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)*
P00001	06-Feb-2019	1300766851	N/A

6. ISSUED BY	CODE	7. ADMINISTERED BY *(If other than Item 6)*	CODE
SPAWAR-Systems Center Lant (CHRL) P.O. BOX 190022 North Charleston SC 29419-9022 [redacted]	N65236	DCMA ATLANTA 2300 LAKE PARK DRIVE, SUITE 300 SMYRNA GA 30080	S1103A SCD: C

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

Product Data Integration Technologies, Inc dba Modulant
4130 Faber Place Drive, Suite 204
North Charleston SC 29405-8503

CAGE CODE	FACILITY CODE
1WAW1	

[X]

9A. AMENDMENT OF SOLICITATION NO.

9B. DATED *(SEE ITEM 11)*

10A. MODIFICATION OF CONTRACT/ORDER NO.
N00178-15-D-8374 / N6523618F3054

10B. DATED *(SEE ITEM 13)*
27-Mar-2018

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)*

SEE SECTION G

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.
[ ]	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).
[X]	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF: 43.103(a) Mutual Agreement FAR 52.232-22 Limitation of Funds
[ ]	D. OTHER *(Specify type of modification and authority)*

E. IMPORTANT: Contractor [ ] is not, [X] is required to sign this document and return 1 copies to the issuing office.

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

SEE PAGE 2

15A. NAME AND TITLE OF SIGNER *(Type or print)*		16A. NAME AND TITLE OF CONTRACTING OFFICER *(Type or print)*	
[redacted]		[redacted]	
15B. CONTRACTOR/OFFEROR	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA	16C. DATE SIGNED
[redacted] *(Signature of person authorized to sign)*	12-Feb-2019	BY [redacted] *(Signature of Contracting Officer)*	13-Feb-2019

GENERAL INFORMATION

The purpose of this modification is to Exercise Option Year 1, CLINs 7100, 7101 and 9100 for the Period 27 March 2019 through 26 March 2020; realign [redacted] ceiling from CLIN 7101 to CLINs 7100 [redacted] and 9100 $[redacted], and to incrementally fund CLIN 7101 in the amount of [redacted] and 9100 in the amount of [redacted]. Accordingly, said Task Order is modified as follows: A conformed copy of this Task Order is attached to this modification for informational purposes only.

NOTE: CLINS 7100, 7101, and 9100 will not be available until 27 March 2019.

The Line of Accounting information is hereby changed as follows:

The total amount of funds obligated to the task is hereby increased from [redacted] by [redacted] to [redacted].

CLIN/SLIN	Type Of Fund	From ($)	By ($)	To ($)
710001	WCF	0.00	[redacted]	[redacted]
910001	WCF	0.00	[redacted]	[redacted]

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

CLIN/SLIN	From ($)	By ($)	To ($)
7100	0.00	[redacted]	[redacted]
7101	0.00	[redacted]	[redacted]
9100	0.00	[redacted]	[redacted]

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
7000	D308	PWS/Subtask Para#6.1 (WCF)	1.0	LO	[redacted]	[redacted]	[redacted]
700001	D308	ACRN: AA PR#: 1300646091 NWA: 300000075062 0020 DOC: NWCF Overhead Funds Expiration: 09/30/2018 (WCF)					
7001	D308	PWS/Subtask Para# 6.2 (Fund Type - TBD)	1.0	LO	[redacted]	[redacted]	[redacted]

For Cost Type / NSP Items

Item	PSC	Supplies/Services	Qty	Unit	Est. Cost	Fixed Fee	CPFF
7003		Not Separately Priced - CDRL's	1.0	LO			NSP

For Cost Type Items:

Item	PSC	Supplies/Services	Qty	Unit	Est. Cost	Fixed Fee	CPFF
7100	D308	PWS/Subtask Para# 6.1 (Fund Type - TBD)	1.0	LO	[redacted]	[redacted]	[redacted]66.42
710001	D308	PR 1300766851 ACRN AB Cost Code A00004897921 Funding Doc NWCF OVHD Funding Expires 9-30-2019 NWA 300000075062 0010 (WCF)					
7101	D308	PWS/Subtask Para# 6.2 (Fund Type - TBD)	1.0	LO	[redacted]	[redacted]	[redacted]

For Cost Type / NSP Items

Item	PSC	Supplies/Services	Qty	Unit	Est. Cost	Fixed Fee	CPFF
7103		Not Separately Priced - CDRL's	1.0	LO			NSP

For Cost Type Items:

Item	PSC	Supplies/Services	Qty	Unit	Est. Cost	Fixed Fee	CPFF
7200	D308	PWS/Subtask Para# 6.1 (Fund Type - TBD)	1.0	LO	[redacted]	[redacted]	[redacted]
		Option					
7201	D308	PWS/Subtask Para# 6.2 (Fund Type - TBD)	1.0	LO	[redacted]	[redacted]	[redacted]

Item	PSC	Supplies/Services	Qty	Unit	Est. Cost	Fixed Fee	CPFF
		Option					

For Cost Type / NSP Items

Item	PSC	Supplies/Services	Qty	Unit	Est. Cost	Fixed Fee	CPFF
7203		Not Separately Priced - CDRL's	1.0	LO			NSP

For Cost Type Items:

Item	PSC	Supplies/Services	Qty	Unit	Est. Cost	Fixed Fee	CPFF
7300	D308	PWS/Subtask Para# 6.1 (Fund Type - TBD)	1.0	LO	[redacted]	[redacted]	[redacted]
		Option					
7301	D308	PWS/Subtask Para# 6.2 (Fund Type - TBD)	1.0	LO	[redacted]	[redacted]	[redacted]
		Option					

For Cost Type / NSP Items

Item	PSC	Supplies/Services	Qty	Unit	Est. Cost	Fixed Fee	CPFF
7303		Not Separately Priced - CDRL's	1.0	LO			NSP

For Cost Type Items:

Item	PSC	Supplies/Services	Qty	Unit	Est. Cost	Fixed Fee	CPFF
7400	D308	PWS/Subtask Para# 6.1 (Fund Type - TBD)	1.0	LO	[redacted]	[redacted]	[redacted]
		Option					
7401	D308	PWS/Subtask Para# 6.2 (Fund Type - TBD)	1.0	LO	[redacted]	[redacted]	[redacted]
		Option					

For Cost Type / NSP Items

Item	PSC	Supplies/Services	Qty	Unit	Est. Cost	Fixed Fee	CPFF
7403		Not Separately Priced - CDRL's	1.0	LO			NSP

For ODC Items:

Item	PSC	Supplies/Services	Qty	Unit	Est. Cost

Item	PSC	Supplies/Services	Qty	Unit	Est. Cost
9000	D308	ODC in support of CLIN 7000 (WCF)	1.0	LO	[redacted]
900001	D308	ACRN: AA PR#: 1300646091 NWA: 300000075062 0020 DOC: NWCF Overhead Funds Expiration: 09/30/2018 (WCF)			
9100	D308	ODC in support of CLIN 7100 (Fund Type - TBD)	1.0	LO	[redacted]
910001	D308	PR 1300766851 ACRN AB Cost Code A00004897921 Funding Doc NWCF OVHD Funding Expires 9-30-2019 NWA 300000075062 0010 (WCF)			
9200	D308	ODC in support of CLIN 7200 (Fund Type - TBD)	1.0	LO	[redacted]
		Option			
9300	D308	ODC in support of CLIN 7300 (Fund Type - TBD)	1.0	LO	[redacted]
		Option			
9400	D308	ODC in support of CLIN 7400 (Fund Type - TBD)	1.0	LO	[redacted]
		Option			

ADDITIONAL SLINS

Additional SLINs will be unilaterally created by the Contracting Officer during performance of this Task Order to accommodate the funding lines that will be provided under this Order.

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

(a) For purposes of this contract, “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 this contract entitled "FIXED FEE" (FAR 52.216-8) or "INCENTIVE FEE", (FAR 52.216-10), as applicable. Such payments shall be submitted by and payable to the Contractor pursuant to the clause of this contract entitled "ALLOWABLE COST AND PAYMENT" (FAR 52.216-7), subject to the withholding terms and conditions of the "FIXED FEE" or "INCENTIVE FEE" clause, as applicable, and shall be paid fee at the hourly rate(s) specified in the table below per man-hour performed and invoiced.

Total fee(s) paid to the Contractor shall not exceed the fee amount(s) set forth in this contract. In no event shall the Government be required to pay the Contractor any amount in excess of the funds obligated under this contract.

Year	CLIN	Fixed Fee	Hours	Fee per Direct Labor Hours
Base	7000	[redacted]		[redacted]
Base	7001	[redacted]	[redacted]	[redacted]
Option 1	7100	[redacted]		[redacted]
Option 1	7101	[redacted]	[redacted]	[redacted]
Option 2	7200	[redacted]		[redacted]
Option 2	7201	[redacted]	[redacted]	[redacted]

Option 3	7300	[redacted]		[redacted]
Option 3	7301	[redacted]	[redacted]	[redacted]
Option 4	7400	[redacted]		[redacted]
Option 4	7401	[redacted]	[redacted]	[redacted]

SECTION C DESCRIPTIONS AND SPECIFICATIONS

SECTION C – DESCRIPTION/SPECS/WORK STATEMENT

SPECIFICATIONS/STATEMENT OF WORK/PERFORMANCE WORK STATEMENT

Work under this performance-based contract 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: SPAWAR Systems Center (SSC) Atlantic Business Intelligence System Data Support

1.0 PURPOSE

1.1 BACKGROUND

Space and Naval Warfare Systems Center Atlantic (SSC Atlantic) owns and operates a business intelligence system that is used jointly with its parent comment, SPAWAR. This system is currently based on SAP Business Objects Business Intelligence Platform 4.2 and SAP Data Services 4.2, along with supporting SAP Desktop Tools (for Business Objects, Data Services, Predictive Analytics, Lumira). There are three instances of Business Objects in place, supporting development, quality assurance / testing, and production, with the production instance sized for about 1400 users. The total number of users may grow to 2000 over the term of this task order. All three instances are configured similarly, with the exception of production being load balanced and clustered with two SAP BI servers. Reports are delivered via the standard BI Launchpad and a small team of report developers, universe designers, and administrators manage the system. The supporting database is ORACLE 12c. All system components are running on Red Hat Linux virtualized servers provided by the Navy Enterprise Data Center (NEDC) except for the SAP Desktop Tools which are virtualized in a pair of Windows Server 2008 R2 / CITRIX XenApp instance provided by the NEDC.

