/Services	Qty	Unit	Est. Cost	Fixed Fee	CPFF
7301	D310	Funding Source 1 - Option Year 3 Labor (Fund Type - TBD) Option	13440.0	LH			
7302	D310	Funding Source 2 - Option Year 3 Labor (Fund Type - TBD) Option	98560.0	LH			

For Cost Type / NSP Items

Item	PSC	Supplies/Services	Qty	Unit	Est. Cost	Fixed Fee	CPFF
7303		Not Separately Priced CDRLs IAW Section J Exhibit A	1.0	LO			NSP

For Cost Type Items:

Item	PSC	Supplies/Services	Qty	Unit	Est. Cost	Fixed Fee	CPFF
7401	D310	Funding Source 1 - Option Year 4 Labor (Fund Type - TBD) Option	13440.0	LH			

Item	PSC	Supplies/Services	Qty	Unit	Est. Cost	Fixed Fee	CPFF
7402	D310	Funding Source 2 - Option Year 4 Labor (Fund Type - TBD) Option	98560.0	LH			

For Cost Type / NSP Items

Item	PSC	Supplies/Services	Qty	Unit	Est. Cost	Fixed Fee	CPFF
7403		Not Separately Priced CDRLs IAW Section J Exhibit A	1.0	LO			NSP

For ODC Items:

Item	PSC	Supplies/Services	Qty	Unit	Est. Cost
9001	D310	ODC's in support of CLIN 7001 (Fund Type - TBD)	1.0	LO	
900101	D310	FY19 O&MN ODC Funding in support of CLIN 7001 (2410a Invoked) (O&MN,N)			
9002	D310	ODC's in support of CLIN 7002 (Fund Type - TBD)	1.0	LO	
900201	D310	FY19 O&MN ODC Funding in support of CLIN 7002 (2410a Invoked) (O&MN,N)			
9101	D310	ODC's in support of CLIN 7101 (Fund Type - TBD) Option	1.0	LO	
9102	D310	ODC's in support of CLIN 7102 (Fund Type - TBD) Option	1.0	LO	
9201	D310	ODC's in support of CLIN 7201 (Fund Type - TBD) Option	1.0	LO	
9202	D310	ODC's in support of CLIN 7202 (Fund Type - TBD) Option	1.0	LO	
9301	D310	ODC's in support of CLIN 7301 (Fund Type - TBD) Option	1.0	LO	
9302	D310	ODC's in support of CLIN 7302 (Fund Type - TBD) Option	1.0	LO	
9401	D310	ODC's in support of CLIN 7401 (Fund Type - TBD) Option	1.0	LO	
9402	D310	ODC's in support of CLIN 7402 (Fund Type - TBD) Option	1.0	LO	

HQ B-2-0015 PAYMENTS OF FEE(S) (LEVEL OF EFFORT – ALTERNATE 1) (NAVSEA) (MAY 2010)

(a) For purposes of this task order, “fee” means “target fee” in cost-plus-incentive-fee type contracts, base fee" in cost-plus award- fee type contracts, or "fixed fee" in cost-plus-fixed-fee type contracts for level of effort type contracts.

(b) The Government shall make payments to the Contractor, subject to and in accordance with the clause in the basic contract entitled "FIXED FEE" (FAR 52.216-8), as applicable. Such payments shall be submitted by and payable to the Contractor pursuant to the clause of the basic contract entitled "ALLOWABLE COST AND PAYMENT" (FAR 52.216-7), subject to the withholding terms and conditions of the "FIXED FEE" clause, as applicable, and shall be paid fee at the hourly rate(s) specified below per staff-hour performed and invoiced. Total fee(s) paid to the Contractor shall not exceed the fee amount(s) set forth in this task order. In no event shall the Government be required to pay the Contractor any amount in excess of the funds obligated under this task order.

Fee paid is based on total fee dollars divided by total staff-hours to be provided.

Year	**CLIN**	**Fixed Fee**	**Hours**	**Fee per Direct Labor Hour**
Base	**7001**		13,440	
Base	**7002**		98,560	
Option Year 1	**7101**		13,440	
Option Year 1	**7102**		98,560	
Option Year 2	**7201**		13,440	
Option Year 2	**7202**		98,560	
Option Year 3	**7301**		13,440	
Option Year 3	**7302**		98,560	
Option Year 4	**7401**		13,440	
Option Year 4	**7402**		98,560	

**To be completed at task order award*

SECTION C DESCRIPTIONS AND SPECIFICATIONS

Work under this performance-based task order will be performed in accordance with the following description/ specifications/ statement of work (SOW) which herein will be referred to as Performance Work Statement (PWS):

SHORT TITLE: Commander, Navy Installations Command (CNIC) N6 Cybersecurity Support

1.0 PURPOSE

1.1 SCOPE

SPAWARSYSCEN Atlantic currently provides technical and programmatic support to help CNIC with their mission to enable and enhance the combat power by providing the most effective, efficient, and cost-wise shore services and support. For this project SPAWARSYSCEN Atlantic will provide Cybersecurity, Information Assurance (IA) and Information Security (IS) support to CNIC N6. SPAWARSYSCEN Atlantic will execute engineering services to assist in ensuring compliance with Federal, Department of Defense (DoD), and Department of Navy (DON) and subservices regulations and policies. Navy IT performance is driven to maximum availability and efficiency through technically capable support teams with specialized knowledge, skills and experience supporting military applications and toolsets used by the United States Navy.

The objective of this Task Order is to assist SPAWARSYSCEN Atlantic in project execution, security operation support services, information assurance, certification and accreditation, Cybersecurity/IA policy, risk management services and network engineering services at locations throughout the Continental US (CONUS) and Outside the Continental US (OCONUS) areas.

1.1.1 Multiple Funding

This task order is funded with multiple appropriations as delineated on specified contract line item numbers (CLINs). The applicable PWS task(s) associated with each funding CLIN is outlined in Section B and Section G.

1.2 BACKGROUND

Navy ashore installations support our Navy's fleets, fighters and families. As the single responsible office, advocate and point of contact for Navy installations, Commander, Navy Installations Command (CNIC) has the mission to provide consistent effective and efficient shore installation services and support to sustain and improve current and future fleet readiness and mission execution. CNIC does this by providing unified and consistent procedures, standards of service, practices and funding to manage and oversee shore installation to the Fleet. CNIC executes delivery of installation services through its regions and installations. This mission involves the coordination of policy, planning, budgeting and reporting of all Navy regions and shore installations.

The mission of the CNIC Command Information Officer (CIO), Code N6, is to execute Department of Navy and Navy Chief Information Officer policies and programs and to provide Information Management/Information Technology/Command & Control (IM/IT/C2) services required to support the mission of the Command. The CNIC N6 organization is tasked to provide an integrated framework of technology aimed at efficiently performing the business of CNIC. The CNIC N6 organization manages all aspects of the systems, and the supporting infrastructure, providing critical systems and infrastructure support enterprise wide.

2.0 PLACE(S) OF PERFORMANCE

The following sites are where the majority of labor hours will be spent; for travel (i.e., temporary duty sites) see Travel Section under TO PWS Para 10.0.

a. Contractor facilities, Any location

b. Government Facilities, Washington D.C./National Capital Region

c. Government Facilities, Norfolk, VA

d. Government Facilities, San Diego, CA

2.1 GOVERNMENT FACILITIES

Government facilities (i.e., office space or lab space) are provided to those labor categories that would otherwise adversely affect the work performance if they were not available on Government site. Contractor personnel with supplied Government facilities shall be located at *San Diego, CA, Washington, D.C., and Norfolk, VA.*

2.1.1 Training Requirements

Contractor personnel working full-time or partially at a Government facility shall complete all applicable mandatory training requirements as specified under Security Training, PWS Para 8.0.

2.2 CONTRACTOR FACILITIES

The contractor can have its facility location *anywhere* as long as the location does not present a hardship to complete work required on task. The contractor shall have real-time communication between the contractor personnel supporting the efforts and government personnel available at time of award.

3.0 PERFORMANCE REQUIREMENTS

The following paragraphs list all required non-personal services tasks that will be required throughout the task order. The contractor shall provide necessary resources with knowledge and experience as cited in the Personnel Qualifications clause to support the listed tasks.

T h e c ontractor shall perform requirements in accordance with Federal Acquisition Regulation (FAR) and/or Defense Federal Acquisition Regulation Supplement (DFARS), which does not include performance of inherently governmental functions. Documentation support for specific systems to include Cyber Security Operations, Compliance Monitoring and Security Services, Cyber Security Assessment and Authorization, and Cyber Security Management.

The contractor is expected to coordinate IT sustainment and support with the representatives from other sustainment contracts that support CNIC. The contractor shall complete all required tasks while controlling and tracking performance and goals in terms of costs, schedules, and resources.

3.1 PROGRAM MANAGEMENT

The following task is supportingCNIC operations and maintenance support.

3.1.1 Program Review Support

3.1.1.1 Program and task order specific metrics and financial reporting in various task formats as required (CDRL A001)

3.1.1.2 Provide Inventory Status with Monthly Invoice Documentation (CDRL A003)

3.1.1.3 Provide Funds Status in the monthly TO Status Report (CFSR) (CDRL A001)

3.1.1.4 Provide WAWF Invoicing Notification and Support Documentation (CDRL A003)

3.1.1.5 Provide Documentation in compliance with applicable regulations (CDRL A011)

3.1.1.6 Provide status report to the Government PM on progress/results of IA testing (CDRL A010)

3.1.1.7 Support and provide minutes and status reports for collaborative meetings in the Program Management Report (CDRL A011)

3.1.1.8 Provide Information Assurance oversight, project management, planning, and logistics for the task (CDRL A010)

3.1.1.9 Utilize capabilities such as: Microsoft SharePoint, Access, or Excel

3.2 TECHNICAL SUPPORT

3.2.1 **Cyber Security Operations**

3.2.1.1 Command/Control Security Operation Center (C2SOC)

3.2.1.2 The Contractor shall integrate capabilities within CNIC's IM/IT/C2 infrastructure to enable the C2SOC staff to monitor, detect, scan, record, audit, analyze, investigate, report, remediate, coordinate, and track security-related "events" such as signs of intrusion, compromise, misuse, and compliance.

3.2.1.3 The Contractor shall provide direct support to CNIC using NMCI computers and all required DoD Enterprise tools.

3.2.1.4 The Contractor shall prepare templates and processes to produce trend analyses, scan reports, and vulnerability history.

3.2.2 Information Security Continuous Monitoring (ISCM)

The CNIC ISCM program is based on the continuous monitoring process described in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-137.

3.2.2.1 The Contractor shall provide technical support for CNIC's ISCM program and strategy.

3.2.2.2 The Contractor shall use the 3-tier risk management model defined in NIST SP 800-53 to support CNIC ISCM strategies.

3.2.2.3 The Contractor shall provide a framework to support the Office of Management

and Budget (OMB) ISCM requirements.

3.2.2.4 The Contractor shall centralize cybersecurity actions as an enterprise services for

effective ISCM support of CNIC managed Information Systems (ISs).

3.2.2.5 The Contractor shall support situational awareness by integrating asset awareness data with real-time vulnerability data.

3.2.2.6 The Contractor shall incorporate real-time vulnerability data, operational data and IT knowledge base at the enterprise level to support informed IT.

3.2.2.7 The Contractor shall create enterprise methods and procedures to assign risk and to reduce maintenance and rework of ISs in order to mitigate risks.

3.2.3 **Mission/business process (Tier 2) level.**

3.2.3.1 The Contractor shall reduce CNIC IS risk posture and enable CNIC to operate within a known and defined risk tolerance with current vulnerability data and risk assessment.

3.2.3.2 The Contractor shall streamline System Development Lifecycle (SDLC) activities by automating tasks to support IS assessment and authorization.

3.2.3.3 Leverage existing and emerging cybersecurity systems and technology to fulfill ISCM requirements.

3.2.3.4 The Contractor shall enable IS stakeholders to effectively manage IS in near real-time

and respond to cybersecurity events and incidents as orderly and systematically as feasible.

3.3 Cybersecurity Watch

All support described below shall be provided by the Contractor on a 24x7x365 basis.

3.3.1 3.3.1 The Contractor shall support C2SOC tasks in the following areas: monitoring, detecting, scanning, recording, auditing, analyzing, reporting, remediation, coordinating, and tracking.

3.4 Tier Cybersecurity Support

3.4.1 3.4.1 The Contractor shall provide cybersecurity watch, in conjunction with the CNIC Enterprise Support Center (CESC), and shall respond as needed to assist with Tier I customer support with potential Cybersecurity related issues.

3.4.2 3.4.2 The watch will follow initial incident response procedures in the C2SOC Standard Operating Procedures (SOP) when an incident is identified.

3.4.3 3.4.3 The watch may perform known and simple remediation actions if applicable. Complex cybersecurity issues shall be escalated by the watch to Tier II or Tier III and SPAWAR COR, per escalation processes defined in conjunction with the CESC.

3.5 Monitoring

3.5.1 The Contractor shall utilize CNIC provided sensors, systems, and tools to monitor all CNIC Networks and Systems for signs of intrusion, compromise, misuse, and non-compliance.

3.5.2 The Contractor shall proactively monitor and track down anomalies, non-compliant systems, and other observed events that are detrimental to the overall security posture of CNIC IM/IT/C2 infrastructure and systems.

3.6 Detecting

3.6.1 The Contractor shall detect for vulnerabilities and sophisticated and nuanced attacks, discern and remove false positives, and analyze the information generated by CNIC Systems.

3.6.2 The Contractor shall perform trend analysis to spot patterns within the CNIC network and depict representations of normal activities.

3.6.3 The Contractor shall provide weekly and monthly reports. The weekly and monthly report shall be done via electronic mail only.

3.7 Vulnerability Scanning

3.7.1 The Contractor shall continuously scan the devices on the CNIC network to identify network and system vulnerabilities.

3.7.2 The Contractor shall monitor the remediation status of the scan results and evaluate the scan results for accuracy and risk.

3.7.3 The Contractor shall provide the analyzed results to the various responsible parties identified by the designated CNIC HQ N6 representative for resolution.

3.7.4 The Contractor shall act as the Subject Matter Experts (SMEs) for the scan results and consult with the remediation teams on various methods for resolution.

3.7.5 The Contractor shall provide network segment(s) scanned, and document who performed/verified scan.

3.7.6 The Contractor shall provide Risk/threat level associated with scan, and Roll up of scan results.

3.7.7 The Contractor shall review and verify network map with scanning results (overlay Pie chart that describes overall scan results).

3.7.8 The Contractor shall provide progress toward the continuous control in weekly and monthly reports , which include:

a. Internet Protocol (IP) Address ranges scanned.

b. Numbers, categories and risks levels of vulnerabilities identified.

c. Remediation efforts being tracked;

d. Remediation report

e. Repeat findings

f. Vulnerability to be tracked and not remediated, Trending Information:

g. Threat Level

h. Sensitivity level of network segment; i.e. Computer Emergency Response Team (CERT) site

3.8 Security Information and Event Management (SIEM)

3.8.1 The Contractor shall record, retain, and archive security event logs from various security systems on CNIC network using current deployed CNIC technology and equipment.

3.8.2 The Contractor shall ensure all security event logs are synchronized with the Network Time Protocol (NTP) server for auditing, analysis and reporting. Logs shall also be maintained in accordance with current Department of Defense (DoD), Department of the Navy (DON), NIST and CNIC security policies to assist in event reconstruction and correlation.

3.8.3 The Contractor is responsible for ensuring they are operating within the current DoD, DON, NIST and CNIC security policies. Security event logs shall include the following data:

a. Source/destination IP address.
b. Protocol/port number.
c. Date and time with time zone.
d. Event name Payload or flow data (Intrusion Detection Systems (IDSs) and Intrusion Prevention Systems (IPSs)
e. Session Duration.