All server applications and desktop applications are approved for Navy use as of date of award. The Navy Functional Area Manager(s) has a policy to migrate to the current vendor supported version prior to lapse of Navy approval or end of vendor support for any application used. Application version updates, upgrades or patches are the responsibility of the Contractor. The software will be provided by the Government for installation under this task order.

In addition to application updates, upgrades or migrations directed by the Navy Functional Area Manger(s) noted above, normal vendor product lifecycles dictate that DWBIS will require multiple major and minor version upgrades over the term of this task order. This may require that the vendor recommend resizing components of the system based on sizing guidelines for the commercial software, or possible migration to a successor system performing similar functions.

Finally, the Navy has recently endorsed a “Cloud First” policy that will result in a system migration to another hosting solution during the first years of this task order with accompanying need to accredit the migrated system.

The work schedule for this task order is for Federal Government workdays (core hours are 0730 – 1600), with three exceptions:

a. Scheduled Extract, Transform, and Load Operations:About 40 SAP R3 reports and ZE-16 extracts are initiated at 8:00 PM local and must be validated by 0400 the next work day to load data staging tablessupporting a large automated load from Navy ERP that runs from 0400 to 0500.Once all data is staged, materialized views are created and validated to make all data available by 0700 on the work day.

b. Extended Work Week for Scheduled Extract, Transform, and Load Operations:Scheduled extended work week is required in September to provide supplemental reports for the Financial and Contracts competencies to close out the fiscal year.Extended Work Week is limited on this task order.

c. System Administration After Hours Support.The hosting Data Center schedules monthly quarterly maintenance on weekends and after hours.This will require system administrators to shut down and restart the system applications and databases cleanly after the scheduled working hours noted above.The system databases (ORACLE) are patched quarterly and also after hours.

1.2 SCOPE

This task order applies to the current business intelligence system, Data Warehouse Business Intelligence System identified in the background above; and any follow on, associated or successor systems hereafter referred to as “assigned systems.”

This system is currently hosted in a Navy Data Center using virtual servers and operating systems provided by the data center. In addition to scheduling updates and upgrades to the supporting operating systems and other infrastructure, the data center also provides certain database administration and overarching maintenance of the system certification and accreditation package. The installation, configuration, update, upgrade and patching required for the hosted applications making up the DWBIS system remain the responsibility of the hosted system owner and are part of this task order scope that follows.

This task order (TO) consists of two (2) projects spanning one (1) base year and four (4) option years:

Project_1: DWBIS System Data Support

Project_2: DWBIS Accreditation, Upgrade and Migration Support

This task order is to provide multiple-year sustainment support in the following areas:

a. Sustain automated daily data extract-transform-validation-load operations for assigned business intelligence systems.

b. Apply and maintain Information Assurance controls for assigned business systems to meet Department of Defense requirements.

c. Adjust Information Assurance controls to meet Navy Functional Area Manager (FAM) supported application version requirements and also support system reaccreditation requirements in or about 2018 and 2021 as directed by the Navy Authorizing Official (NAO)

d. Support system transition or migration under the Navy “Cloud First” policy.

This TO is funded with multiple accounting lines as delineated on specified contract line item numbers (CLINs). The TO period of performance spans one base year and four option years. The applicable PWS tasks associated with each funding CLIN is outlined in Section B and Section G of the RFP.

NOTE: Work will not be performed in Afghanistan.

2.0 APPLICABLE DOCUMENTS (AND DEFINITIONS)

All work shall be accomplished using, in order of precedence, current United States Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG), best commercial practices (for Commercial off the shelf Software (COTS)), or and current acceptable industry standards. The applicable references and standards invoked will vary within individual tasks. In accordance with Defense Acquisition Policy changes, maximum utilization of non-Government standards will be made wherever practical. Where backward compatibility with existing systems is required, selected interoperability standards will be invoked.

2.1 REQUIRED DOCUMENTS

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

	Document Number	**Title**
a.	DoDM 5220.22-M	DoD Manual – National Industrial Security Program Operating Manual (NISPOM) dtd 28 Feb 06
b.	DoDI 5220.22	DoD Instruction – National Industrial Security Program dtd 18 Mar 11
c.	DoD 5200.2-R	DoD Regulation – Personnel Security Program dtd Jan 87 (and subsequent revisions)

	Document Number	Title
d.	DoDD 5205.02E	DoD Directive – Operations Security (OPSEC) Program dtd 20 Jun 12
e.	DoD 5205.02-M	DoD Manual – Operations Security (OPSEC) Program Manual dtd 3 Nov 08
g.	DoDI 8500.01	DoD Instruction – Cybersecurity dtd 14 Mar 14
h.	DoDI 8510.01	DoD Instruction – Risk Management Framework (RMF) for DoD Information Technology (IT) dtd 12 Mar 14
i.	DoDD 8140.01	DoD Directive – CyberSpace Workforce Management dtd August 11, 2015 (supersedes Directive DoD Directive 8570.01, "Information Assurance (IA) Training, Certification, and Workforce Management," August 15, 2004)
j.	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
l.	DON CIO Memorandum	Acceptable Use of Department of the Navy Information Technology (IT) dtd 22 Feb 16
x.	Navy Telecommunications Directive (NTD 10-11)	System Authorization Access Request (SAAR) - Navy
k.	SECNAV M-5239.2	DON Information Assurance Workforce Management Manual dtd May 2009
l.	SECNAV M-5510.30	Secretary of the Navy Manual – DoN Personnel Security Program dtd Jun 2006
m.	SECNAVINST 4440.34	Secretary of the Navy Instruction – Implementation of Item Unique Identification within the DoN, dtd 22 Dec 09
n.	SECNAVINST 5239.3B	DoN Information Assurance Policy, 17 Jun 09
q.	SECNAVINST 5239.20A	Secretary of the Navy Instruction – DON Cyberspace IT and Cybersecurity dtd 10 Feb 16
o.	SECNAVINST 5510.30	DoN Regulation – Personnel Security Program
p.	SPAWARINST 3432.1	SPAWAR Instruction – Operations Security (OPSEC) Policy dtd 2 Feb 05
q.	SPAWARINST 4440.12	Management of Operating Materials and Supplies (OM&S), Government Furnished Property (GFP), Contractor Acquired Property (CAP), Property, Plant and Equipment (PP&E), and Inventory
r.	SPAWARINST 5721.1B	SPAWAR Section 508 Implementation Policy, 17 Nov 09

	Document Number	Title
s.	NAVSUP P-723	Navy Inventory Integrity Procedures, April 2012
t.	NIST SP 800-Series	National Institute of Standards and Technology Special Publications 800 Series – Computer Security Policies, Procedures, and Guidelines
v.	Public Law 93579, December 31, 1974 (5 U.S.C. 552a)	Privacy Act of 1974
w.	Federal Acquisition Regulations (FAR) 52.224 - 1	Privacy Act Notification
x.	Federal Acquisition Regulations (FAR) 52.224 - 2	Privacy Act
y.	Public Law. 107–347, 116 Stat. 2899, 44 U.S.C. § 101, H.R. 2458/S. 803	The E-Government Act of 2002 (PL 107-347)
z.	DoD Instruction 5400.16	Department of Defense Privacy Impact Assessment (PIA) Guidance
aa.	SECNAVINST 5211.5E	The Department of the Navy Privacy Program
ab.	ALLNAV 070/07	Department Of The Navy (Don) Personally Identifiable Information (PII) Annual Training Policy
ac.	DON CIO Message DTG: 091256Z OCT 07	DoN Encryption of Sensitive Unclassified Data At Rest Guidance
ad.	DoDI 8510.01	DoD Information Assurance Certification and Accreditation Process, 28 Nov 07
ae.	SECNAVINST 5239.3B	DoN Information Assurance Policy, 17 Jun 09
af.	United States Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG)	DISA Security Technical Implementation Guides (STIG)
ag.	SPAWARINST 5721.1B	SPAWAR Section 508 Implementation Policy, 17 Nov 09
ah		DON Chief Information Officer Memorandum, Limitation on Obligation of Funds for Data Servers and Centers, of July 18, 2012
ai.		DoD Chief Information Officer Memorandum, Approvals/Waivers for Obligation of Funds for Data Servers and Centers, of June 9, 2014
aj.		DoD Chief Information Officer Memorandum, Office of the Secretary of Defense Guidance for Fiscal Year 2016 Information Technology Budget Submissions, of August 8, 2014

	Document Number	Title
ak.	SPAWARNote 5239 3.c.	Interim Guidance for Privileged and Non-Privileged User Roles for the Navy Enterprise Data Center Hosted Environments
al.	DoN DIACAP Handbook	DoD Information Assurance Certification and Accreditation Process Handbook
am.	DoD Instruction 8510.01	Risk Management Framework (RMF) for DoD Information Technology (IT)

2.2 GUIDANCE DOCUMENTS

The following documents are to be used as guidance. Unless otherwise specified, the document's effective date of issue is the date on the request for proposal.

	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.	DoDI 3020.41	DoD Instruction – Operational Contract Support (OCS), of 20 Dec 10
f.	DoDI 4161.02	DoD Instruction – Accountability and Management of Government Contract Property, Apr 27,2012
g.	DoDD 5000.01	DoD Directive – The Defense Acquisition System
h.	DoDI 5000.02	DoD Instruction – Operation of the Defense Acquisition System
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
i.	ISO/IEC 15288	International Organization for Standardization/ International Electrotechnical Commission: Systems and Software Engineering – System Life Cycle Processes
j.	IEEE Std 12207-2008	Systems and Software Engineering – Software Life Cycle Processes

	Document Number	Title
k.	ANSI/EIA-748A	America National Standards Institute/Electronic Industries Alliance Standard – Earned Value Management (EVM) Systems
l.	HSPD-12	Homeland Security Presidential Directive – Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004
m.	DoDM-1000.13-M-V1	DoD Manual – DoD Identification Cards: ID card Life-Cycle dtd 23 Jan 14
n.	FIPS PUB 201-2	Federal Information Processing Standards Publication 201-2 – Personal Identity Verification (PIV) of Federal Employees and Contractors, August 2013
o.	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
p.	N/A	SSC Atlantic Contractor Checkin portal – https://wiki.spawar.navy.mil/confluence/display/SSCACOG/Contractor+Checkin
q.	N/A	SSC Atlantic OCONUS Travel Guide portal – https://wiki.spawar.navy.mil/confluence/display/SSCACOG/OCONUS+Travel+Guide
r.	SPAWARSYSCENLANTINST 12910.1A	Deployment of Personnel and Contractor Employees to Specific Mission Destinations, of 28 Dec 09

2.3 SOURCE OF DOCUMENTS

The contractor shall obtain all applicable documents. 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.

3.0 PERFORMANCE REQUIREMENTS

The following paragraphs list all required non-personal services tasks that will be required throughout the TO. The contractor shall provide necessary resources with knowledge and experience as cited in the personal qualification clause to support the listed tasks. Contractors shall perform requirements in accordance with Federal Acquisition Regulation (FAR) and/or Defense Federal Acquisition Regulation Supplement (DFARS) which do not include performance of inherently Governmental functions. The contractor shall complete all required tasks while controlling and tracking performance and goals in terms of costs, schedules, and resources.

Note: In compliance with SPAWARINST 4720.1A – SPAWAR Modernization and Installation Policy, all task order installation work performed aboard Navy ships and Navy shore sites is under Installation Management Office (IMO) supervision; otherwise, a formal exemption request has been approved. In accordance with the Fleet Readiness Directorate Standard Operating Procedure (FRD SOP), COMSPAWARSYSCOM letter Ser FRD/235 dated 24 Apr 12, the contractor shall, ensure proper notification and status updates of installation work performed outside of SSC Atlantic respective Areas of Responsibilities (AORs) are provided to the SPAWAR Officer in Charge (OIC) or applicable Geographic Lead.

3.1. RELEVANT EXPERIENCE

3.1.1 Scheduled Extract, Transform, and Load Operations

The contractor shall have expertise in configuring and sustaining daily data extracts from multiple authoritative sources including automated tools (applications) and scripts. Experience with SAP R3 reports and Navy ERP ZE-16 table extracts is also required to automate new requirements. The automated tools include SAP Data Services and Informatica; and scripting languages including ORACLE PL/SQL scripts, PERL and PYTHON used to maximize both the application and efficiency of automation to downloads and to ensure that the data is properly validated for completeness and correctness. Experience validating, transforming and loading data into ORACLE database tables following extract is required. For scheduled or automated transfers, the contractor shall have expertise in setting up source and destination authentication and encryption in transit using DoD PKI or RSA certificates.

3.1.2 DoD Private Key Infrastructure (PKI) Enabling

The contractor shall have expertise in installing, configuring and sustaining the following using DoD Public Key Infrastructure (PKI):

a. PKI enabling privileged and non-privileged user authentication to ORACLE 11g and later databases using DoD PKI hard token certificates
b. PKI enabling authentication for system accounts that connect to ORACLE 11g and later databases using DoD PKI certificates
c. PKI enabling privileged and non-privileged user authentication to Linux servers using DoD PKI hard token certificates
d. PKI enabling authentication for system accounts that connect to Linux servers using DoD PKI certificates

3.1.3 Configuring User and System Accounts to Use Strong Authentication

The contractor shall have expertise in installing, configuring and sustaining applications, databases and Linux servers to enforce:

a. DoD PKI hard token certificate authentication to control user connections for both terminal and file transfer sessions.
b. DoD PKI hard certificate authentication to control application connections for file transfer sessions.
c. Enforcement of FIPS 140-2 validated cryptography modules where supported
d. Strong RSA keys for file transfer sessions

3.1.4 Employ Automated Extract Transfer and Load Applications

The contractor shall have expertise in installing; configuring and sustaining automated applications that perform scheduled extract transform and load operations from disparate data sources to staging areas and ORACLE tables. The contractor shall have expertise in:

a. Translating objective requirements to automation
b. Performing data validation for extracts
c. Transforming extracted data to fit materialized views
d. Cleansing cleanse data for import to ORACLE tables
e. Establishing methods to determine if scheduled loads were successful

3.2. PROGRAM MANAGEMENT

The contractor shall support the Government at the Command and Sponsor level.

1. Program Support

3.2.2 Program Support Documentation

a. The contractor shall develop, draft, and submit program management (PM) documents (CDRL A001) in the form of new or updated JIRA tickets showing status of current and planned tasks and subtasks

b. Maintain Integrated Product Team collaborative workspaces (WIKI) or outreach notices (BLG) entries Command wide.

c. Establish and maintain program office repository in designated Government location

3.2.3 Training and Communications

The contractor shall provide the following User / Customer facing support on a quarterly basis:

a. Develop, deliver and execute communications and user adoption plans (CDRL A002)

b. Develop, deliver and execute training plans (CDRL A002)

c. Prepare or present informal briefings for communities of interest and/or teams to include executive level

d. Write and edit technical and non-technical documentation including project reports to leadership research papers on communication issues, articles, and training curricula. (CDRL A002)

e. Research, analysis, and reporting of information technology utilization and metrics (CDRL A002)

3.3. Operate and Sustain Business Intelligence Extracts

The following tasks require the Contractor to remain current in the capabilities and feature sets for the applications used in DWBIS. The Contractor shall conduct familiarization training with current product versions and capabilities annually, at a minimum, by product research, technical training or certification.

3.3.1 Administer Automated Extract-Transform-Load Applications

Contractor personnel shall be certified as members of the Cyber Security Work Force (CSWF), IT Level II, as described in DoD Directive 8140.01 and SPAWAR Note 5239.3B before commencing work on this task. See section 8.2 and especially section 8.2.3 below for specific certification requirements.

The contractor shall support the Government in the installation, configuration, updates, upgrade, administration and operations of automated extract-transform-load (ETL) applications such as SAP Data Services, SAP Information Steward and Informatica (hereafter, "automated ETL tools") in assigned applications and systems (currently Data Warehouse Business Intelligence System). The contractor shall adjust the order of data fields within records, prepare and process materialized views, and perform other indexing or aggregation functions as determined by weekly production meetings and assigned tickets to support reporting requirements in the DWBIS system. The Contractor shall incorporate new or modified data sources over the term of this task order. Information Assurance requirements are included from Task Order paragraph 3.5 below are included in this task.

The Contractor shall:

a. Install, update, upgrade or configure automated ETL tools and applications on assigned systems

b. Support administration of the automated ETL tools, to include DoD PKI authentication requirements.

c. Support user, user group administration and provisioning for automated ETL tools

d. Support Promotion Management or Version Management for all automated tools for ETL application objects (such as server configurations, application SQL queries used to extract, transform or load data) from the reports development tier to the reports quality assurance tier; and from the reports, quality assurance tier to the reports production tier.

e. Configure updated or established automated ETL tools and applications or their components to meet production, performance, monitoring or information assurance requirements.

f. Implement application monitoring to help system administrators monitor the production systems, alert them within one hour when problems occur, set resource thresholds for alerts, and aid in resolution of problems.

g. Schedule, or cause to be scheduled, monthly information assurance scans of the installed applications

h. Remediate findings found in the course of operations or scans to comply with United States Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG), Computer Task Orders or other requirements for the system in the allotted time.

The contractor shall keep installed or new applications current with respect to the approved versions in the Navy application portfolion in accordance with the requirements of PWS 3.4 of this task order.

The contractor shall perform and document (CDRL A003) quarterly demonstrations of backup and restoration of applications and databases databases in accordance with the current service level agreements for the Navy Data Center and to meet the requirements of PWS Paragraph 3.5.4.

In addition to the general requirements to develop or maintain certification and accreditation (C&A) documentation under Paragraph 3.5 of this task order, the contractor shall draft, develop, and maintain user, system, program, and process documentation (CDRL A004 and CDRL A005) for all assigned applications or systems, to include:

a. Installation configuration settings sufficient to reconstitute the system

b. Step by step procedures for:

1) Start up and shut down

2) Backup (full and incremental)

3) Restoration from Backup

c. Change documents for formal submission to configuration management entities at the enterprise hosting environment and Navy accrediting officials.

These documents shall be maintained in a Government designated repository and updated when changes are made or quarterly at a minimum. Configuration settings shall be checked out of the Government version controlled repository and any modifications checked in daily (CDRL A004 and CDRL A005).

3.3.2 Operate and Sustain Assigned Data Extract, Transform and Load (ETL) Operations

Contractor personnel shall be eligible for access to Navy Enterprise Resource Planning (Navy ERP) in accordance with section 8.2.2.6 of this PWS before commencing work on this task.

Contractor personnel shall be certified as members of the Cyber Security Work Force (CSWF), IT Level II, as described in DoD Directive 8140.01 and SPAWAR Note 5239.3B before commencing work on this task. See section 8.2 and especially section 8.2.3 below for specific certification requirements.

The Contractor shall perform assigned daily and weekly scheduled data extracts, transformation and load operations from multiple systems using a combination of PL/SQL load scripts, flat file imports or secure file transfer protocol (SFTP) transfers, Navy ERP ZE-16 table queries or automated data collection applications such as PERL and PYTHON to populate assigned business intelligence systems. The contractor shall adjust the order of data fields within records, prepare and process materialized views, and perform other indexing or aggregation functions as determined by weekly production meetings and assigned tickets to support reporting requirements in the DWBIS system. The Contractor shall incorporate new or modified data sources over the term of this task order.