3.9 Configuration Audit

3.9.1 The Contractor shall conduct weekly audits on the configuration of security event monitoring devices.

3.9.2 The Contractor shall create a detailed plan for verifying the continuous monitoring, detection and response of security events on CNIC network. Weekly audits must include log reviews of successful and failed authentication attempts, file accesses, security policy changes, account changes (account creation, account deletion, and account privilege assignments), and use of privileges.

3.9.3 The Contractor shall provide audit results in a weekly report for the devices listed.

3.9.4 The Contractor shall demonstrate, and report the status of, remediation efforts in weekly and monthly reports. These reports will incorporate various metrics as they are used in audit and other findings made available to and/or by the Contractor or designated SPAWAR LANT representative and other governing government entities.

3.10 Analysis (Log Review)

3.10.1 The Contractor shall act as a SME in daily log analysis for identifying security incidents, policy violations, and malicious code. Currently CNIC is using McAfee SIEM product suite for centralized audit log management.

3.10.2 The Contractor shall use correlation engine to perform correlation of network IDS/IPS and Host Intrusion Prevention System (HIPS) logs with other records such as firewall/proxy logs, anti-virus, anti-malware, server audit trails as well as vulnerability information on CNIC targets.

3.10.3 The Contractor shall conduct daily analysis of security logs to detect incidents on CNIC network and assist in remediation.

The Contractor shall create trend reports, to include the following, which will be submitted to SPAWAR on a monthly basis:

a. Security events prioritize by Threat Level,
b. Open & Close incidents,
c. black-listed or suspicious source IP targeting CNIC targets, and
d. Forbidden or suspicious protocols and ports active on CNIC network.

3.11 **Incident Response**

If contacted by the CESC, the cybersecurity watch will provide Tier I cybersecurity support, open a log on the incident identified and perform known and simple remediation actions as applicable.

Complex issues will be escalated by the watch and/or CESC for immediate actions.

3.12 **Tier II Support**

Contractor Tier II personnel shall be responsible for problem resolution and for investigating elevated issues by confirming the validity of the problem. Additional tasks that may be required of Tier II personnel would include: software repair, diagnostic testing, remote control tools, and replacing hardware components. Issues shall be escalated to Tier III or additional external support per C_2SOC SOP.

3.13 **Tier III Support**

The Contractor shall provide Tier III technical support that is comprised of senior level technicians who are responsible for handling the most difficult or advanced problems.

3.14 **Coordination with External Resources**

3.14.1 The Contractor shall coordinate with other DoD, DON and US Government agencies continually in order to provide information regarding security incidents that affect CNIC's IM/IT/C2 capabilities.

3.14.2 Contractor shall use information from other agencies to improve the CNIC security posture and quickly react to fast moving threats directed by DoD, DON and/or the United States Computer Emergency Readiness Team (USCERT).

3.14.3 The contractor may coordinate with external resources for further incident response

support. External resources include engineering support from other external DoD resources (e.g., vendor, Original Equipment Manufacturer), as coordinated and/or approved by the SPAWAR LANT COR.

3.15 **Remediation**

3.15.1 The Contractor shall work with CNIC network administrators, program managers and system owners to oversee the remediation of identified security issues within CNIC's IM/IT/C2 capabilities.

3.15.2 The Contractor shall oversee the resolution of security issues that may include:

a. Installation of a software patch

b. Changes of a configuration setting

c. Removal of the affected CNIC asset

3.15.3 The Contractor shall provide a remediation plan that lists opened security issues with their steps and projected timelines for remediation. Remediation shall be tracked via the online portal. The weekly report shall consist of an overview of security issues from the previous week and the status of each security issue including any outstanding issues, problems encountered, planned activities of interest for the next week and any lessons learned. The monthly report shall include only the outstanding issues, a summary of the action taken, problems encountered, responsible individual and milestones for resolution.

3.16 **Incident and Service Tracking**

Incidents, changes, and service requests are all currently controlled through the IPSwitch IssueTrak, ticketing system.

3.16.1 The Contractor shall follow the C2SOC SOP to manage incident ticket while making configuration changes, providing incident containment, eradication and recovery actions and engaging resources for incident response, such as gathering information. Incidents may identify underlying problems that require engineering work to fix design flaws or other issues.

3.16.2 The Contractor shall work with SPAWAR LANT COR for infrastructure problems. This work shall be coordinated with other infrastructure support resources, such as enclave administrators, system owners and other contractors per designated CNIC HQ N6 representative.

3.17 **Reporting (Daily and Monthly) Situation Reporting**

3.17.1 Contractor shall include in the monthly report the number of incidents, changes, and service requests assigned in the reporting period. Continuous improvement is an objective for all processes, and the monthly report shall include all issues and recommendations to improve the process for future changes.

3.17.2 The Contractor shall provide daily and monthly situation reporting. The daily report shall cover each day's activities, the issues being tracked, and the status of each issue. The monthly report shall contain the following items:

a. Duty Roster

b. Summary of critical or urgent security issues being tracked,

c. Status of each area of responsibility,

d. Summary of critical or urgent administrative issues being tracked, and

e. List of any needs/actions from the Government.

3.17.3 The Contractor shall provide a process to upload and maintain reports online – to a site to be specified by designated CNIC HQ N6 representative.

3.17.4 The Contractor shall create a process to store watch logs and watch supervisor turnovers.

3.18 Tools for Cybersecurity Management

3.18.1 The Contractor shall be responsible for operating, tuning, and reviewing maintenance of all cybersecurity tools, software suites, devices, appliances and systems, including:

a. The DoD Host Based Security System Suite (HBSS) suite, including

the HBSS Enterprise Policy Orchestrator (ePO);

b. The DoD Assured Compliance Assessment Solution suite;

c. The McAfee SIEM product suite, including Enterprise Security

Manager (ESM), Enterprise Log Manager (ELM), log receiver,

event correlation engine or the equivalent replacements;

d. ForeScout product suite, including CounterACT Enterprise Manager

(CEM), CT appliances and plug-ins for Virtual Private Network

(VPN) gateways;

e. RedSeal cybersecurity configuration compliance appliances;

f. WebInspect runtime web service cybersecurity monitors;

g. Encase forensics management tool; and

h. IDSs/IPSs

3.18.2 Continuous monitoring of the IDSs/IPSs for signs of compromise, misuse, compliance, and general health within CNIC networks

a. Setup and deployment of IDS/IPS sensors

b. Provide recommended sensor policies

c. Tune sensor policies to reduce false positives

d. Provide specialized signatures

e. Tailor response events

f. Other day-to-day activities related to the IDSs/IPSs.

3.18.3 The contractor shall coordinate with CNIC network administrators, program managers and system owners (to include their contractors) to monitor activities and health of cybersecurity associated devices, such as Websense proxies, firewalls, and C2SOC manageable routers, switches, agent servers and watch workstations.

3.19 **Compliance Monitoring and Security Services**

3.19.1 Operational and Technical Support for Security Services

3.19.2 The Contractor shall provide security services for protection of the ISs, IS domains (Communities of Interest), and Information Content (at rest, in use, and in transit) in accordance with DoD cybersecurity policies and procedures. These operational security services shall be fully integrated with the United States Cyber Command (USCYBERCOM) mandates to ensure confidentiality, integrity, availability, authentication, and non-repudiation requirements.

3.19.3 The Contractor shall implement the necessary Information Assurance/Computer Network Defense (IA/CND) mechanisms to provide these security services, and conduct vulnerability assessments to validate that the necessary security controls (SCs) are in place. As part of implementing these security services, the Contractor shall implement CNIC directed IA/CND direction such as Information Operations Conditions (INFOCONs) and incident reporting (e.g., system anomalies, outages, etc.).

3.19.4 Implementation of IA/CND mandates, to include USCYBERCOM Communications Tasking Orders (CTOs), Warning Orders (WARNORD), Operational Directive Messages (ODMs), Information Special Outage Report (INFOSPOT), Situational Awareness Report (SITREP), and Fragmentary Order (FRAGO) should be accomplished within Government specified timeframes as shown in Table 1 below.

Table 1 Compliance Timelines for Vulnerability Remediation

DoD Severity	NIST Severity	Days For Compliance/Approved Mitigation
Category (CAT) I	HIGH	Immediate – 25 Days
CAT II	MEDIUM	60 Days
CAT III	LOW	180 Days
CAT IV	INFORMATIONAL	240 Days

3.19.5 The Contractor shall provide strategic security services to enhance the confidentiality, integrity, and availability, authenticity, and non-repudiation requirements.

3.19.6 The Contractor provided solutions shall support mechanisms of encryption, access control, user identification and authentication, malicious content detection, audit, and physical and environmental control.

3.19.7 The Contractor shall provide informational feeds to support CNIC oversight, maintain accessible historical data, and deliver summary management reports that detail the security planning functions.

3.19.8 The Contractor shall propose updated and/or revised architecture and/or configuration changes to accommodate

changing requirements, emerging technology, and results of vulnerability assessments for government review and approval.

3.20 **Vulnerability Management**

3.20.1 The Contractor shall meet the provisions of CNIC's Cybersecurity Vulnerability Management (IAVM) program implemented under Chairman of the Joint Chiefs of Staff Manual (JCSM) 6510.01A dated 24 June 2009 to include support for three types of vulnerability notifications:

a. Cybersecurity Vulnerability Alert (IAVA) addresses vulnerabilities resulting in immediate and potentially severe threats to DoD systems and information. Corrective action is of the highest priority due to the severity of the vulnerability risk,

b.Cybersecurity Vulnerability Bulletin (IAVB) addresses new vulnerabilities that do not pose an immediate risk to CNIC systems, but are significant enough that noncompliance with the corrective action could escalate the risk, and

c. Technical Advisory (TA) addresses new vulnerabilities that are generally categorized as low risks to DoD systems.

3.20.2 The Contractor shall support the Vulnerability Management System issuances (IAVAs, IAVBs, and TAs); CNIC estimates a minimum of 25 monthly.

3.20.3 The contractor shall meet the compliance timelines for IAVAs as issued and mandated by USCYBERCOM. The timeline for compliance on IAVBs and TAs vulnerabilities are determined by the assigned severity for the vulnerability coupled with the compliance timelines established by the Defense Information Systems Agency (DISA).

Severity codes ("Security Technical Implementation Guide (STIG) Finding Severity") are documented in the IAVM notices published on the USCYBERCOM Web Page. Table 2 below depicts the DISA compliance requirements based on severity. Such periods may be overridden by direction of the designated CNIC HQ N6 representative and communicated via a Plan of Action and Milestones (POA&M).Work with SPAWAR Government Team to ensure proper communication and direction.

Table 2 Compliance Timeline for IAVM Actions

DoD Severity	NIST Severity	Days for Compliance/Approved
		Mitigation
CAT I	HIGH	Immediate – 25 Days
CAT II	MEDIUM	60 Days
CAT II	LOW	180 Days
CAT IV	INFORMATIONAL	240 Days

3.20.4 The Contractor shall take immediate action to assess the impacts of each vulnerability action, develop patching plans, and begin gathering data for the new "First Report" requirement. The patch plan should consider any other systems that may not be patched by POA&M report date.

3.20.5 In coordination with the network administrator, program manager, and/or system owner, the Contractor shall support the installation, configuration and testing of patches and changes required by Vulnerability Management System issuances (IAVAs, IAVBs, IAVMs). All necessary changes shall be made to the applicable production equipment in accordance with the suspense date articulated by the appropriate government authority. Patches or changes that require down time shall be coordinated with the designated CNIC HQ N6 representative in order to minimize downtime and/or schedule for non-peak time (e.g., nights, weekend). All patches or changes to the servers shall be performed on test servers prior to being applied to production.

3.20.6 The Contractor shall ensure IAVM compliance to include

a. The normal Certification and Accreditation (C&A) or Assessment and Authorization (A&A) process.

b. Monthly scanning of the systems using the most up-to-date version of the USCYBERCOM-approved vulnerability scanning package (currently, this is the Assured Compliance Assessment Solution (ACAS) Nessus Scanner by Tenable). The results of these scans will be sent to the appropriate system/network /enclave Information System Security Officers (ISSOs).

3.21 **Compliance to Connect**

3.21.1 The Contractor shall actively manage and integrate the ForeScout appliance suite with network routers, switches, firewalls and VPN gateways to provide cybersecurity compliance verification, enforcement and available remediation actions, when implemented, for network access control and secure remote computing.

3.22 **Network Equipment Configuration Compliance Monitoring**

3.22.1 The Contractor shall manage RedSeal appliances to continuously monitor cybersecurity compliance of configuration of CNIC network equipment and configuration change activities. Any network equipment configuration changes shall be reviewed to confirm that they are legitimate and authorized changes.

3.23 **Maintenance of Standard Operating Procedures**

The Contractor shall be responsible for maintaining the SOP of the C2SOC, including:

a. Adding new SOP items including new processes, procedures, forms, lists, etc. as they are introduced for C2SOC operations,

b. Updating existing SOP items to reflect changes and deletion of processes, procedures, forms, lists, etc.

c. Maintaining the collection of the latest set of SOP items in the N6C-managed and designated shared portal, and

d. Providing either hardcopy or online access of the latest set of SOP items to all C2SOC watch station and watch analysts.

3.24 **Cybersecurity Reporting**

3.24.1 Per designated CNIC HQ N6 representative review and approval, the Contractor shall implement a real-time dashboard reporting the status of key C2SOC indicators by gathering data from CNIC's security services. The dashboard shall include:

a. Key C2SOC statistics such as number of outstanding incidents and estimated time to resolution, number of outstanding service requests

b. List of top three outstanding incidents and estimated time to resolution

c. List of top three outstanding service requests and estimated time to completion

d. Operational status of all C2SOC tools

3.25 **Weekly Summary and Statistics**

3.25.1 The Contractor shall collect weekly statistics, prepare and submit weekly summary to the SPAWAR LANT COR. Statistics and weekly summary will be delivered to the designated CNIC HQ N6 representative by noon of the first business workday of the following week. The weekly summary shall include:

a. Breakdown of weekly hours expended by each category and/or key subcategory of the cybersecurity operations,

b. Present weekly hours expended by key subcategories in pie chart showing distribution of efforts,

c. Present weekly hours expended by key subcategories in line chart showing trends in the last eight weeks, and

d. Statistics of cybersecurity activities performed, including vulnerabilities scans; vulnerability management, including IAVA and IAVB; incident responses; completion of coordinating DoD mandates, including CTOs, WARNORDs, OTMs, Operational Orders (OPORDs) and FRAGOs.

3.25.2 The Contractor shall assist CNIC in submitting required DoD cybersecurity reports, including:

a. Online Compliance Reporting System (OCRS) or Vulnerability Remediation Asset Manager (VRAM).

b. Continuous Monitoring and Risk Scoring System (CMRS) to follow DISA standards.

3.26 **Cyber Security Assessment and Authorization**

3.26.1 The Contractor shall support and execute requirements for Certification and Accreditation of CNIC's IM/IT/C2 Capabilities.

3.26.2 In compliance with DoD Cybersecurity/IA C&A Directives and Processes, the contractor shall:

a. Provide assistance to system owner, enclave, or site personnel to complete required C&A documentation, addressing Independent Validation and Verification (IV&V) results and assisting enclave personnel in preparing Approval and Interim Approval to Operate (ATO) (IATO) for review by the Validator, Certifying Authority (CA), and the Auhtorizing Official (AO).

b. Review Security Design documentation to ensure comprehensive security requirements and compliance with DoD and Federal requirements and guidelines

c. Review and provide input on physical, application and networking security polices procedures and practices

d. Update CNIC N6 C&A Standard Operating Procedures (SOP) so that it aligns to DoD/DON policies

e. Provide documentation support in the form of assisting with the writing and production of SOPs, Operational Manuals and review of government established and created Policies and Procedures as needed

f. Support the implementation of Federal IT Security regulations, directives and guidance (Federal Information Security Management Act - FISMA, Federal Information Processing Standard - FIPS, National Institute of Standards and Technology - NIST series)

g. Document the IA test plan and procedures templates for inclusion in the C&A Plan to appropriately relate the testing standard identified by the DAA/Navy Authorizing Official (NAO) and CA.