The Contractor shall:

a. Seek to maximize the automation of ETL functions through the use of SAP Data Services, Informatica or PYTHON scripts.

b. Establish and maintain assigned ETL schedules to meet daily and weekly production schedules.

c. Establish and maintain assigned data load and validation procedures to ensure the integrity and availability of data by the daily "data available" deadlines

d. Augment these schedules near the end of the fiscal year for more frequent data loads to support year end close operations.

e. Create and maintain load scripts (CDRL A005) to accomplish extract, transform, load and validate supporting reports/analytics from assigned data sources.

f. Operate and maintain desktop database tools, scripts or queries to process or validate extracted data

g. "Cleanse" data extracted from legacy or foreign systems to conform to the data standards for SSC Atlantic business intelligence systems and other systems

h. Populate assigned databases with validated records from flat files and extracts from other systems

h. Write system documentation (CDRL A004) and user facing documentation including help libraries

i. Conduct a review and update of the interface specifications and interface security agreements for all external data sources

j. Recommend improvements to reduce the number of manual operations required to accomplish data loads.

k. Seek optimization for new and existing ETL procedures

Extract, transform and load schedules, scripts and checklists shall be maintained in a Government designated repository and updated when changes are made quarterly. Configuration settings and extract, transform and load scripts shall be checked out of the Government version controlled repository and any modifications checked in daily (CDRL A004 and CDRL A005).

3.3.3 Administer DoD PKI Authentication and Strong Encryption for ORACLE Databases and Connected Applications

Contractor personnel shall be certified as members of the Cyber Security Work Force (CSWF), IT Level II, as described in DoD Directive 8140.01 and SPAWAR Note 5239.3B before commencing work on this task.

The contractor shall support the Government in the configuration, administration and day to day operations of approved clients for ORACLE databases, assigned applications and systems (currently Data Warehouse Business Intelligence System).

The Contractor shall:

a. Support user administration and provisioning. If the SSC Atlantic business intelligence system is the destination system for a file transfer, act as Destination System Owner to:

1) Allocate storage and stipulate a directory where the files are to be sent.

2) Issue a SSH2/SFTP account to the source system owner

3) Accept the public key(s) from the source system owner or account holder for configuration on the destination system in support of an authentication handshake.

4) Ensure each Destination System Owner has their own unique account and will not be able to view or manipulate data on the destination system other than their own.

b. If the SSC Atlantic business intelligence system is the source system for a file transfer, act as Destination System Owner to:

1) Ensure each Source System Owner has their own account and will not be able to view or manipulate data on the destination system other than their own.

2) Provide public key(s) for the source system or account holder for configuration on the destination system in support of an authentication handshake.

c. Configure manual or automated file transfers and servers to enforce strong encryption, using one of the following technologies:

1) As available, the Contractor shall use DoD PKI certificates as the preferred method of authentication and encryption to transfer data to or from assigned business intelligence systems.

2) Should DoD PKI certificates be unavailable, the Contractor shall use strong authentication with a key strength of RSA 2048 bit key at a minimum.

d. Configure applications to use FIPS-140 compliant encryption when available.

e. Install, update, upgrade or configure applications to run under the least privilege required or in a restricted ("jailed") root directory.

The contractor shall perform and document (CDRL A003) quarterly demonstrations of backup and restoration of servers, applications or databases in accordance with the current service level agreements for the Navy Data Center and to meet the requirements of PWS Paragraph 4.6 of this task order.

In addition to the general requirements to develop or maintain certification and accreditation (C&A) documentation under Paragraph 3.5 of this task order, the contractor shall draft, develop, and maintain user, system, program, and process documentation (CDRL A004 and CDRL A005) for all designated applications or systems, to include:

a. Installation configuration settings sufficient to reconstitute the system

b. Step by step procedures for:

1) Start up and shut down

2) Backup (full and incremental)

3) Restoration from Backup

c. Change documents for formal submission to configuration management entities as specified to meet customer requirements.

Database and client configuration files and scripts shall be maintained in a Government designated repository and updated when changes are made or quarterly. Configuration settings shall be checked out of the Government version controlled repository and any modifications checked in daily (CDRL A004 and CDRL A005).

1. Conform to Current Department of the Navy (DON) Application & Database Management System (*DADMS*) Approved or Allowed Application Portfolio

In addition to the requirements of Sections 4.2, Acquisition of Commercial Software Products, Hardware, and Related Services and 4.5, Registration of DoN Applications Networks and Servers, for assigned systems, databases or applications, the Contractor shall:

a. procure

b. For minor version updates, update installed or planned applications to conform to Navy Last Date Allowed (LDA) policy or guidance to ensure only approved applications are used

c. For major upgrades, upgrade installed or planned applications to conform to Navy Last Date Allowed (LDA) policy or guidance.

d. Create or modify system documentation (CDRL A004 and CDRL A005) and user facing documentation including help libraries

e. Adjust Certification and Accreditation documentation (section 3.5).

These documents shall be maintained in a Government designated repository and updated when changes are made or at least quarterly.

2. Cybersecurity (Information Assurance) Support

Contractor personnel shall be certified as members of the Cyber Security Work Force (CSWF), IT Level II, as described in DoD Directive 8140.01 and SPAWARNote 5239.3B before commencing work on this task . See section 8.2 and especially section 8.2.3 below for specific certification requirements.

Cybersecurity (also known as Information Assurance (IA) includes tasks which the contractor shall protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

3.5.1 Product Selection and Cybersecurity/Computer Security Requirements.

The contractor shall research and recommend software products to the Government to conform to Navy Functional Area Manager version requirements, to remain within commercial product support lifecycles, or to obtain functional or efficiency goals. The contractor shall:

a. Ensure that all products recommended that impact cybersecurity or Information Assurance (IA) shall be selected from the NIAP Validated Products List.

b. Ensure that products chosen shall be based on the appropriate Evaluated Assurance Level (EAL) for the network involved, and utilized in accordance with latest Defense Information Systems Agency (DISA) policy at time of order. This information shall be tracked and available for Government review.

c. Ensure that the recommendation of hardware or software products that perform cryptography or incorporate cryptography modules is limited to those that are validated to conform to the current requirements of the National Institute of Standards and Technology (NIST) issued Federal Information Processing Standards (FIPS) 140-2 Publication Series "FIPS 140-2 Validated Cryptography for Secure Communications"; and that these products are installed and configured to enable FIPS 140-2 encryption or cryptography.

d. Comply with ASD-NII/DOD-CIO Memorandum, "Encryption of Sensitive Unclassified Data-at-Rest on Mobile Computing Devices and Removable Storage."

3.5.2 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 4.2.2. 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.

3.5.3 Cyber Security Planning Services.

The contractor shall provide security services to enhance the confidentiality, integrity, availability, authentication, and non-repudiation requirements for assigned applications or systems. The contractor shall support the use of approved mechanisms of encryption, access control, user identification and authentication, malicious content detection, audit, and physical and environmental control. The contractor shall propose updated and/or revised architecture and/or configuration change designs to accommodate changing requirements, emerging technology, and results of vulnerability assessments for Government review and approval.

3.5.4 Federal Information Security Management Act (FISMA).

The Contractor shall:

3.5.4.1 Monitor Systems or Applications Information Assurance Status

Documents generated under this task shall be transmitted using DoD PL/SQL encrypted e-mail or placed in a Government designated repository appropriate to the level of classification (see PWS 8.4.2).

For systems or applications, the Contractor shall:

a. Serve as the Information Assurance Officer (IAO) for applications

b. Review system or application audit logs either manually or through automated tools

c. Report any system anomaly that could result in an unauthorized disclosure of or access to sensitive information within one hour of identification.

d. Review current threats and outstanding vulnerabilities using Assured Compliance Assessment Solution (ACAS)

e. Perform monthly vulnerability scans for applications or systems. If the scan must be performed by Navy Enterprise Data Center personnel, the Contract shall initiate the request. The Contractor shall protect the vulnerability scan results as UNCLASSIFIED / SENSITIVE.

f. Support security and information assurance evaluations; develop/maintain test and audit records

g. Perform monthly access audits and suspend and restore user accounts to control access.

h. Perform and document (CDRL A003) quarterly tests of the backup and restore capability for each application or database.

i. Conduct or support annual security reviews (CDRL A003) in accordance with the Department of Navy DoD Information Assurance Certification and Accreditation Process Handbook and adjust Certification and Accreditation Documents under section 3.5.4.

3.5.4.2 Establish or Adjust System and Application Security Controls to Meet Requirements of DoD Information Assurance Vulnerability Management (IAVM) Program

Documents generated under this task shall be transmitted using DoD PKI encrypted e-mail or placed in a Government designated repository appropriate to the level of classification (see PWS 8.4.2).

For systems or applications, the Contractor shall:

a. Apply DISA Security Technical Implementation Guides (STIG) to configure systems, operating systems and applications to meet DoD Information Assurance requirements.

b. Apply vendor updates, patches and version upgrades to meet functional requirements or Department of Defense Information Assurance requirements (e.g., Information Assurance Vulnerability Management (IAVM) Program (such as Information Assurance Vulnerability Alerts (IAVA), Information Assurance Vulnerability Bulletins (IAVB), Technical Advisories (TA) or Computer Tasking Orders (CTO)) within the time limits described by current US CYBER COMMAND guidance.

c. Update and document applicable Certification and Accreditation artifacts (CDRL A006) to support accreditation or reaccreditation.

3.5.5 Adjust Certification and Accreditation Documentation

Documents generated under this task shall be transmitted using DoD PKI encrypted e-mail or placed in a Government designated repository appropriate to the level of classification (see PWS 8.4.2).

The Contractor shall:

3.5.5.1 Support obtaining certification and accreditation (C&A) for applications or systems, to include process support, analysis support, coordination support, conduct of various IA control validation activities, compiling validation results, and creation or execution of Plan of Actions and Milestones (POA&Ms) (CDRL A003).

3.5.5.2 Ensure that all Certification and Accreditation (C&A) documentation (CDRL A006) are created or maintained, and where applicable, updated to include any deployment of new software products or the inclusion of new interfaces that require Information Assurance (IA) updates.

3.5.6 Cyber Security, Information Assurance (IA) and Cyber Network Defense (CND)

Documents generated under this task shall be transmitted using DoD PKI encrypted e-mail or placed in a Government designated repository appropriate to the level of classification (see PWS 8.4.2).

3.5.6.1 Security Operational Services. The contractor shall provide cyber security services for protection of the Information Systems, Information System Domains (Communities of Interest), and Information Content (at rest, in use, and in transit) in accordance with DoD Information Assurance policies and procedures. These security services shall be provided to protect all sensitive information.

3.5.6.2 Vulnerability Assessments. The contractor shall implement the necessary IA/CND mechanisms to provide cyber security services, and shall conduct vulnerability assessments to validate that the necessary controls are in place.

3.5.6.3 Response to Government Directed Information Assurance directives. As part of implementing these cyber security services, the contractor shall be responsible for implementing Government directed IA/CND direction such as Information Operations Conditions (INFOCONs) and incident reporting (e.g., system anomalies, outages.). Implementation of IA/CND mandates, applicable DoD and Navy cybersecurity orders, JTF-GNO Communications Tasking Orders (CTOs), Task Orders (TASKORDs), Operational Orders (OPORDs), Warning Orders (WARNORD), Operational Directive Messages (ODM), Information Special Outage Report (INFOSPOT), Situational Awareness Report (SITREP), and Fragmentary Orders (FRAGOs), Navy Administration Order (NAVADMIN) within Government specified timeframes.

3.5.6.4 Vulnerability Management. The contractor shall provide vulnerability management support for applications and systems. The contractor shall:

a. Take immediate action to assess the impacts of each vulnerability, develop patching plans and begin gathering data for the "First Report" requirement (CDRL A006). The patch plan should consider any other systems that may not be patched by the POA&M report date. The Program Manager shall begin evaluating these systems for possible POA&M actions as soon as possible.

b. Install, configure, and test patches and changes required by Vulnerability Management System issuances (IAVAs, IAVBs, IAVMs). All necessary changes shall be made to systems in accordance with the suspense date articulated by the appropriate Government authority. Patches or changes that require down time shall be coordinated with the Government and scheduled after 5 p.m. or performed during the weekend. The contractor shall install all patches or changes to the servers on test servers prior to being applied to production.

c. Ensure IAVM compliance through

(1) The normal Certification and Accreditation (C&A) process, and

(2) Monthly scanning of the systems using the current Navy Enterprise Data Center vulnerability scanning package.

3.6 Design, Development, Integration and Systems Engineering Support

Contractor personnel shall be certified as members of the Cyber Security Work Force (CSWF), IT Level II, as described in DoD Directive 8140.01 and SPAWAR Note 5239.3B before commencing work on this task.

The contractor shall draft design and sustainment requirements (CDRL A007) for new and existing business systems, develop and execute significant alterations to existing systems, revise or establish new interfaces for existing equipment or software into different applications or platforms.

The contractor shall plan for and execute version upgrades for systems to meet Navy Functional Area Manager Last Use Dates or other authorized use deadlines.

The contractor shall plan for compatibility with existing data structures used by NAVY ERP or other external information systems, and current extract, transform and load requirements. The contractor shall incorporate new data requirements, review logical and physical database designs, assess utilization and performance estimates for existing or proposed databases, analyze data dictionaries, prepare software and database design assessment reports (CDRL A007), define data items, and perform structured entity based analysis and design of databases.

3.6.1 Technical Review of Proposed Designs.

The contractor shall conduct technical reviews of system/subsystem designs (including recommended commercial implementations) for independent validation and verification purposes (CDRL A003).

3.6.2 Database Engineering.

Performance of this task requires that contractor personnel be certified as members of the Cyber Security Work Force (CSWF), IT Level II, as described in DoD Directive 8140.01 and SPAWAR Note 5239.3B before commencing work on this task. See section 8.2 and especially section 8.2.3 below for specific certification requirements.

The contractor shall develop or support the re-engineering of database applications for new or re-engineered processes. The applications shall be based on new, upgraded or reengineered systems, databases, and processes and employ installed technology (e.g., ORACLE DBMS) (CDRL A007).

3.6.3 System Design and Specifications.

The contractor shall design and implement system/subsystems, hardware, firmware or software required for business systems. The contractor shall develop and produce system and subsystem design and product specifications for implementation under this task (CDRL A007).

3.6.4 System Interface Design and Specifications.

The contractor shall design and implement system/subsystems interfaces for business systems. The contractor shall develop and produce system and subsystem interface specifications (CDRL A007).

3.6.5 System or Application Backup and Recovery.

The contractor shall design, develop, maintain, and implement database backup/recovery procedures suitable for a MAC III sensitive system (CDRLs A004, A007).

3.6.6 Migration and Sustainment Support.

The contractor shall provide transition planning support to the government for migration to new or reengineered applications, systems, or hosting environments (e.g., Navy approved Cloud providers). Work under this task includes planning to transition to new versions of current applications. Deliverables under this task shall include (CDRL A008, CDRL A022):

a. Work package development

b. Project Plans

c. Resource Requirements

d. Architectural Systems and Operational Views

3.7 Configuration Management (CM) Support

The contractor shall review and evaluate other re-engineering documents for configuration management compliance in order to support change control boards.

The contractor shall support and document (CDRL A007) requirements definition, design reviews for both internal (to SSC Atlantic) and external change control boards.

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 RDT&E network.

4.1.2 Follow DoDI 8510.01 of 12 Mar 2014 when deploying, integrating, and implementing IT capabilities.

4.1.3 Migrate all Navy Ashore production systems to the 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 of 17 June 2009 & DoDI 8510.01 of 12 Mar 2014 prior to integration and implementation of IT solutions or systems.

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

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

The Government will procure any software or licenses required under this task.

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 Enterprise Licensing Agreement/DoD Enterprise Software Initiative Program

Pursuant to DoN Memorandum – Mandatory use of DoN Enterprise Licensing Agreement (ELA) dtd 22 Feb 12, contractors that are authorized to use Government supply sources per FAR 51.101 shall verify if the product is attainable through DoN ELAs and if so, procure that item in accordance with appropriate ELA procedures. If an item is not attainable through the DoN ELA program, contractors shall then utilize DoD Enterprise Software Initiative (ESI) program (see DFARS 208.74) and government-wide SmartBuy program (see DoD memo dtd 22 Dec 05). The contractor shall ensure any items purchased outside these programs have the required approved waivers as applicable to the program. Software requirements will be specified at the TO/contract level.

4.2.2 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.

4.2.3 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.

4.3 Section 508 Compliance

The contractor shall ensure that 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 of 17 Nov 2009. In accordance with FAR 39.204, this requirement does not apply to contractor acquired software that is incidental to the task, software procured/developed to support a program or system designated as a National Security System (NSS) or if the product is located in spaces frequented only by service personnel for maintenance, repair or occasional monitoring of equipment.

4.4. SOFTWARE DEVELOPMENT/MODERNIZATION AND HOSTING

The contractor shall ensure all programs utilizing this contract for software development/ modernization (DEV/MOD), including the development of IT tools to automate SSC Atlantic business processes are compliant with DON Information Management/Information Technology (DON IM/IT) Investment Review Process Guidance requirements. Contractors shall neither host nor develop IT tools to automate SSC Atlantic business processes unless specifically tasked within the task order. IT tools developed to automate SSC Atlantic business processes shall be delivered with full documentation (CDRL A004) and source code (CDRL A005) to allow non-proprietary operation and maintenance by any source. The contractor shall ensure all programs are submitted with proof of completed DEV/MOD certification approval from the appropriate authority in accordance with DON policy prior to TO award. (DITPR-DON Update)

*Note must be listed on Investment Review Board (IRB) approved list.

4.5 REGISTRATION OF DON APPLICATIONS NETWORKS AND SERVERS

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 DADMS and are FAM approved. All integrated, installed, or operational applications hosted on Navy networks must also be registered in DON Application and Database Management System (DADMS) and approved by the FAM. No operational systems or applications will be integrated, installed, or operational on the RDT&E network. All systems supported shall be registered within the DoD IT Repository (DITPR). The contractor shall ensure that all networks, servers, or associated devices procured and/or connected to a Navy network complete DADMS registration and receive FAM approval. Specific requirements will be evaluated/approved by the Government prior to issuance of task order.

a. Contractor-owned or maintained-IT systems under task order to DON must be registered in the Department of Defense IT Portfolio Registry (DITPR)-DON.

4.6 IT ARCHITECTURE, INFORMATION ASSURANCE AND FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA)

The contractor shall:

4.6.1 Support security/Information Assurance requirements definition by identifying controls to be put in place for the identified systems and networks.

4.6.2 Recommend processes for maintaining and enforcing security/Information Assurance for identified systems, networks and applications in support of security engineering.

4.6.3 Ensure that the certification and accreditation (C&A) requirements and processes are documented in accordance with DoDI 8510.01 in support of security engineering delivering Section 3 of the Systems Security Authorization Agreement (SSAA), System Identification Profile (SIP), and Plan of Actions and Milestones (POA&M).

4.6.4 Ensure that requirements are coordinated to ensure all pertinent, regulatory IA policies are complied with.

4.6.5 Ensure that all SSAAs and associated accreditation support documentation are in compliance with current Chairman of the Joint Chiefs Staff instructions (CJCSI), DoD, DON, and SPAWAR mandates and regulations in support of security engineering as it relates to the SSAA.

4.7 WIRELESS DATA SERVICE OR SERVICE WITH STRONG AUTHENTICATION, NONREPUDIATION, AND PERSONAL IDENTIFICATION WHEN ACCESSING A DOD INFORMATION SYSTEM

The contractor shall ensure that all wireless local area network (LAN) traffic shall be protected, at a minimum, by a Federal Information Processing Standards (FIPS) 140-2 certified device that authenticates and encrypts at Layer 2 of the Open Systems Interconnection (OSI) model. The contractor shall comply with DoDI 8420.01 dated 3 Nov 09 when implementing Wireless Local Area Network (WLAN) Device systems. All WLAN traffic must be compliant with IEEE 802.11i standards and meet Wi-Fi Protected Access-2 (WPA-2) certification.

4.8 NAVY INFORMATION DOMINANCE APPROVAL SYSTEM (NAV-IDAS) APPROVAL REQUIRED PRIOR TO THE PURCHASE / LEASE / RENTAL OF NEW OR UPGRADED SERVERS, APPLICATION HOSTING OR DATA CENTER INFRASTRUCTURE

Server and application hosting are subject to review and approval by the Department of Navy Command Information Officer (DoN CIO) prior to obligation of funds. The SSC Atlantic business intelligence systems are currently hosted in a Navy Enterprise Data Center and use those resources for virtualized servers, networks and other infrastructure. The contractor shall ensure compliance with the FY12 National Defense Authorization Act (NDAA), DoD Chief Information Officer Memorandum, Office of the Secretary of Defense Guidance for Fiscal Year 2016 Information Technology Budget Submissions, of August 8, 2014 for any servers procured connecting to a Navy network that do not meet an exemption. The contractor shall ensure that DoN CIO approvals are obtained prior to the procurement of any server, network, data center infrastructure or application hosting solution.