3.26.3 Provide assistance to system owner, enclave, or site personnel to complete required C&A or A&A documentation, addressing Independent Validation and Verification (IV&V) results and assisting enclave personnel in preparing Approval and Interim Approval to Operate (ATO) (IATO) for review by the Validator, Certifying Authority (CA), and the AO

a. Review Security Design documentation to ensure comprehensive security requirements and compliance with DoD and Federal requirements and guidelines

b. Review and provide input on physical, application and networking security polices procedures and practices

c. Update CNIC N6 C&A Standard Operating Procedures (SOP) so that it aligns to DoD/DON policies

d. Provide documentation support in the form of assisting with the writing and production of SOPs, Operational Manuals and review of government established and created Policies and Procedures as needed

e. Support the implementation of Federal IT Security regulations, directives and guidance (Federal Information Security Management Act - FISMA, Federal Information Processing Standard - FIPS, National Institute of Standards and Technology - NIST series)

f. Document the IA test plan and procedures templates for inclusion in the C&A Plan to appropriately relate the testing standard identified by the DAA/Navy Authorizing Official (NAO) and CA.

3.27 **Support C&A Program Efforts with stakeholders**

3.27.1 In compliance with DoD Cybersecurity/IA C&A Directives and Processes, the contractor shall:

a. Review updates of the DIACAP/Risk Management Framework (RMF) artifacts from the system owner and track status of changes

b. Assist in the development of the path to complete accreditation

c. Assemble the DIACAP/RMF Package, (DIACAP/RMF Scorecard, POA&M, Certification Documentation, and System-provided System Identification Profiles (SIPs) and DIACAP/RMF Implementation Plans) as appropriate

d. Deliver the DIACAP/RMF Package to the CA in a trusted manner consistent with CNIC and/or Program requirements

e. Provide C&A support in the areas of network topologies, file/application

f. Assess IA POA&M scheduling and completeness status and report

g. Track assigned system from initiation to retirement, staying informed of IV&V milestones and DIACAP/RMF POA&M deadlines

h. Address accreditation questions from the Program Management Office (PMO)

i. Maintain accreditation schedules for systems. Work with the PMO to ensure the correct C&A process is being followed

j. Adhere to certification guidance received from the CA and perform actions necessary to complete certification

k. Participate in all test execution and planning activities, including meetings and working groups, as needed

l. Participate in DIACAP/RMF Team Meetings and System review related meetings to provide technical and non-technical guidance,

m. Identify and elevate the need for any additional IA test events needed to support accreditation (Includes scheduling of annual reviews)

3.28 **Cybersecurity Validation Readiness Review**

3.28.1 In compliance with DoD Cybersecurity/IA C&A Directives and Processes, the contractor shall:

a. Review and evaluation Self-Assessment results and evidence during Readiness Review to determine if the security is sufficiently mature to execute an IA certification test event

b. Determine the IA test level of effort for each planned System and participate in all test execution and planning activities, including meetings and working groups.

3.29 **Independent Verification and Validation (IV&V)**

3.29.1 In compliance with DoD Cybersecurity/IA C&A Directives and Processes, the contractor shall:

a. Review DIACAP/RMF documentation prior to IV&V to determine security readiness of system, site, or enclave

b. Support the IV&V testing of each system, site, or enclave under the CA andAO purview

c. Participate in all test execution and planning activities, including meetings and working groups

d. Review all C&A documentation to ensure the information is current, accurate, and applicable to the article of test.

e. To support standardization, ensure that all IA test procedures are up to date with all current applicable requirements and that those methods of testing are widely visible and available for CNIC to apply to all necessary systems across its enterprise

f. Produce individualized IA test procedures for inclusion in the Test Plan that describe how to perform validation actions as outlined in the applicable STIG checklists

g. Analyze previous IA testing artifacts to tailor IA tests

h. Develop IV&V Test Plan, provide to system owner, documentation team, and IV&V team

i Oversee the execution of IA certification testing to identify all vulnerabilities, and document residual risks by conducting thorough risk assessments

j. Provide the IA risk analysis and mitigation determination results for use in the test report

k. Implement/Utilize automated tools, for the creation of necessary test evidence, risk assessment, and certification artifacts for each system

l. Perform wireless discovery using DoD software Flying Squirrel and Caribou

m. Perform testing with WebInspect

n. Perform testing with tools to manage the test procedures and results

o. Validator and IV&V Representatives to review DIACAP/RMF documentation prior to IV&V

p. Schedule IV&V events and assign IV&V team members to meet the requirements of the IV&V test plan

q. Provide status report to the Government PM on progress/results of IA testing

r. Identify and elevate the need for any additional IA test events needed to support accreditation (Includes scheduling of annual reviews)

s. Coordinate test planning with SMEs identified from IA Validation Team with the CA

3.30 **Certification and Accreditation (C&A) Documentation Support**

3.30.1 Develop all C&A documentation in accordance with DoD policies, CNIC policies and procedures to ensure that accreditation packages are complete and system compliance is met for Navy Authorizing Official

a. Maintain documentation of Plan of Action and Milestones

b. Develop C&A documentation to ensure the information is current, accurate, and applicable to the article of test

c. Develop IA self-assessment results and evidence during Information Assurance Validation Readiness Review (IAVRR) to determine if the system security is sufficiently mature to execute the IA certification test event

d. Participate in DIACAP / RMF Team Meetings

e. Utilize Enterprise Mission Assurance Support Services (eMASS) and the Vulnerability Remediation Asset Manager (VRAM) for the documentation of test evidence and risk assessment for each system

f. Develop required artifacts and provide security control implementation information for C&A Packages

g. Develop associated DIACAP / RMF IA Artifacts to include the System Security Plan, System Design and Architecture, Contingency Plan/COOP Plan, Incident Response Plan, Audit Design, Change Control Board, Identification and Authentication, Physical and Environmental, and Remote Access artifacts

3.31 **Information Assurance Self Assessments and Cybersecurity Inspection and Certification Program (CISCP) Phase II Cybersecurity Inspections**

3.31.1 Preparations:

a. Work with IV&V Lead from CNIC to develop Test Plan

b. Participate in System related meetings

c. Prepare for onsite self-assessment and/or CSICP Phase II inspection

3.31.2 Self-Assessment Execution:

a. Execute tests per the Test Plan

b. Prepare test events status reports and outbriefs

c. Populate Validator database/VRAM/eMASS with test results

d. Contribute to Test Event Reporting

e. Assemble DIACAP / RMF Package (DIACAP / RMFScorecard)

f. Plans of Action & Milestones (POA&M), Certification Documentation, and System-provided System Identification Profiles (SIP) & DIACAP / RMF Implementation Plans)

g. Develop plans to validation actions as outlined in the applicable Security Technical Implementation Guide (STIG) checklists

h. Validate DIACAP / RMF Implementation Plan (DIP)

i. Assist IA Analyst / Test Team Lead with evaluating IA self-assessment results and evidence

j. Participate in DIACAP / RMF Team Meetings

k. Ensure IA test procedures are available and visible for use of replication across System using the same software

l. Utilize eMASS and VRAM for the documentation of test evidence and risk assessment for each System

m. Create Policy and provide Policy Guidance

i. Develop/maintain agency level cybersecurity policy and processes that implements DoD Cybersecurity program

ii. Develop/maintain agency level cybersecurity policies and processes

iii. Develop/maintain agency level RMF policy

iv. Provide training, reporting, guidance and support to meet the requirements of the DoD IA Workforce Improvement Program

v. Provide guidance on recommended contracting language for built in security for IT solutions

vi. Ensures enterprise-wide compliance reporting is standardized across CNIC and meets DoD cybersecurity policy requirements

vii. Provide IT Exercise and Contingency Planning

viii. Provide guidance and support related IT contingency planning (ITCP)

ix. Develop templates in support of ITCP

x. Develop and maintain procedures related to tabletop exercises for contingency plans,as well as develop scenarios

xi. Support execution of tabletop exercises for CNIC community

xii. Participating in the tabletop exercises

3.31.3 **Cybersecurity Workforce (CSWF) Report**

3.31.3.1 CSWF Reports (CDRL A007) shall be developed, maintained, and submitted monthly at the contract or task order level. If Information Assurance (IA) support is provided, the contractor shall provide a Cybersecurity Workforce (CSWF) list that identifies those individuals who are IA trained and certified.

3.31.3.2 Asset reports are required for the physical and electronic receipt, inventory, and transfer of cybersecurity related hardware, software, appliances, equipment, and resources. The contractor shall actively manage all assets of cybersecurity related hard, software, appliances and systems, including:

a Maintenance of asset database to the extent that inventory updates of newly installed or moved systems are input,

b Maintenance of configuration,

c Management of receiving of new assets, shipment of assets and their location, deployment status,

d Disposition of N6 approved hardware, software, appliances, equipment and resources, including data destruction of the sensitive data on CNIC IT equipment to be disposed in accordance with N6 approved data deposition process,

e Yearly audit of cybersecurity operational inventory with Code N6 supervision

f Projection of annual recurring costs for software license and support service renewal

g Recommendation of new assets requirements, and

h Preparation of asset reports based on inventory data, projections and recommendations.

3.31.4 **Configuration Management**

3.31.4.1 The Contractor shall actively manage configuration of all assets of cybersecurity managed related hardware, software, appliances and system. Configuration Management (CM) provides governance to establish and maintain the integrity of asset Configuration Items (CIs), such as IT service software, assets, products, devices, and documentation, throughout the CI lifecycle. CM provides governance over the procedures by which tasks can effectively manage, modify, and version these service asset CIs in order to create and maintain an accurate baseline. This baseline is the foundation for lifecycle.

a. Administer the CNIC cybersecurity management related CM program in accordance with established CM policy,

b. Provide the daily management and oversight of the CM tools,

c. Establish and document Operations and Maintenance procedures for the CM tools

d. Maintain applicable items in the N6 electronic document library for cybersecurity assets,

e. Review all cybersecurity CM related documentation and provide valuable comments/feedback,

f. Participate in all CM related ad hoc meeting requests,

g. Maintain an accurate accounting of all configuration items that are associated with CNIC cybersecurity,

h. Recommend and document configuration identification standards for software, hardware, and documentation CIs,

i. Conduct a review of the system CIs for each release to ensure systems comply with the establishment of a baseline for each release

j. Conduct configuration audits and accounting at least annually.

k. Conduct the following Change Management activities:

i. Administer the CNIC cybersecurity related Change Management program in accordance with established policy,

ii. Provide project support and have knowledge of the CNIC Code N6 Change Control Processes,

iii. Assist in review and impact assessment of various cybersecurity related Change Requests (CRs) as necessary,

iv. Update change policy to support lean and service oriented change practices, and

v. Continuously evaluate external and internal policies and practices to reduce unessential practices.

3.31.5 **Software engineering**

Software engineering includes the design and documentation of software to support a specific government requirement.

3.31.5.1 The contractor shall utilize certified software and computer personnel. The contractor (prime and/or subcontractor) that supports software efforts shall define a software approach appropriate for the computer software effort to be performed under each task.

3.31.5.2 The contractor shall document the approach in the CNIC Software Development Plan (SDP).

3.31.5.3 The contractor shall follow this SDP for all computer software to be developed or maintained under this effort.

3.31.5.4 The contractor shall ensure the SDP meets the criteria specified in the CDRL DD1423 using IEEE Std 12207-2008 and the PWS tasking.

4.0 INFORMATION TECHNOLOGY (IT) SERVICES REQUIREMENTS

4.1 INFORMATION TECHNOLOGY (IT) GENERAL REQUIREMENTS

The contractor shall be responsible for the following:

4.1.1 Ensure that no production systems are operational on any research, development, test and evaluation (RDT&E) network.

4.1.2 Follow DoDI 8510.01 when deploying, integrating, and implementing IT capabilities.

4.1.3 Migrate all Navy Ashore production systems to the Navy, Marine Corps Intranet (NMCI) environment where available.

4.1.4 Work with Government personnel to ensure compliance with all current Navy IT & cybersecurity policies, including those pertaining to Cyber Asset Reduction and Security (CARS).

4.1.5 Follow SECNAVINST 5239.3B & DoDI 8510.01 prior to integration and implementation of IT solutions or systems.

4.1.6 Register any contractor-owned or contractor-maintained IT systems utilized on task order in the Department of Defense IT Portfolio Registry (DITPR)-DON.

4.1.7 Ensure all software recommended, procured, and/or developed is compliant with Section 508 of the Rehabilitation Act of 1973, 26 CFR Part 1194 and pursuant to SPAWARINST 5721.1B.

4.1.8 Only perform work specified within the limitations of the basic contract and task order.

4.2 ACQUISITION OF COMMERCIAL SOFTWARE PRODUCTS, HARDWARE, AND RELATED SERVICES

Contractors recommending or purchasing commercial software products, hardware, and related services supporting Navy programs and projects shall ensure they recommend or procure items from approved sources in accordance with the latest DoN and DoD policies.

4.2.1 DoN Application and Database Management System (DADMS)

The contractor shall ensure that no Functional Area Manager (FAM) disapproved applications are integrated, installed or operational on Navy networks. The contractor shall ensure that all databases that use database management systems (DBMS) designed, implemented, and/or hosted on servers and/or mainframes supporting Navy applications and systems be registered in DoN Application and Database Management System (DADMS) and are FAM approved. All integrated, installed, or operational applications hosted on Navy networks must also be registered in DADMS and approved by the FAM. No operational systems or applications will be integrated, installed, or operational on the RDT&E network.

4.2.2 Cybersecurity/Computer Security Requirements

The contractor shall ensure that all products recommended and/or procured that impact cybersecurity or Information Assurance (IA) shall be selected from the National Information Assurance Partnership (NIAP) Validated Products List. The contractor shall ensure the products chosen are based on the appropriate Evaluated Assurance Level (EAL) for the network involved, and are utilized in accordance with latest Defense Information Systems Agency (DISA) policy at time of order. The contractor shall store all product information and have it available for government review at any time.

4.3 SECURITY IT POSITION CATEGORIES

Pursuant to DoDI 8500.01, DoD 8570.01-M, SECNAVINST 5510.30, SECNAV M-5239.2, and applicable to unclassified DoD information systems, a designator is assigned to certain individuals that indicates the level of IT access required to execute the responsibilities of the position based on the potential for an individual assigned to the position to adversely impact DoD missions or functions. As defined in DoD 5200.2-R (and subsequent revisions), SECNAVINST 5510.30 and SECNAV M-5510.30, three basic DoN IT levels/Position categories exist:

- IT-I (Privileged access)
- IT-II (Limited Privileged, sensitive information)
- IT-III (Non-Privileged, no sensitive information)

Note: The term IT Position is synonymous with the older term Automated Data Processing (ADP) Position (as used in DoD 5200.2-R, Appendix 10).

Investigative requirements for each category vary, depending on the role and whether the individual is a U.S. civilian contractor or a foreign national. The contractor PM shall assist the Government Project Manager or Contracting Officer's Representative (COR) in determining the appropriate IT Position Category assignment for all contractor personnel. All required Single-Scope Background Investigation (SSBI), SSBI Periodic Reinvestigation (SSBI-PR), and National Agency Check (NAC) adjudication will be performed Pursuant to DoDI 8500.01 and SECNAVINST 5510.30. Requests for investigation of contractor personnel for fitness determinations or IT eligibility without classified access are submitted by SPAWARSYSCEN Atlantic Security Office, processed by the OPM, and adjudicated by Department of Defense Consolidated Adjudications Facility (DoD CAF). IT Position Categories are determined based on the following criteria:

4.3.1 IT-I Level (Privileged)

Personnel in this position support cybersecurity roles at command enclave infrastructure to include RDT&E, Data Centers and any other network and/or are responsible for the planning, direction, and implementation of a computer security program; major responsibility for the direction, planning and design of a computer system, including the hardware and software; or, can access a system during the operation or maintenance in such a way, and with a relatively high risk for causing grave damage, or realize a significant personal gain. Personnel whose duties meet the criteria for IT-I Position designation shall have a favorably adjudicated Tier 5 (T5) investigation (formerly a Single Scope Background Investigation (SSBI) or SSBI-PR). The T5 is updated a minimum of every 5 years. Personnel assigned to designated IT-I positions shall have a U.S. citizenship unless a waiver request is approved by CNO. IT-1 roles include the following:

- Boundary Devices Management (proxies, firewalls, traffic analyzers, VPN Gateways)
- Intrusion Detection/Prevention Systems (IDS/IPS)
- Host Based Security Systems (HBSS)
- Network infrastructure (routers, switches, enterprise wireless)
- Domain and Authentication System Administrators (Active Directory, LDAP, Kerberos, etc.) (enclave wide scope)
- Vulnerability Scanner Operators (Retina, ACAS, HP Web Inspect, etc.)
- Virtualization Technology Administrators that host any of the above (ESX, Solaris Zones, etc.)

4.3.2 IT-II Level (Limited Privileged)

Personnel in this position support the-direction, planning, design, operation, or maintenance of a computer system, have privileged access to assets and systems that are tenants on SPAWARSYSCEN Atlantic networks and/or similar system constructs, and has work that is technically reviewed by a higher authority at the IT-II Position level to ensure the integrity of the system. Personnel whose duties meet the criteria for an IT-II Position shall have a favorably adjudicated Tier 3 (T3) investigation (formerly National Agency Check with Law and Credit (formerly ANACI/NACLC). Personnel assigned to designated IT-II positions shall have a U.S. citizenship unless a waiver request is approved by CNO. Examples of IT-II roles include the following:

- Webserver Administrators
- Developers
- Testers
- Database Administrators

4.3.3 IT-III Level (Non-privileged)

Personnel in this position support include all other positions (not considered IT-I or IT-II) involved in computer activities. A contractor in this position has non-privileged access to one or more DoD information systems/applications or database to which they are authorized access. Personnel whose duties meet the criteria for an IT-III Position designation shall have a favorably adjudicated Tier 1 (T1) investigation National Agency Check with Written Inquiries (formerly NACI).

4.4 CYBERSECURITY SUPPORT

Cybersecurity (which replaced the term Information Assurance (IA)) is defined as prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. Contractor personnel shall perform tasks to ensure Navy applications, systems, and networks satisfy Federal/DoD/DON/Navy cybersecurity requirements.

4.4.1 Cyber IT and Cybersecurity Personnel

4.4.1.1 The Cyberspace workforce elements addressed include contractors performing functions in designated Cyber IT positions and Cybersecurity positions. In accordance with DFARS Subpart 239.71, DoDD 8140.01, SECNAVINST 5239.20A, and SECNAV M-5239.2, contractor personnel performing cybersecurity functions shall meet all cybersecurity training, certification, and tracking requirements as cited in DoD 8570.01-M and subsequent manual [DoD 8140] when applicable prior to accessing DoD information systems. Proposed contractor Cyber IT and cybersecurity personnel shall be appropriately qualified prior to the start of the task order performance period or before assignment to the task order during the course of the performance period.

4.4.1.2 Contractors that access Navy IT shall also follow guidelines and provisions documented in Navy Telecommunications Directive (NTD 10-11) and are required to complete a System Authorization Access Request (SAAR) – Navy form as documented in Para 8.2.2.4(b).

4.4.1.3 Contractor personnel with privileged access shall acknowledge special responsibilities with a Privileged Access Agreement (PAA) IAW SECNAVINST 5239.20A.

4.4.2 Design, Integration, Configuration or Installation of Hardware and Software

The contractor shall ensure any equipment/system installed or integrated into Navy platform will meet the cybersecurity requirements as specified under DoDI 8500.01. The contractor shall ensure that any design change, integration change, configuration change, or installation of hardware and software is in accordance with established DoD/DON/Navy cyber directives and does not violate the terms and conditions of the accreditation/authorization issued by the appropriate Accreditation/Authorization official. Contractors that access Navy IT are also required to follow the provisions contained in DON CIO Memorandum: Acceptable Use of Department of the Navy Information Technology (IT) dtd 12 Feb 16. Use of blacklisted software is specifically prohibited and only software that is registered in DON Application and Database Management System (DADMS) and is Functional Area Manager (FAM) approved can be used as documented in Para 4.2.1. Procurement and installation of software governed by DON Enterprise License Agreements (ELAs) – Microsoft, Oracle, Cisco, Axway, Symantec, ActivIdentity, VMware, Red Hat, NetApp, and EMC shall be in accordance with DON CIO Policy and DON ELAs awarded.

4.4.3 Cybersecurity Workforce (CSWF) Report

In accordance with DFARS clause 252.239-7001 and DoD 8570.01-M, the contractor shall identify cybersecurity personnel, also known as CSWF and Cyber IT workforce personnel. The contractor shall develop, maintain, and submit a monthly CSWF Report (CDRL A007) identifying CSWF individuals who are IA trained and certified. Utilizing the format provided in CDRL A007 of Exhibit A, the prime contractor shall be responsible for collecting, integrating, and reporting all subcontractor personnel. See applicable DD Form 1423 for additional reporting details and distribution instructions. Although the minimum frequency of reporting is monthly, the COR can require additional updates at any time. Contractor shall verify with the COR or other Government representative the proper labor category CSWF designation and certification requirements. The primary point of contact (POC) for all related CSWF questions is the Command CSWF Program Manager (PM) in the office of the SPAWARSYSCEN Atlantic Information Systems Security Manager (ISSM).

4.4.4 Cybersecurity Workforce (CSWF) Designation

CSWF contractor personnel shall perform cybersecurity functions. In accordance with DoD 8570.01-M Information Assurance Workforce Improvement Program Manual, the CSWF is comprised of the following categories: IA Technical (IAT) and IA Management (IAM)); and specialties: Computer Network Defense Service Providers (CND-SPs) and IA System Architects and Engineers (IASAEs). Based on the IA function provided by the individual, an IA designator is assigned that references an IA

category or specialty. The following Labor Categories shall meet the IA Designator, IA Level/Position, and have the estimated Primary/Additional/Embedded hours performing IA duties:

Labor Category	Quantity Personnel	IA Designator	IA level/Position	25 hrs	15-24 hrs	1-14 hrs
SME 1	1	IAM	Level 2	X		
SME 1	1	IAT	Level 1	X		
SME 3	2	IAM	Level 1	X		
SME 3	1	IAM	Level 3	X		
SME 4	2	IAM	Level 1	X		
SME 4	1	IAT	Level 1	X		
SME 4	1	CND	Level 1	X		
SME 4	1	IAT	Level 2	X		
SME 4	1	IAM	Level 2	X		
SME 4	1	IAM	Level 3	X		
SME 5	3	IAM	Level 1	X		
SME 5	1	IAT	Level 1	X		
SME 5	5	IAM	Level 3	X		
Engineer/Scientist 3	1	IAT	Level 1	X		
Engineer/Scientist 3	6	IAM	Level 2	X		
Engineer/Scientist 3	1	IAM	Level 3	X		
Engineer/Scientist 4	7	IAM	Level 1	X		
Engineer/Scientist 4	1	IAT	Level 1	X		
Engineer/Scientist 4	1	IAT	Level 2	X		
Engineer/Scientist 4	2	IAM	Level 2	X		
Engineer/Scientist 5	9	IAM	Level 1	X		
Engineer/Scientist 5	2	IAM	Level 3	X		
Engineer/Scientist 5	1	IAT	Level 3	X		

5.0 TASK ORDER ADMINISTRATION

Administration of the work being performed is required; it provides the Government a means for task order management and monitoring. Regardless of the level of support, the ultimate objective of the contractor is ensuring the Government's requirements are met, delivered on schedule, and performed within budget.

5.1 CONTRACTING OFFICER REPRESENTATIVE (COR) DESIGNATION

The COR for this task order is identified in task order clause G-TXT-01.

5.2 CONTRACTOR LIAISON

The contractor shall assign a technical single point of contact, also known as the Program Manager (PM) who shall work closely with the Government Contracting Officer and COR. The contractor PM, located in the contractor's facility, shall ultimately be responsible for ensuring that the contractor's performance meets all Government contracting requirements within cost and schedule. PM shall have the requisite authority for full control over all company resources necessary for task order performance and be available to support emergent situations. The PM shall ultimately be responsible for the following: personnel management; management of Government material and assets; and personnel and facility security. In support of open communication, the contractor shall initiate periodic meetings with the COR.

5.3 CONTRACTOR MONITORING AND MAINTENANCE

The contractor shall have processes established in order to provide all necessary resources and documentation during various times throughout the day including business and non-business hours in order to facilitate a timely task order response or modification in particularly during urgent requirements.

5.3.1 Task order Administration & Documentation

Various types of administration documents are required throughout the life of the task order. At a minimum, the contractor shall provide the following documentation:

5.3.1.1 Task Order Status Report (TOSR)

The contractor shall develop a Task Order Status Reports (CDRL A001) and submit them monthly, weekly, and/or as cited in the requirements of this task order. The prime contractor shall be responsible for collecting, integrating, and reporting all subcontractor reports. The TOSR include the following variations of reports:

(a) Monthly TOSR – the contractor shall develop and submit a Task Order Status Report monthly at least 30 days after task order award and on the 10th of each month for those months the task order is active. The contractor shall report on various task order functions: performance, schedule, financial, business relations, and staffing plan/key personnel; see applicable DD Form 1423 for additional reporting details and distribution instructions. This CDRL includes a Staffing Plan (CDRL A001) and Personnel Listing (CDRL A001) necessary for additional data collection as applicable.

(b) Data Calls – the contractor shall develop and submit a data call report which is e-mailed to the COR within six working hours of the request. The contractor shall ensure all information provided is the most current. Cost and funding data will reflect real-time balances. Report will account for all planned, obligated, and expended charges and hours. At a minimum, the contractor shall include in the data call the following items and data:

1. Percentage of work completed

2. Percentage of funds expended

3. Updates to the POA&M and narratives to explain any variances

4. List of personnel (by location, security clearance, quantity)

5.3.1.2 Task Order Closeout Report

The contractor shall develop a Task Order Closeout Report (CDRL A002) and submit it no later than 15 days before the task order completion date. The prime contractor shall be responsible for collecting, integrating, and reporting all subcontracting information. See applicable DD Form 1423 for additional reporting details and distribution instructions.

5.3.1.3 Enterprise-wide Contractor Manpower Reporting Application

Pursuant to NMCARS 5237.102-90, the contractor shall report all contractor labor hours (including subcontractor labor hours) required for performance of services provided under this task order for the DoD via a secure data collection website – Enterprise-wide Contractor Manpower Reporting Application (eCMRA). The Product/Service Codes (PSC) for contracted services excluded from reporting are as follows:

(1) W, Lease/Rental of Equipment;

(2) X, Lease/Rental of Facilities;

(3) Y, Construction of Structures and Facilities;

(4) S, Utilities ONLY;

(5) V, Freight and Shipping ONLY.

The contractor shall completely fill-in all required data fields using the following web address: https://www.ecrma.mil/. Reporting inputs consists of labor hours executed during the task order period of performance within each Government fiscal year (FY) which runs from October 1 through September 30. While inputs may be reported any time during the FY, the contractor shall report all data no later than October 31 of each calendar year. Contractors may direct questions to the help desk at https://www.ecrma.mil/.

5.3.1.4 WAWF Invoicing Notification and Support Documentation

Pursuant to DFARS clause 252.232-7003 and 252.232-7006, the contractor shall submit payment requests and receiving reports using DoD Invoicing, Receipt, Acceptance, and Property Transfer (iRAPT) application (part of the Wide Area Work Flow (WAWF) e-Business Suite) which is a secure Government web-based system for electronic invoicing, receipt, and acceptance. The contractor shall provide e-mail notification to the COR when payment requests are submitted to the iRAPT/WAWF and the contractor shall include cost back–up documentation (e.g., delivery receipts, time sheets, & material/travel costs, etc.) to the invoice in iRAPT/WAWF. When requested by the COR, the contractor shall directly provide a soft copy of the invoice and any supporting invoice documentation (CDRL A003) directly to the COR within 24 hours of request to assist in validating the invoiced amount against the products/services provided during the billing cycle.

5.3.1.5 ODC Limitation Notification

The contractor shall monitor Other Direct Costs (ODCs) as part of the monthly TOSR. For this monitoring purpose, ODCs include incidental material, travel, and other non-labor costs (excluding subcontracting and consultant labor cost) required in performance of the service. For any given period of performance, if the cumulative total cost of ODCs exceeds the awarded total cost of ODCs (regardless of any modifications to the awarded amount) by 10%, the contractor shall send notice and rationale (CDRL A008) for exceeding cost to the COR who will then send a memorandum signed by the PM (or equivalent) to the Contracting Officer documenting the reasons justifying the increase of ODC. The ability of a contractor to monitor ODCs will be included in the task order QASP.

5.3.1.6 Limitation of Subcontracting

In accordance with FAR clause 52.219-14, limitation of subcontracting is applicable for task orders that have been wholly or partially set aside for small business or 8(a) concerns. The contactor shall develop and submit a Limitation of Subcontracting Report (LSR) (CDRL A009) every 3 months. See applicable DD Form 1423 for reporting details and distribution instructions. The labor cost provided should correspond to the cumulative monthly submitted invoices. The Government reserves the right to perform spot checks and/or request copies of any supporting documentation.

5.4 CONTRACTOR PERFORMANCE MANAGEMENT

Contractor performance standards and requirements are outlined in the task order QASP. The ability of a contractor to perform to the outlined standards and requirement will be captured in the Contractor Performance Assessment Reporting System (CPARS). In support of tracking contractor performance, the contractor shall provide the following documents: Cost and Schedule Milestone Plan (CDRL A004) submitted 10 days after task order award and CPARS Draft Approval Document (CDAD) Report (CDRL A005) submitted monthly.

5.5 EARNED VALUE MANAGEMENT (EVM)

In accordance with DoD policy, this task order does not require Earned Value Management (EVM) implementation due to the majority of efforts on this task order is non-scheduled based (*i.e.*, level of effort) and does not lend itself to meaningful EVM information.

6.0 DOCUMENTATION AND DELIVERABLES

6.1 CONTRACT DATA REQUIREMENTS LIST (CDRL)

The following listing identifies the data item deliverables required under this task order and the applicable section of the PWS for which they are required. Section J includes the DD Form 1423s that itemize each Contract Data Requirements List (CDRL) required under the basic contract. The contractor shall establish a practical and cost-effective system for developing and tracking the required CDRLs generated under each task. The contractor shall not develop any CDRL classified TOP SECRET with SCI.