5.0 TASK ORDER ADMINISTRATION

Contract administration is required for all contracts; it provides the government a means for contract 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 CONTRACT 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 Contracting Officer's Representative (COR), as applicable. Note: For Indefinite Delivery/Indefinite Quantity (IDIQ) contracts, CORs will be at the task order level. 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 contract performance. The PM shall have authority to approve task order proposals or modifications in 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, unless otherwise directed at the task order level, periodic meetings with the COR.

5.2 TASK ORDER MONITORING AND MAINTENANCE

The contractor shall have processes established in order to provide all necessary resources and documentation during various times throughout the day in order to facilitate a timely task order (TO) award or modification. Prior to task order award, the contractor shall be responsible for providing any required support documentation in a timely manner so as to not disrupt the TO award process. To address urgent requirements, the contractor shall have processes established during business and non-business hours/days in order to provide all necessary documentation and resources to facilitate a timely TO award or modification. *NOTE: Directly billing to a TO prior to TO award is prohibited.*

5.2.1 Contract Administration Documentation

Various types of contract administration documents are required throughout the life of the contract. At a minimum, the contractor shall provide the following documentation, unless otherwise specified:

5.2.1.1 Task Order Status Report (TOSR)

Task Order Status Reports (CDRL A008) shall be developed and submitted monthly, weekly, and/or as required as cited in the requirements of each task order. The prime 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 TO status report monthly no more than 30 days after TO award on the 10th of each month for those months the TO is active. The contractor shall report on various TO 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 (Attachment 1), Personnel Listing (Attachment 2), and Government Furnished Property (GFP) Template (Attachment 3) necessary for additional data collection as required.

(b) Weekly TOSR – the contractor shall develop and submit a weekly TO Status Report shall be e-mailed to the COR no later than close of business (COB) every Friday. The first report shall be required on the first Friday following the first full week after the TO award date. The initial report shall include a projected Plan Of Action and Milestones (POA&M). In lieu of a formal weekly report, larger, more complex TOs shall require an updated Earned Value Management report. At a minimum unless otherwise noted, the contractor shall include in the weekly status report the following items and data:

1. Percentage of work completed
2. Percentage of funds expended per ship/sub/shore command and system
3. Updates to the POA&M and narratives to explain any variances
4. If applicable, notification when obligated costs have exceeded 75% of the amount authorized

(c) 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, unless otherwise specified. The contractor shall ensure all information provided is the most current. Cost and funding data shall reflect real-time balances. Report shall account for all planned, obligated, and expended charges and hours. At a minimum unless otherwise noted, 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. Most current GFP and/or CAP listing

5.2.1.2 Task Order Closeout Report

A task order (TO) closeout report (CDRL A009) shall be developed and submitted no later than 15 days before the TO completion date. Prime shall be responsible for collecting, integrating, and reporting all subcontracting information. See applicable DD Form 1423 for additional reporting details and distribution instructions.

5.2.1.3 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 Cybersecurity Workforce (CSWF) and Cyber IT workforce personnel. The contractor shall develop, maintain, and submit a monthly CSWF Report (CDRL A010) identifying CSWF individuals who are IA trained and certified. Utilizing the format provided in CDRL A010 Attachment 1of 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.

5.2.1.4 Contractor Manpower Reporting

The following reporting is required for all DoD contracts acquiring services regardless if cost type or firm-fixed price contract:

(a) Contractor Manpower Quarterly Status Report (QSR)

The contractor shall provide a Contractor Manpower Quarterly Status Report (CDRL A011) to the Government four times throughout the calendar year. Required by SSC Atlantic for all active service contracts, beginning at the time of task order award, the Manpower report shall itemize specific task order administrative data for SSC Atlantic. Utilizing the format provided in QSR CDRL Attachment 1, the contractor shall collect required data throughout the specified performance period and shall submit one cumulative report on the applicable quarterly due date. See applicable DD Form 1423 for additional reporting details and distribution instructions. The following table lists the pre-set submittal due dates and the corresponding performance periods:

#	QUARTERLY DUE DATE	PERFORMANCE PERIOD
1	15 January	1 October – 31 December
2	15 April	1 January – 31 March
3	15 July	1 April – 30 June
4	15 Oct	1 July – 30 September

(b) Enterprise-wide Contractor Manpower Reporting Application

In addition to the QSR CDRL reporting requirements noted above and 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 contract for the DoD via a secure data collection website – Enterprise-wide Contractor Manpower Reporting Application (eCMRA). Contracted services excluded from reporting are based on Product Service Codes (PSCs). The excluded PSCs are:

(1) W, Lease/Rental of Equipment;

(2) X, Lease/Rental of Facilities;

(3) Y, Construction of Structures and Facilities;

(4) S, Utilities ONLY;

(5) V, Freight and Shipping ONLY.

5.2.1.5 WAWF Invoicing Notification and Support Documentation

In accordance with DFARS clause 252.232-7003, 252.232-7006, and local clause 5252.216-9210, the contractor shall submit payment requests and receiving reports using DoD Invoicing, Receipt, Acceptance, and Property Transfer (iRAPT) application (formerly known as Wide Area Work Flow (WAWF)) 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 WAWF. In accordance with local clause 5252.216-9210, the contractor shall include cost back–up documentation (e.g., delivery receipts, time sheets, & material/travel costs) to the invoice in iRAPT/WAWF. The contractor shall also provide a soft copy of the invoice and any supporting invoice documentation (CDRL A012) directly to the COR to assist in validating the invoiced amount against the products/services provided during the billing cycle. As applicable, the contractor shall forward copies of invoices to the COR within 24 hours after submittal of iRAPT /WAWF payment request.

5.2.1.6 Labor Rate Limitation Notification

For all cost type, labor-hour service TOs (not applicable for wholly firm fix-priced contracts/TO), the contractors shall monitor the following labor rates as part of the monthly TO status report (see TOSR CDRL Attachment 2 – Personnel Listing). The contractor shall initiate required notification if specified threshold values are met. NOTE: TOs that are wholly firm-fixed price are exempt from this requirement. The ability of a contractor to monitor labor rates effectively shall be included in the contract/task order Quality Assurance Surveillance Plan (QASP).

(a) Fully burdened labor rates per person (subcontractor included) charged on task order – If the actual invoiced fully burden rate (inclusive of fee) of any individual in any labor category exceeds the threshold amount of $165.00/hour and the individual's rate was not disclosed in pre-award of the basic task order, the contractor shall send notice and rationale (CDRL A013) for the identified labor rate to the COR who will then send appropriate notification to the Contracting/Ordering Officer. NOTE: Within one labor category, if the total collective estimated and/or actual hours in any given period of performance are less than or equal to 500 labor hours, the labor category is excluded from the required CDRL notification regardless if an individual within that labor category exceeds the threshold.

(b) Average actual labor rates (total actual fully burdened labor costs "divided by" total number of hours performed) compared to average negotiated labor rates (total negotiated fully burdened labor costs "divided by" total number of hours negotiated) – If the average actual burdened labor rates exceeds the average proposed/negotiated rate by 15%, the contractor shall send notice and rationale (CDRL A013) for the rate variance to the COR who will then send appropriate notification to the Contracting /Ordering Officer. Additionally, contractors shall notify the COR if variances exceed 15% for more than three consecutive months. Contractors shall annotate the variance percentage of monthly average actual labor rates versus average negotiated labor rates in the monthly contract/TO status reports.

5.2.1.7 ODC Limitation Notification

Contractors shall monitor Other Direct Costs (ODCs) as part of the monthly contract/TO status reports. For this monitoring purpose, ODCs shall 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 A013) 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 shall be included in the contract/task order Quality Assurance Surveillance Plan (QASP).

5. 3 CONTRACT ORGANIZATIONAL CONFLICT OF INTEREST (OCI)

Due to the type of work performed, there are organizational conflict of interest clauses that are applicable to this task order. The contractor shall follow the restrictions as cited in clause 5252.209-9203.

In accordance with clause 5252.209-9203 of this task order, the Contractor shall submit an organizational conflict of interest mitigation plan (CDRL A014) that is acceptable to the Government before being authorized access to sensitive or proprietary data under this Task Order.

5.4 EARNED VALUE MANAGEMENT (EVM)

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

6.0 QUALITY

6.1 QUALITY SYSTEM

Upon task order award, the prime contractor shall have and maintain a quality assurance process that meets task order requirements and program objectives while ensuring customer satisfaction and defect-free products/process. The quality system shall be documented and contain procedures, planning, and all other documentation and data necessary to provide an efficient and effective quality system based on a contractor's internal auditing system. Thirty (30) days after task order award, the contractor shall provide to the Government a copy of its Quality Assurance Plan (QAP) and any other quality related documents (CDRL A014) as required in the TO. The quality system shall be made 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 and development of quality related documents. At a minimum, the contractor's quality system shall meet the following key criteria:

a. Establish documented, capable, and repeatable processes

b. Track issues and associated changes needed

c. Monitor and control critical product and process variations

d. Establish mechanisms for feedback of field product performance

e. Implement and effective root-cause analysis and corrective action system

f. Establish methods and procedures for continuous process improvement

6.2 QUALITY MANAGEMENT PROCESS COMPLIANCE

6.2.1 General

The contractor shall have processes in place that shall coincide with the Government's quality management processes. As required, 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 event-driven milestones and reviews as stated in the Defense Acquisition University's (DAU's) DoD Integrated Defense Acquisition, Technology, and Logistics Life Cycle Management System Chart which is incorporates multiple DoD directives and instructions – specifically 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 of Lean Six Sigma methodologies in compliance with SSC Atlantic requirements and with the SSC Engineering Process Office (EPO) Capability Maturity Model Integration (CMMI) program. As part of a team, the contractor shall support projects at SSC Atlantic that are currently, or in the process of, being assessed under the SSC EPO CMMI program. The contractor shall be required to utilize the processes and procedures already established for the project and the SSC EPO CMMI program and deliver products that are compliant with the aforementioned processes and procedures. Although having a formal CMMI appraisal is desired, it is not required.