6.1.1 Administrative CDRL

The following table lists all required administrative data deliverables, CDRLs, applicable to this task:

CDRL's	Deliverable Title	PWS Reference Para	Frequency	Date Due
A001	Task Order Status Report (TOSR)	3.1.1.1, 3.1.1.3, 5.3.1.1, 8.1.2, 8.2.3.1	MTHLY	30 DATO and monthly on the 10th
A002	Task Order Closeout Report	5.3.1.2	1TIME	NLT 15 days before completion date
A003	Invoice Support Documentation	5.3.1.4	ASREQ	Within 24 hrs from request
A004	Cost and Milestones Schedule Plan	5.4	One time with revisions (ONE/R)	NLT 10 DATO; revision NLT 7 days after receipt of Govt review
A005	Contractor CPARS Draft Approval Document (CDAD) Report	5.4	MTHLY	30 DATO and monthly on the 10th
A006	OCONUS Deployment Package	11.3.1	1TIME	NLT 30 days prior to travel
A007	Cybersecurity Workforce (CSWF) Report	3.31.4.1, 4.5.3, 8.1.2, 8.2.3.1	MTHLY	30 Days after task order award (DATO) and monthly on the 10th
A008	Limitation Notification & Rationale	5.3.1.6	ASREQ	Within 24 hrs from occurrence
A009	Limitation to Subcontracting Report	5.3.1.7	QRTLY	NLT 105 DATO and every third month on the 10th
A010	Technical/Analysis Reports, General	3.1.1.1.6, 3.1.1.1.8	QRTLY	NLT 105 DATO and every third month on the 10th
A011	Program Management Reports, General	3.1.1.1.5, 3.1.1.1.7	QRTLY	NLT 105 DATO and every third month on the 10th

6.2 ELECTRONIC FORMAT

At a minimum, the contractor shall provide deliverables electronically by e-mail; hard copies are only required if requested by the Government. To ensure information compatibility, the contractor shall guarantee all deliverables (i.e., CDRLs), data, correspondence, etc., are provided in a format approved by the receiving Government representative. The contractor shall provide all data in an editable format compatible with SPAWARSYSCEN Atlantic corporate standard software configuration as specified below. Contractor shall conform to SPAWARSYSCEN Atlantic corporate standards within 30 days of task order award. *The initial or future*

upgrades costs of the listed computer programs are not chargeable as a direct cost to the Government.

	Deliverable	**Software to be used**
a.	Word Processing	Microsoft Word
b.	Technical Publishing	PageMaker/Interleaf/SGML/ MSPublisher
c.	Spreadsheet/Graphics	Microsoft Excel
d.	Presentations	Microsoft PowerPoint
e.	2-D Drawings/ Graphics/Schematics (new data products)	Vector (CGM/SVG)
f.	2-D Drawings/ Graphics/Schematics (existing data products)	Raster (CALS Type I, TIFF/BMP, JPEG, PNG)
g.	Scheduling	Microsoft Project
h.	Computer Aid Design (CAD) Drawings	AutoCAD/Visio
i.	Geographic Information System (GIS)	ArcInfo/ArcView

6.3 INFORMATION SYSTEM

6.3.1 Electronic Communication

The contractor shall have broadband Internet connectivity and an industry standard email system for communication with the Government. The contractor shall be capable of Public Key Infrastructure (PKI) client side authentication to DOD private web servers. Unless otherwise specified, all key personnel on task shall be accessible by e-mail through individual accounts during all hours.

6.3.2 Information Security

Pursuant to DoDM 5200.01, the contractor shall provide adequate security for all unclassified DoD information passing through non-DoD information system including all subcontractor information systems utilized on task. The contractor shall disseminate unclassified DoD information within the scope of assigned duties and with a clear expectation that confidentiality is preserved. Examples of such information include the following: non-public information provided to the contractor, information developed during the course of the task order, and privileged task order information (e.g., program schedules and task order-related tracking).

6.3.2.1 Safeguards

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

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

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

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

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

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

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

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

(h) Do not post DoD information to Web site pages that are publicly available or have access limited only by domain or Internet protocol restriction. Such information may be posted to Web site pages that control access by user identification or password, user certificates, or other technical means and provide protection via use of TLS or other equivalent technologies. Access control may be provided by the intranet (vice the Web site itself or the application it hosts).

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

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

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

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

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

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

6.3.2.2 Compliance

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

7.0 QUALITY

7.1 QUALITY SYSTEM

Upon task order award, the prime contractor shall have and maintain a quality system that meets contract and task order requirements and program objectives while ensuring customer satisfaction and defect-free products/process. The contractor shall have an adequately documented quality system which contains processes, procedures, planning, and all other documentation and data necessary to provide an efficient and effective quality system, which includes an internal auditing system. Thirty (30) days after task order award, the contractor shall be able to provide, as requested by the Government, a copy of the contractor's Quality Assurance Plan (QAP) and any other quality related documents (CDRL A. The contractor shall make their quality system available to the Government for review at both a program and worksite services level during predetermined visits. Existing quality documents that meet the requirements of this task order may continue to be used. If any quality documentation is disapproved or requires revisions, the contractor shall correct the problem(s) and submit revised documentation NLT 2 weeks after initial disapproval notification. The contractor shall also require all subcontractors to possess a quality assurance and control program commensurate with the services and supplies to be provided as determined by the prime's internal audit system. The Government reserves the right to disapprove the contractor's and/or subcontractor's quality system or portions thereof when the quality system(s) fails to meet contractual requirements at either the program or worksite services level. The Government reserves the right to participate in the process improvement elements of the contractor's quality assurance plan or quality system, and development of quality related documents. At a minimum, the contractor shall ensure their quality system meets the following key criteria:

- Establish documented, capable, and repeatable processes
- Track issues and associated changes needed
- Monitor and control critical process, product, and service variations
- Establish mechanisms for feedback of field product and service performance

- Implement and effective root-cause analysis and corrective action system
- Establish methods and procedures and create data used for continuous process improvement

7.2 MANAGE QUALITY COMPLIANCE

7.2.1 General

The contractor shall have quality processes or a Quality Management System (QMS) processes in place that coincide with the Government's Manage Quality processes which address Quality Control, Quality Assurance, Software Quality, and/or project Quality System tasks. The contractor shall use best industry practices including, when applicable, ISO/IEC 15288 for System life cycle processes and ISO/IEC 12207 for Software life cycle processes. As applicable, the contractor shall also support and/or participate in Acquisition Milestones, Phases, and Decision Points, which are standard elements of the Defense Acquisition System and support DoDD 5000.01 and DoDI 5000.02. The contractor shall provide technical program and project management support that will mitigate the risks to successful program execution including employment and objective evidence of Lean Six Sigma, Risk Management, and System Engineering methodologies; and System and Software Engineering best practices

7.3 QUALITY ASSURANCE

The contractor shall perform all quality assurance process audits necessary in the performance of the various tasks as assigned and identified in the contractor's Quality Assurance Plan (QAP) or by the respective WBS, POA&M, or quality system/QMS documentation in support of continuous improvement. The contractor shall deliver related QAP and any associated procedural documents upon request. The Government reserves the right to perform any additional audits deemed necessary to assure that the contractor processes, products, and related services, documents, and material meet the prescribed requirements and to reject any or all processes or related products, services, documents, and material in a category when noncompliance is established.

7.4 QUALITY CONTROL

The contractor shall perform all quality control inspections necessary in the performance of the various tasks as assigned and identified in the contractor QAP or by the respective WBS, POA&M, or quality system/QMS documentation.

8.0 SECURITY

8.1 ORGANIZATION

8.1.1 Security Classification

As specified in the DoD Contract Security Classification Specification, DD Form 254 (PWS Attachment 2), the contractor shall perform classified work under this task order. At time of task order award, the contractor shall have a SECRET facility clearance (FCL).

8.1.1.1 U.S. Government security clearance eligibility is required to access and handle classified and certain controlled unclassified information (CUI), attend program meetings, and work within restricted areas unescorted. The government will escort contractors into secure areas as required following protocols established for those areas. The contractor shall not generate any SCI deliverables.

8.1.1.2 This task order allows for various levels of security to support specific PWS tasks. The following table outlines the minimum required security clearance per task. The contractor shall provide personnel meeting the specific minimum personnel clearance (PCL) to support the PWS tasks listed below

Required Security Clearance	**PWS Task Paragraph**
Secret	3.1 and 3.20
SSBI IT 1	3.2, 3.3, 3.4, 3.5, 3.6, 3.7, 3.8, 3.9, 3.10, 3.11, 3.12, 3.13, 3.14, 3.15, 3.16, 3.17, 3.18, 3.19, 3.21, 3.22,

	3.23, 3.24, 3.25, 3.26, 3.27, 3.28, 3.29, 3.30, and 3.31
None required	N/A

8.1.2 Security Officer

The contractor shall appoint a Facility Security Officer (FSO) to support those contractor personnel requiring clearance and/or access to Government facility/installation and/or access to information technology systems under this task order. The FSO is typically a key management person who is the contractor's main POC for security issues. The FSO shall have a U.S. Government security clearance equal to or higher than the FCL required on this/task order. The FSO shall be responsible for tracking the security requirements for all personnel (subcontractors included) utilized on task order. Responsibilities include tracking all personnel assigned Government badges and entering/maintaining personnel security mandatory training information within the Staffing Plan document, which is an attachment to the Task Order Status Report (TOSR) (CDRL A001), and if applicable, updating and tracking data in the CSWF Report (CDRL A007).

8.2 PERSONNEL

The contractor shall conform to the security provisions of DoDI 5220.22/DoD 5220.22-M – National Industrial Security Program Operating Manual (NISPOM), SECNAV M-5510.30, DoD 8570.01-M, and the Privacy Act of 1974. Prior to any labor hours being charged on this task order, the contractor shall ensure all personnel (including administrative and subcontractor personnel) have obtained and can maintain favorable background investigations at the appropriate level(s) for access required for the task order, and if applicable, are certified/credentialed for the CSWF (CDRL A007) A favorable background determination is determined by either a Tier 1 (T1) investigation, Tier 3 (T3) investigation, or Tier 5 (T5) investigation and favorable Federal Bureau of Investigation (FBI) fingerprint checks. Investigations are not necessarily required for personnel performing unclassified work who do not require access to Government installations/facilities, Government IT systems and IT resources, or SPAWARSYSCEN Atlantic information. *Cost to meet these security requirements is not directly chargeable to task order.*

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

8.2.1 Personnel Clearance

Some personnel associated with this task order shall possess SSBI IT 1 access for personnel security clearance (PCL) and some shall possess Secret access. On a case-by case basis, SSBI IT 1 clearances are eligible for access to Sensitive Information. These programs/tasks include, as a minimum, contractor personnel having the appropriate clearances required for access to classified data as applicable. Prior to starting work on the task, contractor personnel shall have the required clearance granted by the DoD CAF and shall comply with IT access authorization requirements. In addition, contractor personnel shall possess the appropriate IT level of access for the respective task and position assignment as applicable per DoDI 8500.01, DoD Instruction for Cybersecurity. Any future revision to the respective directive and instruction will be applied as a task order modification. Contractor personnel shall handle and safeguard any Controlled Unclassified Information (CUI) and/or classified information in accordance with appropriate Department of Defense, Navy, and SPAWARSYSCEN Atlantic security regulations. The contractor shall immediately report any security violation to the SPAWARSYSCEN Atlantic Security Management Office, the COR, and Government Project Manager. Foreign national employees employed in their home countries shall meet equivalent host U.S. Installation Command security requirements and Status of Forces Agreement (SOFA).

The following table specifies the personnel clearance by labor category:

Labor Category	Quantity Personnel	SSBI IT 1	Secret
SME 1	2	2	
SME 3	3	3	
SME 4	7	6	1

SME 5	9	9	
Engineer/Scientist 3	8	6	2
Engineer/Scientist 4	11	10	1
Engineer/Scientist 5	12	12	
Management Analyst	3		3
Program Manager	1		1

8.2.2 Access Control of Contractor Personnel

8.2.2.1 Physical Access to Government Facilities and Installations

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

(a) The majority of Government facilities require contractor personnel to have an approved visit request on file at the facility/installation security office prior to access. For admission to SPAWARSYSCEN Atlantic facilities/installations, the contractor shall forward a visit request to Joint Personnel Adjudication System (JPAS) /SMO 652366, or submit request on company or agency letterhead by fax to (843)218-4045 or mail to Space and Naval Warfare Systems Center Atlantic, P.O. Box 190022, North Charleston, SC 29419-9022, Attn: Security Office. For visitation to all other Government locations, the contractor shall forward visit request documentation directly to the on-site facility/installation security office.

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

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

8.2.2.2 Identification and Disclosure Requirements

Contractor and subcontractor employees shall take all means necessary to not represent themselves as Government employees. All contractor personnel shall follow the identification and Government facility disclosure requirement as specified in clause H-TXT-25, Contractor Identification.

8.2.2.3 Government Badge Requirements

Some contract personnel shall require a Government issued picture badge in accordance with clause H-TXT-01, Contractor Picture Badge. While on Government installations/facilities, contractors shall abide by each site's security badge requirements. Various Government installations are continually updating their security requirements to meet Homeland Security Presidential Directive (HSPD-12) identification standards. Contractors are responsible for obtaining and complying with the latest security identification requirements for their personnel. Contractors shall submit valid paper work (e.g., site visit request, request for picture badge, and/or SF-86 for CAC) to the applicable Government security office via the COR. The contractor FSO shall track all personnel holding local Government badges at the task order level.

8.2.2.4 Common Access Card (CAC) Requirements

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

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

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

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

3. Completion of background vetting requirements according to FIPS PUB 201-2 and DoD 5200.2-R – at a minimum, the completion of FBI fingerprint check with favorable results and submission of a T1 investigation to the Office of Personnel Management (OPM), or a DoD-determined equivalent investigation. NOTE: Contractor personnel requiring logical access shall obtain and maintain a favorable T3 investigation. Contractor personnel shall contact the SPAWARSYSCEN Atlantic Security Office to obtain the latest CAC requirements and procedures.

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

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

1. For annual DoD Cybersecurity/IA Awareness training, contractors shall use this site: https://twms.nmci.navy.mil/. For those contractors requiring initial training and do not have a CAC, contact the SPAWARSYSCEN Atlantic ISSM office at phone number (843)218-6152 or e-mail questions to ssc_lant_iam_office.fcm@navy.mil for additional instructions. Training can be taken at the IAM office or online at http://iase.disa.mil/Pages/index.aspx.

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

8.2.2.5 Contractor Check-in and Check-out Procedures

All SPAWARSYSCEN Atlantic contractor personnel requiring or possessing a Government badge and/or CAC for facility and/or IT access shall have a SPAWARSYSCEN Atlantic Government sponsor and be in compliance with the most current version of Contractor Check-in and Check-out Instruction and Forms as posted on the Command Operating Guide (COG) website. Throughout task order performance, the contractor shall provide necessary employee information and documentation for employees hired, transferred, and/or terminated in support of this task order within the required timeframe as cited in the Check-in and Check-out instructions. The contractor (FSO, if applicable) shall ensure all contractor employees whose services are no longer required on this task order return all applicable Government documents/badges to the appropriate Government representative. NOTE: If the contractor does not have access to the SPAWARSYSCEN Atlantic COG website, the contractor shall get all necessary instruction and forms from the COR.

8.2.3 Security Training

Applicable for unclassified and classified contracts, contractor personnel (including subcontractors) shall complete all required mandatory Government training in accordance with COMSPAWARSYSCOM Code 80330 mandatory training webpage: https://wiki.spawar.navy.mil/confluence/display/HQ/Employee+Mandatory+Training. Contractors without access to the SPAWAR webpage shall coordinate with the COR concerning mandatory training as listed on the training webpage.

8.2.3.1 The contractor shall be responsible for verifying applicable personnel receive all required training. At a minimum, the contractor (FSO, if applicable) shall track the following information: security clearance information; dates possessing CACs; issuance

and expiration dates for SPAWARSYSCEN Atlantic badge; Cybersecurity training; Privacy Act training; Personally Identifiable Information (PII) training; CSWF certifications; etc. The contractor shall report individual contractor personnel training status by completing and updating the monthly task order status report (TOSR) Staffing Plan (CDRL A001 of Exhibit A), Training tab. For Cybersecurity Workforce (CSWF) contractor personnel, all mandatory cybersecurity training and certifications shall be reported in the CSWF Report (CDRL A007).

8.2.3.2 The contractor shall educate employees on the procedures for the handling and production of classified material and documents, and other security measures as described in the PWS in accordance with DoD 5220.22-M.

8.3 OPERATIONS SECURITY (OPSEC) REQUIREMENTS

Security programs are oriented towards protection of classified information and material. Operations Security (OPSEC) is an operations function which involves the protection of any critical information – focusing on unclassified information that may be susceptible to adversary exploitation. Pursuant to DoDD 5205.02E and SPAWARINST 3432.1, SPAWARSYSCEN Atlantic's OPSEC program implements requirements in DoD 5205.02-M – OPSEC Program Manual and SPAWARSYSCENLANTINST 3070.1B. Note: OPSEC requirements are applicable when task order personnel have access to either classified information or unclassified Critical Program Information (CPI)/sensitive information.

8.3.1 Local and Internal OPSEC Requirement

Contractor personnel, including subcontractors if applicable, shall adhere to the OPSEC program policies and practices as cited in the SPAWARINST 3432.1 and existing local site OPSEC procedures. The contractor shall development their own internal OPSEC program specific to the task order and based on SPAWARSYSCEN Atlantic OPSEC requirements. At a minimum, the contractor's program shall identify the current SPAWARSYSCEN Atlantic site OPSEC Officer/Coordinator.

8.3.2 OPSEC Training

Contractor shall track and ensure applicable personnel receive initial and annual OPSEC awareness training in accordance with requirements outline in the Security Training, Para 8.2.3. OPSEC training requirements are applicable for personnel during their entire term supporting this SPAWARSYSCEN Atlantic task order.

8.3.3 SPAWARSYSCEN Atlantic OPSEC Program

Contractor shall participate in SPAWARSYSCEN Atlantic OPSEC program briefings and working meetings, and the contractor shall complete any required OPSEC survey or data call within the timeframe specified.

8.3.4 Classified Contracts

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

8.4 EFFECTIVE USE OF CONTROLS

The contractor shall screen all electronic deliverables or electronically provided information for malicious code using DoD approved anti-virus software prior to delivery to the Government. The contractor shall utilize appropriate controls (firewalls, password protection, encryption, digital certificates, etc.) at all times to protect task order related information processed, stored or transmitted on the contractor's and Government's computers/servers to ensure confidentiality, integrity, availability, authentication and non-repudiation. The contractor shall ensure provisions are in place that will safeguard all aspects of information operations pertaining to this task order in compliance with all applicable PWS references. In compliance with Para 6.4.2.1, the contractor shall ensure Data-at-Rest is required on all portable electronic devices including storage of all types. Encryption/digital signing of communications is required for authentication and non-repudiation. The contractor shall follow minimum standard in SECNAV M-5510.36 for classifying, safeguarding, transmitting, and destroying classified information.

9.0 GOVERNMENT FURNISHED INFORMATION (GFI)

Government Furnished Information (GFI) is Government owned intellectual property provided to the contractor for performance on a task order. For the purposes of this task order, GFI includes manuals, technical specifications, maps, building designs, schedules, drawings, test data, etc. Depending on information contained in a document, the contractor shall comply with additional controls (e.g., completion of a Non-Disclosure Agreements, etc.) for access and distribution.

GFI is not anticipated on this task order. Any processes, documentation, and controls will be available but are not considered GFI.

10.0 GOVERNMENT PROPERTY

As defined in FAR Part 45, Government property is property owned or leased by the Government which includes Government-furnished property (GFP) and Contractor-acquired property (CAP). Government property is material, equipment, special tooling, special test equipment, and real property.

GFP will not be provided and CAP is not anticipated on this task order.

10.1 GOVERNMENT-FURNISHED PROPERTY (GFP)

As defined in FAR Part 45, GFP is property in the possession of, or directly acquired by, the Government and subsequently furnished to the contractor for performance of a contract. GFP includes spares and property furnished for repair, maintenance, overhaul, or modification. GFP includes Government-furnished equipment (GFE), Government-furnished material (GFM), Special Tooling (ST) and Special Test Equipment (STE).

GFP will not be provided on this task order.

10.1.1 Government-Furnished Equipment

GFE will not be provided by the government. however NMCI computers and all DoD Enterprise required and utilized tools are not considered GFE and will be provided.

10.1.2 Government-Furnished Material

GFM will not be provided on this task order.

10.1.3 Special Test Equipment

STE will not be provided on this task order.

10.1.4 Special Tooling

ST will not be provided on this task order.

10.2 CONTRACTOR-ACQUIRED PROPERTY (CAP)

CAP is not anticipated on this task order.

11.0 TRAVEL

11.1 LOCATIONS

The contractor shall be prepared to travel to the following locations. Prior to any travel taken in support of this task order, the contractor shall obtain COR concurrence. Although estimated sites are listed, the contractor shall be prepared to travel to any of the following alternative sites. Travel to foreign countries outside of the continental United States (OCONUS) is required. The applicable countries are include the list below. Prior to travel, the contractor shall meet all necessary travel requirements for their company and personnel to support work in the noted foreign OCONUS sites.

# Trips	**# People**	**# Days/Nights**	**From (Location)**	**To (Location)**
4	2	5/4	CONTRACTOR FACILITIES	WASHINGTON, D.C.
4	2	5/4	CONTRACTOR FACILITIES	SAN DIEGO, CA
2	2	5/4	CONTRACTOR FACILITIES	HAWAII
2	2	5/4	CONTRACTOR FACILITIES	NEW ENGLAND
2	2	5/4	CONTRACTOR FACILITIES	SEATTLE/BANGOR, WA
2	2	5/4	CONTRACTOR FACILITIES	SAN DIEGO, CA
2	2	5/4	CONTRACTOR FACILITIES	PORTSMOUTH, VA
2	2	5/4	CONTRACTOR FACILITIES	CRANE, IN
2	2	6/5	CONTRACTOR FACILITIES	WASHINGTON, DC
2	2	6/5	CONTRACTOR FACILITIES	NORFOLK, VA
2	1	10/9	CONTRACTOR FACILITIES	BAHRAIN
2	1	10/9	CONTRACTOR FACILITIES	SOUTH KOREA (INCL CHINHAE
2	1	10/9	CONTRACTOR FACILITIES	SINGAPORE
2	1	10/9	CONTRACTOR FACILITIES	INDONESIA
2	1	10/9	CONTRACTOR FACILITIES	JEBIL ALI, UAE
2	1	10/9	CONTRACTOR FACILITIES	ROMANIA
2	1	10/9	CONTRACTOR FACILITIES	POLAND
2	1	10/9	CONTRACTOR FACILITIES	CUBA (INCL GUANTANAMO BAY)
2	1	10/9	CONTRACTOR FACILITIES	SPAIN (INCL ROTA)
2	1	10/9	CONTRACTOR FACILITIES	GREECE, CRETE, SOUDA BAY
2	1	10/9	CONTRACTOR FACILITIES	STUTTGART, GERMANY
2	1	10/9	CONTRACTOR FACILITIES	ITALY (INCL SIGONELLA AND NAPLES)

11.2 OCONUS TRAVEL REQUIREMENTS

Pursuant to SPAWARSYSCENLANTINST 12910.1B, DoDI 3020.41, and the latest DoD Foreign Clearance Guide requirements, the contractor shall travel outside the continental United States (OCONUS) sites to support deployed forces. SOFA requirements shall be reviewed and executed for contractors within areas requiring compliance.

11.2.1 General OCONUS Requirements

The contractor shall ensure compliance with applicable clauses and travel guide requirements prior to traveling to each of the specified travel locations. The contractor shall be responsible for knowing and understanding all travel requirements as identified by the applicable combatant command (CCMD) and country. The contractor shall be responsible for submitting applicable deployment forms and/or deployment packages (CDRL A006) to the COR or task order technical POC and SPAWARSYSCEN Atlantic Deployment Manager no later than 30 days prior to travel. For all OCONUS travel, the contractor shall submit an official OCONUS Travel Form (SPAWARSYSCENLANT 12990/12) and shall ensure all OCONUS travel has an approved Aircraft and Personnel Automated Clearance System (APACS) request. The task order COR will provide a blank travel form after task order award.

11.2.2 OCONUS Immunization Requirements

Pursuant to DoDI 6205.4, SPAWARSYSCENLANTINST 12910.1B, and any additional DON specific requirements, contractor employees who deploy to OCONUS locations both shore and afloat shall require up to date immunizations.

12.0 SAFETY ISSUES

12.1 Occupational Safety and Health Requirements

The contractor shall be responsible for ensuring the safety of all company employees, other working personnel, and Government property. The contractor is solely responsible for compliance with the Occupational Safety and Health Act (OSHA) (Public Law 91-596) and the resulting applicable standards, OSHA Standard 29 CFR 1910 (general), 1915 (shipboard/submarine) and 1926 (shore), and for the protection, safety and health of their employees and any subcontractors assigned to this task order. Without Government assistance, the contractor shall make certain that all safety requirements are met, safety equipment is provided, and safety procedures are documented as part of their quality management system. If performing within Government facilities, contractor shall immediately report any accidents involving Government or contractor personnel injuries or property/equipment damage to the Contracting Officer and COR. Additionally, the contractor is responsible for securing the scene and impounding evidence/wreckage until released by the COR or on-site Government representative.

12.2 SAFETY EQUIPMENT

The contractor shall provide their personnel with any safety equipment required to perform work under this task order and the equipment must be in satisfactory working order. Personal safety equipment includes items such as hard-hats, safety shoes, safety gloves, goggles, hearing protection, non-flammable clothing for hot work personnel, gas/oxygen detectors for confined spaces, face shields, and other types of safety equipment required to assure a safe work environment and compliance with applicable federal, state and local safety regulations.

12.3 SAFETY TRAINING

The contractor shall be responsible to train all personnel that require safety training. Specifically, where contractors are performing work at Navy shore installations, that requires entering manholes or underground services utility the contractor shall provide a qualified person as applicable in 29 CFR 1910 or 29 CFR 1926 or as recommended by the National Institute for Occupational Safety and Health (NIOSH) Criteria Document for Confined Spaces. Also, when contractors are required to scale a tower, all applicable personnel shall have Secondary Fall Protection and Prevention training.

13.0 SUBCONTRACTING REQUIREMENTS

13.1 APPROVED SUBCONTRACTORS

In accordance with FAR clause 52.244-2, prior to a prime contractor utilizing a subcontractor, the subcontractor is required to be approved by the Contracting Officer at the basic contract. As a team member, the subcontractor may be proposed on any upcoming task order competition but is not automatically approved for use on any pre-existing task order. After task order award, the prime contractor shall submit a written request to the Contracting Officer requesting approval to add any new subcontractors.

14.0 ACCEPTANCE PLAN

Inspection and acceptance is performed by the COR on all services, data, and non-data deliverables in accordance with the QASP, Attachment 1.

15.0 OTHER CONDITIONS/REQUIREMENTS

15.1 FUNDING ALLOCATION

This task order is funded with multiple appropriations with various Accounting Classification Reference Numbers (ACRNs) which may or may not cross multiple contract performance years. Depending on the services performed and the applicable timeframe, the contractor shall invoice cost in accordance with Section B, Section C, and Section G of the task order award. Unless otherwise advised, the contractor shall itemize all summary of work and financial information in the TOSR CDRL by each task order funding CLIN. The ability of the contractor to perform adequate billing and accounting will be reflected in the contractor's annual Government CPARS rating.

16.0 APPLICABLE DOCUMENTS (AND DEFINITIONS)

The contractor shall ensure all work accomplished utilizes the latest, relevant industry practices and standards when applicable unless otherwise indicated by text. In accordance with Defense Acquisition Policy, maximum utilization of non-Government standards will be made wherever practical.

16.1 REQUIRED DOCUMENTS

The contractor shall utilize the following mandatory documents in support of this task order. The documents referenced in this section list the minimum version dates; however, the contractor shall meet requirements for any referenced document including subsequent updates applicable at time the task order request for proposal is posted.

	Document Number	**Title**
a.	DoD 5200.2-R	DoD Regulation – Personnel Security Program dtd Jan 87 (and subsequent revisions)
b.	DoDM 5200.01	DoD Manual – Information Security Program Manual dtd 24 Feb 12
c.	DoDD 5205.02E	DoD Directive – Operations Security (OPSEC) Program dtd 20 Jun 12
d.	DoD 5205.02-M	DoD Manual – Operations Security (OPSEC) Program Manual dtd 3 Nov 08
e.	DoD 5220.22-M	DoD Manual – National Industrial Security Program Operating Manual (NISPOM) dtd 28 Feb 06
f.	DoDI 5220.22	DoD Instruction – National Industrial Security Program (NISP) dtd 18 Mar 11
g.	DoDI 6205.4	DoD Instruction – Immunization of Other Than U.S. Forces (OTUSF) for Biological Warfare Defense dtd 14 Apr 00
h.	DoDD 8140.01	DoD Directive – Cyberspace Workforce Management dtd 11 Aug 15
i.	DoDI 8500.01	DoD Instruction – Cybersecurity dtd 14 Mar 14

	Document Number	Title
j.	DoDI 8510.01	DoD Instruction – Risk Management Framework (RMF) for DoD Information Technology (IT) dtd 12 Mar 14
k.	DoD 8570.01-M	DoD Manual – Information Assurance Workforce Improvement Program dtd 19 Dec 05 with Change 3 dtd 24 Jan 12 and Change 4 dtd 10 Nov 15 (and subsequent revisions)
l.	DON CIO Memorandum	Acceptable Use of Department of the Navy Information Technology (IT) dtd 22 Feb 16
m.	SECNAV M-5239.2	Secretary of the Navy Manual – DON Information Assurance Workforce Management Manual dtd May 2009 (and subsequent revisions)
n.	SECNAV M-5510.30	Secretary of the Navy Manual – DoN Personnel Security Program dtd Jun 2006
o.	SECNAV M-5510.36	Secretary of the Navy Manual – DoN Information Security Program dtd Jun 2006
p.	SECNAVINST 4440.34	Secretary of the Navy Instruction – Implementation of Item Unique Identification within the DoN dtd 22 Dec 09
q.	SECNAVINST 5239.3B	Secretary of the Navy Instruction – DoN Information Assurance Policy dtd 17 Jun 09
r.	SECNAVINST 5239.20A	Secretary of the Navy Instruction – DON Cyberspace IT and Cybersecurity dtd 10 Feb 16
s.	SECNAVINST 5510.30	Secretary of the Navy Instruction – DoN Regulation – Personnel Security Program dtd 6 Oct 06
t.	SPAWARINST 3432.1	Space and Naval Warfare Instruction – Operations Security (OPSEC) Policy dtd 2 Feb 05
u.	SPAWARINST 4440.12A	Space and Naval Warfare Instruction – Management of Operating Materials and Supplies (OM&S), Government Furnished Property (GFP), and Inventory
v.	SPAWARINST 5721.1B	Space and Naval Warfare Instruction – Section 508 Implementation Policy dtd 17 Nov 09
w.	SPAWARSYSCENLANTINST 3070.1B	Space and Naval Warfare Systems Center Atlantic Instruction – Operations Security Policy dtd 20 Jan 17
x.	SPAWARSYSCENLANTINST 12910.1B	Space and Naval Warfare Systems Center Atlantic Instruction – Deployment of Government and Contractor Personnel Outside the Continental Unlisted States dtd 23 Aug 16
y.	Navy Telecommunications Directive (NTD 10-11)	System Authorization Access Request (SAAR) - Navy
z.	Privacy Act of 1974	United States federal law, Pub.L. 93–579, 88 Stat. 1896, dtd December 31, 1974, 5 U.S.C. § 552a

16.2 GUIDANCE DOCUMENTS

The contractor shall utilize the following guidance documents in support of this task order. The documents referenced in this section list the minimum version dates; however, the document's effective date of issue is the task order's request for proposal issue date.