6.3 QUALITY ASSURANCE

The contractor shall perform all quality assurance process audits necessary in the performance of the various tasks as and identified by the respective WBS, POA&M, or quality system, and the contractor shall deliver related quality plan/procedural documents upon request. The Government reserves the right to perform any additional audits deemed necessary to assure that the contractor processes and related services, documents, and material meet the prescribed requirements and to reject any or all processes or related services, documents, and material in a category when noncompliance is established.

6.4 QUALITY CONTROL

The contractor shall perform all quality control inspections necessary in the performance of the various tasks as and identified by the respective WBS, POA&M, or quality system, and the contractor shall submit related quality objective evidence upon request. Quality objective evidence (CDRL A014) shall include any of the following as applicable:

a. Detailed incoming receipt inspection records

b. First article inspection records

c. Certificates of Conformance

d. Detailed sampling inspection records based upon MIL-STD-1916 (Verification Level III)

e. Quality Measurement and Analysis metrics/data

The Government reserves the right to perform any inspections or pull samples as deemed necessary to assure that the contractor provided services, documents, material, and related evidence meet the prescribed requirements and to reject any or all services, documents, and material in a category when nonconformance is established.

6.5 QUALITY MANAGEMENT DOCUMENTATION

In support of the contract's Quality Assurance Surveillance Plan (QASP) and Contractor Performance Assessment Reporting System (CPARS), the contractor shall provide the following documents: Cost and Schedule Milestone Plan (CDRL A015) submitted 10 days after Task

Order award, and Contractor CPARS Draft Approval Document (CDAD) Report (CDRL A016) submitted monthly.

7.0 DOCUMENTATION AND DELIVERABLES

7.1 CONTRACT DATA REQUIREMENT LISTINGS (CDRLs)

The following CDRL listing identifies the data item deliverables required under this contract and the applicable section of the PWS for which they are required. 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.

CDRL #	Deliverable Title	PWS Ref Para	Frequency	Date Due	Security Classification (up to S/TS or unclassified)
A001	Program Management Reports, General	3.2.2	ASREQ	Within 24 hrs from request	Unclassified
A002	Training Documentation – training plans, training presentation materials, training curricula	3.2.3	ASREQ	Within 24 hrs from request	Unclassified
A003	Technical/Analysis Reports, General	3.3.1 - 3.3.3, 3.5.4, 3.5.5, 3.6.1	ASREQ	Within 24 hrs from request or scheduled quarterly test	Unclassified / SENSITIVE
A004	Software Documentation/Programmer's Guide	3.3.1, 3.3.2, 3.3.3, 3.4, 3.6.5, 4.4	ONE/R	Revise Quarterly or after software version upgrade	Unclassified / SENSITIVE
A005	Source Code	3.3.1, 3.3.2, 3.3.3, 3.4, 4.4	ONE/R	Revise Quarterly or after software version upgrade	Unclassified / SENSITIVE
A006	C&A Documentation	3.5.4, 3.5.5, 3.5.6	ASREQ	Within 24 hrs from request	Unclassified
A007	Engineering Design Documentation, General	3.6, 3.6.2 – 3.6.5, 3.7	ASREQ	Within 24 hrs from request	Unclassified / SENSITIVE
A008	Task Order Status Report	3.6.6, 5.2.1.1, 11.2, 11.4.3	MTHLY	30 DATO and monthly on the 10th	Unclassified
A009	Task Order Closeout Report	5.2.1.2, 11.5	1TIME	NLT 15 days before completion date	Unclassified
A010	Cybersecurity Workforce (CSWF) Report	5.2.1.3, 8.1.2	MTHLY	30 DATO and monthly on the 10th	Unclassified
A011	Contractor Manpower Quarterly Status Report (QSR)	5.2.1.4	QTRLY	15 Jan, 15 Apr, 15 Jul, & 15 Oct	Unclassified
A012	Invoice Support Documentation	5.2.1.5	ASREQ	Within 24 hrs from request	Unclassified
A013	Limitation Notification & Rationale	5.2.1.6, 8.1.2	ASREQ	Within 24 hrs from request	Unclassified
A014	Quality Documentation	6.1, 6.4	ASREQ	Within 24 hrs from request	Unclassified
A015	Cost and Milestones Schedule Plan	6.5	One time with revisions (ONE/R)	NLT 10 DATO; revision NLT 7 days after receipt of govt review	Unclassified
A016	Contractor CPARS Draft Approval Document (CDAD) Report	6.5	MTHLY	30 DATO and monthly on the 10th	Unclassified
A017	Organizational Conflict of Interest Mitigation Plan	17.7	ONCE/R	On Award	Unclassified

7.2 ELECTRONIC FORMAT

At a minimum, the contractor shall provide deliverables electronically by e-mail; hard copies are only required if requested by the government. To ensure information compatibility, the contractor shall guarantee all deliverables (i.e., CDRLs), data, and correspondence 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 contract award unless otherwise specified. *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

7.3 INFORMATION SYSTEM

7.3.1 Electronic Communication

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

7.3.2 Information Security

Pursuant to DoDM 5200.01, the contractor shall provide adequate security for all unclassified DoD information passing through non-DoD information system including all subcontractor information systems utilized on contract. The contractor shall disseminate unclassified DoD information within the scope of 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 contract, and privileged contract information (e.g., program schedules, contract-related tracking).

7.3.2.1 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 utilized subcontractors shall abide by the following safeguards:

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

(b) Protect information by one physical or electronic barrier at a minimum (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 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 application-provided password protection level encryption.

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

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

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

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

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

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

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

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

7.3.2.2 Compliance

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

8.0 SECURITY

8.1 ORGANIZATION

8.1.1 Security Classification

As specified in clause 5252.204-9200 and the DoD Contract Security Classification Specification, DD Form 254, classified work is performed under this TO. The contractor shall have at the time of TO award and prior to commencement of classified work, a SECRET facility security clearance (FCL).

Prior to commencement of work on this task order, all contractor personnel (including administrative and subcontractor personnel) shall have, at a minimum, a favorable Trustworthiness Determination, which is determined by a NACLC and favorable FBI fingerprints.

The following PWS task(s) requires access to classified information up to the level of SECRET: PWS Paragraph 3.4 Information Assurance. Access to SECRET information will be limited to that determined by the Government as required to satisfy Computer Tasking Orders that apply to business intelligence systems. U.S. Government security clearance eligibility is required to access and handle classified and certain controlled unclassified information (CUI), attend program meetings, and/or work within restricted areas unescorted.

8.1.2 Security Officer

The contractor shall appoint a Facility Security Officer (FSO) to support those contractor personnel requiring access to Government facility/installation and/or access to information technology systems under this task order. The FSO is a key management personnel who is the contractor's main POC for security issues. The FSO shall have a U.S. Government security clearance equal to or higher that the FCL required on this contract. The FSO shall be responsible for tracking the security requirements for all personnel (subcontractors included) utilized on contract. Responsibilities include entering and updating the personnel security related and mandatory training information within the Staffing Plan document, which is part of TOSR Attachment 1 (CDRL A013) – applicable Staffing Plan sheets include: Security Personnel Tracking sheet, CAC SPAWAR Badge Tracking sheet, Mandatory Training Sheet. The FSO shall also update and track CSWF data (CDRL A010).

8.2 PERSONNEL

The contractor shall conform to the security provisions of DoDI 5220.22/DoD 5220.22M – National Industrial Security Program Operating Manual (NISPOM), SECNAVINST 5510.30, DoD 8570.01M, and the Privacy Act of 1974. Prior to any labor hours being charged on contract, the contractor shall ensure their personnel (including administrative and subcontractor personnel) have obtained and can maintain favorable background investigations at the appropriate level(s) for access required for the task order, and if applicable, are certified/credentialed for the Cybersecurity Workforce (CSWF). A favorable background determination is determined by either a 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 fitness standard, the contractor shall permanently remove the individual from SSC Atlantic facilities, projects, and/or programs. If an individual who has been submitted for a fitness determination or security clearance is "denied" or receives an "Interim Declination," the contractor shall remove the individual from SSC 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 task and contract.

8.2.1 Personnel Clearance

The following personnel associated with this contract shall possess a SECRET personnel security clearance (PCL). 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 Department of Defense Consolidated Adjudications Facility (DoD CAF) and shall comply with IT access authorization requirements. In addition, contractor personnel shall possess the appropriate IT level of access for the respective task and position assignment as applicable per DoDI 8500.01, DoD Instruction for Cybersecurity. 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.

See section 17.2 Cybersecurity Workforce (CSWF) for the minimum personnel security clearance and Cybersecurity certifications required for each labor category.

8.2.2 Access Control of Contractor Personnel

8.2.2.1 Physical Access to Government Facilities and Installations

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

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

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

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

8.2.2.3 Government Badge Requirements

As specified in contract clause 5252.204-9202, some contract personnel shall require a government issued picture badge. While on government installations/facilities, contractors shall abide by each site's security badge requirements. Various government installations are continually updating their security requirements to meet Homeland Security Presidential Directive (HSPD-12) identification standards. Contractors are responsible for obtaining and complying with the latest security identification requirements for their personnel. Contractors shall submit valid paper work (e.g., site visit request, request for picture badge, and/or SF-86 for Common Access Card (CAC)) to the applicable government security office via the contract COR. The contractor's appointed Security Officer, which is required in clause 5252.204-9200, shall track all personnel holding local government badges at contract or TO 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 Common Access Card (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 DoD Manual (DoDM-1000.13-M-V1), issuance of a CAC is based on the following four criteria:

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

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

3. completion of background vetting requirements according to FIPS PUB 201-2 and DoD Regulation 5200.2-R – at a minimum, the completion of Federal Bureau of Investigation (FBI) fingerprint check with favorable results and submission of a National Agency Check with Inquiries (NACI) investigation to the Office of Personnel Management (OPM), or a DoD-determined equivalent investigation. NOTE: Contractor personnel requiring logical access shall obtain and maintain a favorable National Agency Check with Law and Credit (NACLC) investigation. Contractor personnel shall contact the 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, one document from the Form I-9 list must be a valid (unexpired) State or Federal Government-issued picture identification (ID). The identity documents will be inspected for authenticity, scanned, and stored in the DEERS.