	Document Number	Title
a.	MIL-HDBK-61A	Configuration Management
b.	MIL-STD-130N	DoD Standard Practice – Identification Marking of US Military Property
c.	MIL-STD-881C	Work Breakdown Structure for Defense Materiel Items
d.	MIL-STD-1916	DoD Test Method Standard – DoD Preferred Methods for Acceptance Of Product
e.	DoDM 1000.13-V1	DoD Manual – DoD Identification Cards: ID card Life-Cycle, Volume 1, dtd 23 Jan 14

	Document Number	Title
f.	DoDI 3020.41	DoD Instruction – Operational Contract Support (OCS) dtd 20 Dec 10
g.	DoDI 4161.02	DoD Instruction – Accountability and Management of Government Contract Property dtd 27 Apr 12
h.	NAVSEA TS9090-310F	NAVSEA Technical Specification 9090-310 dtd 12 Feb 15 (and subsequent revisions)
i.	ISO 9001 (ANSI/ASQ Q9001)	International Organization for Standardization (American National Standard Institute/American Society for Quality) – Quality Management Systems, Requirements
j.	ISO/IEC 12207	International Organization for Standardization/ International Electrotechnical Commission: Systems and Software Engineering – Software Life Cycle Processes
k.	ISO/IEC/IEEE 15288	International Organization for Standardization/ International Electrotechnical Commission: Systems and Software Engineering – System Life Cycle Processes
l.	ASTM Std E-2135-06	American Section of the International Association for Testing Materials, Standard
m.	IEEE Std 12207-2008	Institute of Electrical and Electronics Engineers – Systems and Software Engineering, Software Life Cycle Processes
n.	EIA-748C	Electronic Industries Alliance Standard – Earned Value Management (EVM) Systems, March 2013
o.	HSPD-12	Homeland Security Presidential Directive – Policy for a Common Identification Standard for Federal Employees and Contractors dtd 27 Aug 04
p.	FIPS PUB 201-2	Federal Information Processing Standards Publication 201-2 – Personal Identity Verification (PIV) of Federal Employees and Contractors, August 2013
q.	Form I-9, OMB No. 115-0136	US Department of Justice, Immigration and Naturalization Services, Form I-9, OMB No. 115-0136 – Employment Eligibility Verification
r.	N/A	NAVSEA Standard Items (NSI) – http://www.navsea.navy.mil/
s.	N/A	SPAWARSYSCEN Atlantic Contractor Check-in portal – https://wiki.spawar.navy.mil/confluence/display/SSCACOG/Contractor+Checkin
t.	N/A	COMSPAWARSYSCOM Code 80330 mandatory training webpage – https://wiki.spawar.navy.mil/confluence/display/HQ/Employee+Mandatory+Training
u.	N/A	DoD Foreign Clearance Guide – https://www.fcg.pentagon.mil/fcg.cfm

16.3 SOURCE OF DOCUMENTS

The contractor shall obtain all applicable documents necessary for performance on this task order. Many documents are available from online sources. Specifications and commercial/industrial documents may be obtained from the following sources:

Copies of Federal Specifications may be obtained from General Services Administration Offices in Washington, DC, Seattle, San Francisco, Denver, Kansas City, MO., Chicago, Atlanta, New York, Boston, Dallas and Los Angeles.

Copies of military specifications may be obtained from the Commanding Officer, Naval Supply Depot, 3801 Tabor Avenue, Philadelphia, PA 19120-5099. Application for copies of other Military Documents should be addressed to Commanding Officer, Naval Publications and Forms Center, 5801 Tabor Ave., Philadelphia, PA 19120-5099.

All other commercial and industrial documents can be obtained through the respective organization's website.

CLAUSES INCORPORATED BY FULL TEXT

C-TXT-11 PERSONNEL QUALIFICATIONS (MINIMUM)

(a) Personnel assigned to or utilized by the Contractor in the performance of this task order shall, as a minimum, meet the experience, educational, CSFW designation, or other background requirements set forth below and shall be fully capable of performing in an efficient, reliable, and professional manner. If the offeror does not identify the labor categories listed below by the same specific title, then a cross-reference list should be provided in the offeror's proposal identifying the difference.

(b) The Government will review resumes of contractor personnel proposed to be assigned, and if personnel not currently in the employ of Contractor, a written agreement from potential employee to work will be part of the technical proposal.

(c) If the Ordering Officer questions the qualifications or competence of any persons performing under this task order, the burden of proof to sustain that the persons is qualified as prescribed herein shall be upon the contractor.

(d) The Contractor must have personnel, organization, and administrative control necessary to ensure that the services performed meet all requirements specified in delivery orders. The work history of each Contractor employee shall contain experience directly related to the tasks and functions to be assigned. The Ordering Officer reserves the right to determine if a given work history contains necessary and sufficiently detailed, related experience to reasonably ensure the ability for effective and efficient performance.

Program Manager

Education: Bachelor's degree in Engineering, Physical Sciences, Mathematics, Management Information Systems, or Business.

Experience: Fifteen (15) years of technical experience, to include: Equipment Support, System Support, and Programmatic Support. Eight (8) years of Program Management experience, to include: Technology Assessments, Systems Design, Systems Analysis, Programmatic Support, Acquisition Planning, and Budget Planning. Five (5) years as manager. Note: Experience may be concurrent. Knowledge of Federal Acquisition Regulation (FAR) and DoD procurement policies and procedures.

Engineer/Scientist 3

Education: Bachelor's degree in Engineering, Physical Sciences, Mathematics, Management Information Systems, or Business.

Experience: Six (6) years of experience, to include: Systems Analysis, Systems Architecture, Systems/Equipment Support, Test and Evaluation, and Logistics support of C4ISR requirements. Three (3) years of technical experience. Note: Experience may be concurrent.

Engineer/Scientist 4

Education: Bachelor's degree in Engineering, Physical Sciences, Mathematics, Management Information Systems, or Business.

Experience: Ten (10) years of experience, to include: Technology Analysis and Assessment, Design Definition, Development of Systems Specification, Systems Analysis, Systems Architecture, Systems/Equipment Integration, Test & Evaluation Criteria, and Logistics support of C4ISR requirements. Five (5) years of technical experience. Note: Experience may be concurrent.

Engineer/Scientist 5

Education: Bachelor's degree in Engineering, Physical Sciences, Mathematics, Management Information Systems, or Business.

Experience: Fifteen (15) years of experience, to include: Technology Analysis and Assessment, Design Definition, Development of Systems Specification, Systems Analysis, Systems Architecture, Systems/Equipment Integration, Test & Evaluation Criteria, and Logistics support of C4ISR requirements. Note: Experience may be concurrent.

Management Analyst 3

Education: Bachelor's degree in Engineering, Physical Sciences, Mathematics, Management Information Systems, Business or other related field.

Experience: Six (6) years of Contract Management experience, to include: Development of Program Acquisition Documentation, Data Collection and Analysis, Development of Cost Estimates, and Development of Program Status Reports. Knowledge of Federal Acquisition Regulation (FAR) and DoD procurement policies and procedures.

Subject Matter Expert (SME) 1

Education: Technical Training in Systems Requirements, Operational Requirements, Test & Evaluation, and Training.

Experience: Eight (8) years of hands-on experience, to include three (3) of the following four (4) areas: Systems Requirements, Operational Requirements, Test & Evaluation, and Training.

Subject Matter Expert (SME) 3

Education: Technical Training in Systems Requirements, Operational Requirements, Test & Evaluation, and Training.

Experience: Twelve (12) years of hands-on experience, to include three (3) of the following four (4) areas: Systems Requirements, Operational Requirements, Test & Evaluation, and Training.

Subject Matter Expert (SME) 4

Education: Technical Training in Systems Requirements, Operational Requirements, Test & Evaluation, and Training.

Experience: Fourteen (14) years of hands-on experience, to include three (3) of the following four (4) areas: Systems Requirements, Operational Requirements, Test & Evaluation, and Training.

Subject Matter Expert (SME) 5

Education: Technical Training in Systems Requirements, Operational Requirements, Test & Evaluation, and Training.

Experience: Eighteen (18) years of hands-on experience, to include three (3) of the following four (4) areas: Systems Requirements, Operational Requirements, Test & Evaluation, and Training.

SECTION D PACKAGING AND MARKING

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

SECTION E INSPECTION AND ACCEPTANCE

Inspection and acceptance of the services to be furnished hereunder shall be made at destination by the Task Order Manager or his/her duly authorized representative.

CLAUSES INCORPORATED BY REFERENCE

52.246-3	Inspection of Supplies Cost-Reimbursement	MAY 2001
52.246-5	Inspection Of Services Cost-Reimbursement	APR 1984

SECTION F DELIVERABLES OR PERFORMANCE

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

7001	5/23/2019 - 5/22/2020
7002	5/23/2019 - 5/22/2020
9001	5/23/2019 - 5/22/2020
9002	5/23/2019 - 5/22/2020

CLIN - DELIVERIES OR PERFORMANCE

The periods of performance are as follows:

Base Year: Date of award through one year thereafter.

Option Years: If exercised, date of option exercised through twelve months thereafter.

Services to be performed hereunder will be provided at Government and Contractor facilities in accordance with Section C.

The above periods 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 task order clause at FAR 52.217-9 "Option to Extend the Term of the Contract."

Services to be performed hereunder will be provided at the locations identified in Section C.

CLAUSES INCORPORATED BY REFERENCE

52.242-15 - Stop-Work Order, AUG 1989

52.242-15 Alt I - Stop-Work Order (Aug 1989) - Alternate I

SECTION G CONTRACT ADMINISTRATION DATA

The SPAWAR Atlantic Ombudsman is Robin Rourk, (843) 218-5115.

252.204-0012 (Other) Payment Clause

CLINs have multiple funding from multiple customers. Payment cannot be made using any of the PGI 204.7108 clauses due to one customer's funds would be paying for another customer's work. Use PGI 204.7108 (d)(12) Other and pay from the ACRNs cited on the invoice. Government advises contractor on ACRNS to invoice.

G-TXT-07 PAYMENT INSTRUCTION (PGI 204.7108)

The payment office shall allocate and record the amounts paid to the accounting classification citations in the task order using the table below based on the type of payment request submitted (see DFARS 252.232-7006) and the type of effort: PGI 204.7108(d)(12)

252.204-7006 BILLING INSTRUCTIONS (OCT 2005)

When submitting a request for payment, the Contractor shall—

a. Identify the contract line item(s) on the payment request that reasonably reflect contract work performance; and

b. Separately identify a payment amount for each contract line item included in the payment request.

252.232-7006 WIDE AREA WORKFLOW PAYMENT INSTRUCTIONS (MAY 2013)

(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 System for Award Management 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.

(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

(Contracting Officer: Insert applicable document type(s).
Note: If a "Combo" document type is identified but not supportable by the Contractor's business systems, an "Invoice" (stand-alone) and "Receiving Report" (stand-alone) document type may be used instead.)

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

N65236

(Contracting Officer: Insert inspection and acceptance locations or "Not applicable.")

(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	N65236
Admin DoDAAC	N65236
Inspect By DoDAAC	N65236
Ship To Code	N65236
Ship From Code	N/A
Mark For Code	N65236
Service Approver (DoDAAC)	N65236
Service Acceptor (DoDAAC)	N/A
Accept at Other DoDAAC	N/A
LPO DoDAAC	N65236
DCAA Auditor DoDAAC	HAA47B
Other DoDAAC(s)	N/A

** To be inserted at award*

(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 e-mail address identified below in the "Send Additional Email Notifications" field of WAWF once a document is submitted in the system.

scott.h.bell@navy.mil, Role: COR

(Contracting Officer: Insert applicable email addresses or "Not applicable.")

(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.

Ms. Laverne Brown, E-Mail: Laverne.Brown@navy.mil
(Contracting Officer: Insert applicable information or "Not applicable.")

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

(End of clause)

G-TXT-01 Designation of Contracting Officer's Representative

(a) The Contracting Officer hereby appoints the following individual as Contracting Officer's Representative(s) (COR) for this contract/order:

CONTRACTING OFFICER REPRESENTATIVE

Name: Scott Bell

Code: 59210

Address: P.O. Box 190022

North Charleston, SC 29419-9022

Phone Number: 843-218-6241

E-mail: scott.h.bell@navy.mil

(b) It is emphasized that only the Contracting Officer has the authority to modify the terms of the contract, therefore, in no event will any understanding agreement, modification, change order, or other matter deviating from the terms of the basic contract between the Contractor and any other person be effective or binding on the Government. When/If, in the opinion of the Contractor, an effort outside the existing scope of the contract is requested, the Contractor shall promptly notify the PCO in writing. No action shall be taken by the Contractor unless the Procuring Contracting Officer (PCO) or the Administrative Contracting Officer (ACO) has issued a contractual change.

(End of text)

G-TXT-04 TYPE OF CONTRACT

This is a **Cost-Plus-Fixed-Fee (CPFF), Level of Effort, and Cost-Reimbursement** task order.

(End of text)

5252.232-9206 SEGREGATION OF COSTS (DEC 2003)

(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 contract 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.

(c) Except when payment requests are submitted electronically as specified in the clause at DFARS 252.232-7003, Electronic Submission of Payment Requests and Receiving Reports, one copy of each invoice or voucher will be provided, at the time of submission to DCAA:

(1) to the Contracting Officer's Representative

Accounting Data

SLINID	PR Number	Amount
700101	13006773820003	
LLA :		
AA 1791804 52CY 257 00520 0 056521 2D ITW1WG 05219RC0022Q		
2410a Authority Invoked		
700201	13006773820005	
LLA :		
AA 1791804 52CY 257 00520 0 056521 2D ITW1WG 05219RC0022Q		
2410a Authority Invoked		
900101	13006773820004	
LLA :		
AA 1791804 52CY 257 00520 0 056521 2D ITW1WG 05219RC0012Q		
2410a Authority Invoked		
900201	13006773820006	
LLA :		
AA 1791804 52CY 257 00520 0 056521 2D ITW1WG 05219RC0012Q		
2410a Authority Invoked		

BASE Funding
Cumulative Funding
MOD P00001 Funding
Cumulative Funding
MOD P00002 Funding
Cumulative Funding

SECTION H SPECIAL CONTRACT REQUIREMENTS

H-TXT-01 CONTRACTOR PICTURE BADGE

(a) A contractor picture badge may be issued to contractor personnel by the http://www.public.navy.mil/spawar/Atlantic/Documents/ContactUs/SSCAtlanticVisitorGuide-Charleston.pdf 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 **[N/A]** 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 http://www.public.navy.mil/spawar/Atlantic/Documents/ContactUs/SSCAtlanticVisitorGuide-Charleston.pdf a list of all unreturned badges with a written explanation of any missing badges.

(End of text)

H-TXT-07 EMPLOYMENT OF NAVY PERSONNEL RESTRICTED

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.

(End of text)

5252.216-9122 LEVEL OF EFFORT (DEC 2000)

(a) The Contractor agrees to provide the total level of effort specified in the next sentence in performance of the work described in Sections B and C of this contract. The total level of effort for the performance of this contract shall be **560,000** total man-hours of direct labor, including subcontractor direct labor for those subcontractors specifically identified in the Contractor's proposal as having hours included in the proposed level of effort.

(b) Of the total man-hours of direct labor set forth above, it is estimated that 0 man-hours are uncompensated effort.

Uncompensated effort is defined as hours provided by personnel in excess of 40 hours per week without additional compensation for such excess work. All other effort is defined as compensated effort. If no effort is indicated in the first sentence of this paragraph, uncompensated effort performed by the Contractor shall not be counted in fulfillment of the level of effort obligations under this task order.

(c) Effort performed in fulfilling the total level of effort obligations specified above shall only include effort performed in direct support of this contract and shall not include time and effort expended on such things as (local travel to and from an employee's usual work location), uncompensated effort while on travel status, truncated lunch periods, work (actual or inferred) at an employee's residence or other non-work locations (except as provided in paragraph (j) below), or other time and effort which does not have a specific and direct contribution to the tasks described in Sections B and C.

(d) The level of effort for this contract shall be expended at an average rate of approximately **2,154** hours per week. It is understood and agreed that the rate of man-hours per month may fluctuate in pursuit of the technical

objective, provided such fluctuation does not result in the use of the total man-hours of effort prior to the expiration of the term hereof, except as provided in the following paragraph.

(e) If, during the term hereof, the Contractor finds it necessary to accelerate the expenditure of direct labor to such an extent that the total man-hours of effort specified above would be used prior to the expiration of the term, the Contractor shall notify the Contracting Officer in writing setting forth the acceleration required, the probable benefits which would result, and an offer to undertake the acceleration at no increase in the estimated cost or fee together with an offer, setting forth a proposed level of effort, cost breakdown, and proposed fee, for continuation of the work until expiration of the term hereof. The offer shall provide that the work proposed will be subject to the terms and conditions of this contract and any additions or changes required by then current law, regulations, or directives, and that the offer, with a written notice of acceptance by the Contracting Officer, shall constitute a binding contract. The Contractor shall not accelerate any effort until receipt of such written approval by the Contracting Officer. Any agreement to accelerate will be formalized by contract modification.

(f) The Contracting Officer may, by written order, direct the Contractor to accelerate the expenditure of direct labor such that the total man-hours of effort specified in paragraph (a) above would be used prior to the expiration of the term. This order shall specify the acceleration required and the resulting revised term. The Contractor shall acknowledge this order within five days of receipt.

(g) If the total level of effort specified in paragraph (a) above is not provided by the Contractor during the period of this contract, the Contracting Officer, at its sole discretion, shall either (i) reduce the fee of this contract as follows:

$$\text{Fee Reduction} = \text{Fee} \left(\frac{\text{Required LOE - Expended LOE}}{\text{Required LOE}} \right)$$

or (ii) subject to the provisions of the clause of this contract entitled "LIMITATION OF COST" (FAR 52.232-20) or "LIMITATION OF COST (FACILITIES)" (FAR 52.232-21), as applicable, require the Contractor to continue to perform the work until the total number of man-hours of direct labor specified in paragraph (a) above shall have been expended, at no increase in the fee of this contract.

(h) The Contractor shall provide and maintain an accounting system, acceptable to the Administrative Contracting Officer and the Defense Contract Audit Agency (DCAA), which collects costs incurred and effort (compensated and uncompensated, if any) provided in fulfillment of the level of effort obligations of this contract. The Contractor shall indicate on each invoice the total level of effort claimed during the period covered by the invoice, separately identifying compensated effort and uncompensated effort, if any.

(i) Within 45 days after completion of the work under each separately identified period of performance hereunder, the Contractor shall submit the following information in writing to the Contracting Officer with copies to the cognizant Contract Administration Office and to the DCAA office to which vouchers are submitted: (1) the total number of man-hours of direct labor expended during the applicable period; (2) a breakdown of this total showing the number of man-hours expended in each direct labor classification and associated direct and indirect costs; (3) a breakdown of other costs incurred; and (4) the Contractor's estimate of the total allowable cost incurred under the contract for the period. Within 45 days after completion of the work under the contract, the Contractor shall submit, in addition, in the case of a cost underrun; (5) the amount by which the estimated cost of this contract may be reduced to recover excess funds and, in the case of an underrun in hours specified as the total level of effort; and (6) a calculation of the appropriate fee reduction in accordance with this clause. All submissions shall include subcontractor information.

(j) Unless the Contracting Officer determines that alternative worksite arrangements are detrimental to contract performance, the Contractor may perform up to 10% of the hours at an alternative worksite, provided the Contractor has a company-approved alternative worksite plan. The primary worksite is the traditional “main office” worksite. An alternative worksite means an employee’s residence or a telecommuting center. A telecommuting center is a geographically convenient office setting as an alternative to an employee’s main office.

The Government reserves the right to review the Contractor's alternative worksite plan. In the event performance becomes unacceptable, the Contractor will be prohibited from counting the hours performed at the alternative worksite in fulfilling the total level of effort obligations of the contract. Regardless of work location, all contract terms and conditions, including security requirements and labor laws, remain in effect. The Government shall not incur any additional cost nor provide additional equipment for contract performance as a result of the Contractor's election to implement an alternative worksite plan.

(k) Notwithstanding any of the provisions in the above paragraphs, the Contractor may furnish man-hours up to five percent in excess of the total man-hours specified in paragraph (a) above, provided that the additional effort is furnished within the term hereof, and provided further that no increase in the estimated cost or fee is required.

H-TXT-16 LIMITED RELEASE OF CONTRACTOR CONFIDENTIAL BUSINESS INFORMATION

(a) Definition.

"Confidential Business Information," (Information) as used in this text, 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)(15), 252.227-7015(a)(5), and 252.227-7018(a)(20). Similarly, Information does not include computer software/computer software documentation, as those terms are defined in DFARS 252.227-7014(a)(4) and -7014(a)(5) and 252.227-7018(a)(4) and -7018(a)(5).

(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 task order. 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 text.

(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 text.

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

(End of text)

H-TXT-23 REIMBURSEMENT OF TRAVEL COSTS

(a) Contractor Request and Government Approval of Travel

The estimated travel requirements under this task order are listed in paragraph 11.1 of the Performance Work Statement. Any travel under this task order must be specifically requested in writing, by the contractor prior to incurring any travel costs. 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 task order. 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 task order, 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.

(vi) "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

(End of text)

H-TXT-25 CONTRACTOR IDENTIFICATION

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

(b) Contractor personnel and their subcontractors must identify themselves as contractors or subcontractors during meetings, telephone conversations, in electronic messages, or correspondence related to this contract.

(c) Contractor-occupied facilities (on Department of the Navy or other Government installations) such as offices, separate rooms, or cubicles must be clearly identified with Contractor supplied signs, name plates or other identification, showing that these are work areas for Contractor or subcontractor personnel.

(End of text)

H-TXT-26 REQUIRED INFORMATION ASSURANCE AND PERSONNEL SECURITY REQUIREMENTS FOR ACCESSING GOVERNMENT INFORMATION SYSTEMS AND NONPUBLIC INFORMATION

Definition. As used in this text, "sensitive information" includes:

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;

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 2101-2107);

Information properly marked as “business confidential,” “proprietary,” “procurement sensitive,” “source selection sensitive,” or other similar markings;

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

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.

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—

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;

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;

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.

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;

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.

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.

The requirements of this text 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.

Subcontracts. The Contractor shall insert paragraphs (a) through (f) of this text 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.

(End of text)

5252.242-9518 CONTRACTOR PERFORMANCE ASSESSMENT REPORTING SYSTEM (CPARS) (NAVAIR)(FEB 2009)

a. The Contractor Performance Assessment Reporting System (CPARS) has been established to collect past p erformance information on defense contractors as required by FAR 42.1502 (Class Deviation 2013-O0018).T he frequency and type of CPARS reports (initial, intermediate, final, out-of-
cycle, and addendum) shall be as required in the CPARS Policy Guide that is available at

http://www.cpars.csd.disa.mil/cparsmain.htm

b. For orders placed against contracts and agreements the contractor's performance shall be assessed on an o rder- by-order basis [_X] or total contract/agreement basis [ ].

NAVSEA 5252.232-9104 ALLOTMENT OF FUNDS (JAN 2008)

(a) This task order is incrementally funded with respect to both cost and fee. The amount(s) presently availa ble and allotted to this task order for payment of fee for incrementally funded contract line item number/co ntract sub line item number (CLIN/SLIN), subject to the clause entitled "FIXED FEE" (FAR 52.216-8) or "I NCENTIVE FEE" (FAR 52.216-10), as appropriate, is specified below. The amount(s) presently available an d allotted to this task order for payment of cost for incrementally funded CLINs/SLINs is set forth below. As provided in the clause of this contract entitled "LIMITATION OF FUNDS" (FAR 52.232-22), the CLINs/SLI Ns covered thereby, and the period of performance for which it is estimated the allotted amount(s) will cover are as follows:

Item(s)	Allotted to Cost	Allotted to Fee	Estimated Period of Performance
7001			5/23/2019 - 5/22/2020
7002			5/23/2019 - 5/22/2020
7101			*
7102			*
7201			*
7202			*
7301			*
7302			*
7401			*
7402			*
9001			5/23/2019 - 5/22/2020
9002			5/23/2019 - 5/22/2020
9101			*

9102	*
9201	*
9202	*
9301	*
9302	*
9401	*
9402	*

* Will be inserted upon option exercise

(b) The parties contemplate that the Government will allot additional amounts to this task order from time to time for the incrementally funded CLINs/SLINs by unilateral task order modification, and any such modification shall state separately the amount(s) allotted for cost, the amount(s) allotted for fee, the CLINs/SLINs covered thereby, and the period of performance which the amount(s) are expected to cover.

(c) CLINs/SLINs
_____ are fully funded and performance under these CLINs/SLINs is subject to the clause of the basic contract entitled "LIMITATION OF COST" (FAR 52.232-20).

(d) The Contractor shall segregate costs for the performance of incrementally funded CLINs/SLINs from the costs of performance of fully funded CLINs/SLINs.

SECTION I CONTRACT CLAUSES

FAR CLAUSES INCORPORATED BY REFERENCE:

52.251-1 GOVERNMENT SUPPLY SOURCES (APR 2012)

252.251-7000 ORDERING FROM GOVERNMENT SUPPLY SOURCES (AUG 2012)

52.224-2 PRIVACY ACT (APR 1984)

252.229-7005 TAX EXEMPTIONS (SPAIN) (MAR 2012)

FAR CLAUSES INCORPORATED BY FULL TEXT:

52.204-23-Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Jul 2018)

Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities.

As prescribed in 4.2004, insert the following clause:

Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Jul 2018)

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

Covered article means any hardware, software, or service that--

(1) Is developed or provided by a covered entity;

(2) Includes any hardware, software, or service developed or provided in whole or in part by a covered entity; or

(3) Contains components using any hardware or software developed

in whole or in part by a covered entity.

Covered entity means--

(1) Kaspersky Lab;

(2) Any successor entity to Kaspersky Lab;

(3) Any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or

(4) Any entity of which Kaspersky Lab has a majority ownership.

(b) Prohibition. Section 1634 of Division A of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115-91) prohibits Government use of any covered article. The Contractor is prohibited from--

(1) Providing any covered article that the Government will use

on or after October 1, 2018; and

(2) Using any covered article on or after October 1, 2018, in the development of data or deliverables first produced in the performance of the contract.

(c) Reporting requirement. (1) In the event the Contractor identifies a covered article provided to the Government during contract performance, or the Contractor is notified of such by a subcontractor at any tier or any other source, the Contractor shall report, in writing, to the Contracting Officer or, in the case of the Department of Defense, to the website at https://dibnet.dod.mil/. For indefinite delivery contracts, the Contractor shall report to the Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at https://dibnet.dod.mil/.

(2) The Contractor shall report the following information pursuant to paragraph (c)(1) of this clause:

(i) Within 1 business day from the date of such identification or notification: The contract number; the order number(s), if applicable; supplier name; brand; model number (Original Equipment Manufacturer (OEM) number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the report pursuant to paragraph (c)(1) of this clause: Any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of a covered article, any reasons that led to the use or submission of the covered article, and any additional efforts that will be incorporated to prevent future use or submission of covered articles.

(d) Subcontracts. The Contractor shall insert the substance of this clause, including this paragraph (d), in all subcontracts, including subcontracts for the acquisition of commercial items.

(End of clause)

52.217-9 -- OPTION TO EXTEND THE TERM OF THE CONTRACT. (MAR 2000)

(a) The Government may extend the term of this task order by written notice to the Contractor within 30 days prior to completion of the base period; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 days before the task order expires. The preliminary notice does not commit the Government to an extension.

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

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

52.219-27 -- Notice of Service-Disabled Veteran-Owned Small Business Set-Aside (Nov 2011)

(a) *Definition.* “Service-disabled veteran-owned small business concern”--

(1) Means a small business concern--

(i) Not less than 51 percent of which is owned by one or more service-disabled veterans or, in the case of any publicly owned business, not less than 51 percent of the stock of which is owned by one or more service-disabled veterans; and

(ii) The management and daily business operations of which are controlled by one or more service-disabled

veterans or, in the case of a service-disabled veteran with permanent and severe disability, the spouse or permanent caregiver of such veteran.

(2) “Service-disabled veteran” means a veteran, as defined in 38 U.S.C. 101(2), with a disability that is service-connected, as defined in 38 U.S.C. 101(16).

(b) *Applicability*. This clause applies only to--

(1) Contracts that have been set aside or reserved for service-disabled veteran-owned small business concerns;

(2) Part or parts of a multiple-award contract that have been set aside for service-disabled veteran-owned small business concerns; and

(3) Orders set aside for service-disabled veteran-owned small business concerns under multiple-award contracts as described in 8.405-5 and 16.505(b)(2)(i)(F).

(c) *General*.

(1) Offers are solicited only from service-disabled veteran-owned small business concerns. Offers received from concerns that are not service-disabled veteran-owned small business concerns shall not be considered.

(2) Any award resulting from this solicitation will be made to a service-disabled veteran-owned small business concern.

(d) *Agreement*. A service-disabled veteran-owned small business concern agrees that in the performance of the contract, in the case of a contract for--

(1) Services (except construction), at least 50 percent of the cost of personnel for contract performance will be spent for employees of the concern or employees of other service-disabled veteran-owned small business concerns;

(2) Supplies (other than acquisition from a nonmanufacturer of the supplies), at least 50 percent of the cost of manufacturing, excluding the cost of materials, will be performed by the concern or other service-disabled veteran-owned small business concerns;

(3) General construction, at least 15 percent of the cost of the contract performance incurred for personnel will be spent on the concern's employees or the employees of other service-disabled veteran-owned small business concerns; or

(4) Construction by special trade contractors, at least 25 percent of the cost of the contract performance incurred for personnel will be spent on the concern's employees or the employees of other service-disabled veteran-owned small business concerns.

(e) A joint venture may be considered a service-disabled veteran owned small business concern if--

(1) At least one member of the joint venture is a service-disabled veteran-owned small business concern, and makes the following representations: That it is a service-disabled veteran-owned small business concern, and that it is a small business concern under the North American Industry Classification Systems (NAICS) code assigned to the procurement;

(2) Each other concern is small under the size standard corresponding to the NAICS code assigned to the procurement; and

(3) The joint venture meets the requirements of paragraph 7 of the explanation of Affiliates in 19.101 of the Federal Acquisition Regulation.

(4) The joint venture meets the requirements of 13 CFR 125.15(b)

(f) Any service-disabled veteran-owned small business concern (nonmanufacturer) must meet the requirements in

19.102(f) of the Federal Acquisition Regulation to receive a benefit under this program.

(End of Clause)

SECTION J LIST OF ATTACHMENTS

PWS Exhibit A - CDRLs - DD Form 1423

PWS Attachment 1 - QASP

PWS_Attachment_2_DD254