(b) When a contractor requires logical access to a government IT system or resource (directly or indirectly), the required CAC will have a Public Key Infrastructure (PKI). A hardware solution and software (e.g., ActiveGold) is required to securely read the card via a personal computer. Pursuant to DoDM 1000.13-M-V1, CAC PKI certificates will be associated with an official government issued e-mail address (e.g. .mil, .gov, .edu). Prior to receipt of a CAC with PKI, contractor personnel shall complete the mandatory Cybersecurity Awareness training and submit a signed System Authorization Access Request Navy (SAAR-N) form to the contract's 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 Assurance Management (IAM) office:

1. For annual DoD Cybersecurity/IA Awareness training, contractors shall use this site: https://twms.nmci.navy.mil/. For those contractors requiring initial training and do not have a CAC, contact the SPAWARSYSCEN Atlantic IAM 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/index2.html.

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

8.2.2.5 Contractor Check-in and Check-out Procedures

All 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. At contract award throughout contract completion, the contractor shall provide necessary employee information and documentation for employees hired, transferred, and/or terminated in support of this contract within the required timeframe as cited in the Check-in and Check-out instructions. Contractor's Security Officer shall ensure all contractor employees whose services are no longer required on contract return all applicable government documents/badges to the appropriate government representative. NOTE: If the contractor does not have access to the SPAWAR COG website, the contractor shall get all necessary instruction and forms from the COR.

8.2.2.6 Accessing Navy Enterprise Resources Planning (ERP) System

Contractor personnel to perform work under this task order shall require access to Navy Enterprise Resource Planning (Navy ERP) Management System for certain tasks. Prior to accessing any Navy ERP System, contractor personnel shall contact the task order COR or Contracting Officer to obtain the applicable Navy, Marine Corps Internet (NMCI) Assistant Customer Technical Representative (ACTR) who can assign each personnel with an NMCI account. ACTRs can be found on the NMCI Homeport website at: https://nmcicustomerreporting/CTR_Lookup/index.asp.

After an NMCI account has been established, the contractor shall submit a request for Navy ERP access and the role required via the COR to the Competency Role Mapping point of contact (POC). The task order COR will validate the need for access, ensure all prerequisites are completed, and with the assistance of the Role Mapping POC, identify the Computer Based Training requirements needed to perform the role. Items to have been completed prior to requesting a role for Navy ERP include:

System Authorization Access Request Navy (SAAR-N) (DD Form 2875, Aug 2009),

Annual Information Assurance (IA) training certificate, and

Questionnaire for Public Trust Positions, Standard Form 85P

For directions on completing the Questionnaire for Public Trust Positions, the contractor is instructed to consult with its company's Security Officer. Pursuant to DFARS clause 252.239-7001 and DoDD 8570.01, contractor personnel performing IA functions shall meet additional information assurance (IA) training certification, and tracking requirements in accordance with DoD 8570.01-M prior to accessing DoD information systems. Personnel tracking information, which includes subcontractor personnel, shall be included in the monthly task order status report.

(a) For directions on completing the SF85P, the contractor is instructed to consult with its company's Security Manager. In order to maintain access to required systems, the contractor shall ensure completion of annual IA training, monitor expiration of requisite background investigations, and initiate re-investigations as required.

(b) For DoD Information Assurance Awareness training, contractor shall use this site:

http://iase.disa.mil/index2.html.

Directions (Subject to Change): On the right side under "IA Training:" select

"IA Training Available Online". On the next page select the frame with "DoD Information Assurance Awareness".

When the next page comes up, select "Launch DoD Information Assurance Awareness".

8.2.3 IT Position Categories

Positions that 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 require 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. Assignment to designated IT-I positions requires U.S. citizenship unless a waiver request is approved by CNO. IT-1 roles include:

a. Boundary Devices Management (proxies, firewalls, traffic analyzers, VPN Gateways)

b. Intrusion Detection/Prevention Systems (IDS/IPS)

c. Host Based Security Systems (HBSS)

d. Network infrastructure (routers, switches, enterprise wireless)

e. Domain and Authentication System Administrators (i.e., Active Directory, LDAP, Kerberos) (enclave wide scope)

f. Vulnerability Scanner Operators (i.e., Retina, ACAS, HP Web Inspect)

g. Virtualization Technology Administrators that host any of the above (i.e., ESX, Solaris Zones)

8.2.3.2 IT-II Level (Limited Privileged)

Is required for Positions in which the incumbent is responsible for the-direction, planning, design, operation, or maintenance of a computer system, have privileged access to assets and systems that are tenants on LANT networks and/or similar system constructs and whose work is technically reviewed by a higher authority at the IT-II Position level to insure the integrity of the system. Personnel whose duties meet the criteria for an IT-II Position require a favorably adjudicated Tier 3 (T3) investigation (formerly National Agency Check with Law and Credit (formerly ANACI/NACLC). Assignment to designated IT-II positions requires U.S. citizenship unless a waiver request is approved by CNO. Examples of IT-II roles include:

- Webserver Administrators
- Developers
- Testers
- Database Administrators

8.2.3.3 IT-III Level (Non-privileged)

All other positions involved in computer activities. Incumbent 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 require a favorably adjudicated Tier 1 (T1) investigation National Agency Check with Written Inquiries (formerly NACI).

8.2.3.4 Information Assurance Contractor Training and Certification

The Contractor shall ensure that personnel accessing information systems have the proper and current information assurance certification to perform information assurance functions in accordance with DoD 8570.01-M, Information Assurance Workforce Improvement Program. The Contractor shall meet the applicable information assurance certification requirements, including—

(1) DoD-approved information assurance workforce certifications appropriate for each category and level as listed in the current version of DoD 8570.01-M; and

(2) Appropriate operating system certification for information assurance technical positions as required by DoD 8570.01-M.

Upon request by the Government, the Contractor shall provide documentation supporting the information assurance certification status of personnel performing information assurance functions.

Contractor personnel who do not have proper and current certifications shall be denied access to DoD information systems for the purpose of performing information assurance functions.

8.2.3.4 Computing Environment (CE) Certification Requirement

The Contractor shall ensure that personnel accessing information systems have the proper and current information assurance baseline certifications to perform information assurance functions in accordance with DoD 8570.01-M, Information Assurance Workforce Improvement Program. The Contractor shall meet the applicable information assurance certification requirements, IATs with privileged access must obtain appropriate Computing Environment (CE) certifications for the operating system(s) and/or security related tools/devices they support as required by their employing organization. If supporting multiple tools and devices, an IAT should obtain CE certifications for all the tools and devices they are supporting. At a minimum the IAT should obtain a certification for the tool or device he or she spends the most time supporting.

8.2.4 Security Training

Regardless of the task order security level required, the contractor shall be responsible for verifying applicable personnel (including subcontractors) receive all required training. At a minimum, the contractor's designated Security Officer shall track the following information: security clearance information, dates possessing Common Access Cards, issued & expired dates for SSC Atlantic Badge, Cybersecurity training, Privacy Act training, Personally Identifiable Information (PII) training, and Cyber Security Workforce (CSWF) certifications. 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 5220.22M.

8.2.5 Disclosure of Information

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

8.2.6 Handling of Personally Identifiable Information (PII)

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

8.3 OPERATIONS SECURITY (OPSEC) REQUIREMENTS

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

8.3.1 Local and Internal OPSEC Requirement

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

8.3.2 OPSEC Training

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

8.3.3 SSC Atlantic OPSEC Program

Contractor shall participate in SSC Atlantic OPSEC program briefings and working meetings as required, 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 task order shall have specific OPSEC requirements listed on the DD Form 254.

8.4 DATA HANDLING AND USER CONTROLS

8.4.1 Data Handling

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

8.4.2 Effective Use of Controls

The contractor shall screen all electronic deliverables or electronically provided information for malicious code using DoD approved anti-virus software prior to delivery to the Government. The contractor shall utilize appropriate controls (firewalls, password protection, encryption, and digital certificates) 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. This includes ensuring that 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 7.3.2.1, 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.

9.0 GOVERNMENT FACILITIES

Government facilities (i.e., office space, computer hardware/software, or lab space) will be provided to those labor categories that would otherwise adversely affect the work performance if they were not available on-site. All Contractor personnel with supplied Government facilities shall be located at SSC Atlantic in Charleston, SC. Note: *The burdened labor rate for those contractor personnel designated as "Government site" shall include overhead costs allocable to Government site work, consistent with the contractor's established accounting practices.*

10.0 CONTRACTOR FACILITIES

A significant portion of the work under this task order will require close liaison with the Government with attendance at meetings required with reasonable notification. The contractor shall be prepared to establish a local facility within a thirty (30)-mile radius of SSC Atlantic in Charleston, SC. Close proximity allows for proper task order administration duties. The contractor's facility is not necessary for the exclusive use of this task order and can be utilized on a shared basis. The Charleston local facility shall include sufficient physical security to protect Government assets. The contractor's facility shall meet all location and size requirements to perform work requirements within 30 days after task order award. Facility space shall include offices, conference rooms, lab work, and a staging area for materials and equipment, as required.

11.0 TASK ORDER PROPERTY ADMINISTRATION

Contract property is either intangible (i.e., intellectual property and software IAW FAR Part 27) or tangible (i.e., Government property IAW FAR Part 45). The contractor shall have established property management procedures and an appropriate property management point of contact who shall work with the Government Property Administrator (PA) to ensure their property management system is acceptable. This task order will have the following property in support of the tasking requirements in PWS Para 3.0.

11.1 Government Furnished Information (GFI)

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

GFI will be utilized on this task order. For project specific and applicable documents (PWS Para 16.0) not available online, the Government will provide the GFI listed in the table below in an authorized Government repository. The contractor shall inventory all GFI by tracking distribution and location and provide a GFI inventory to the Government. The contractor shall use the GFI provided to support this TO only – use of GFI document(s) to support other projects beyond this TO is not allowed. Unless otherwise specified, all GFI will be provided by the Government by the estimated delivery date listed in the table below, and the contractor shall return all GFI to the Government at completion of the TO. If a contractor requires additional GFI other than what is listed, the contractor shall submit a request to the COR within 30 days after TO award.

Item #	Description	GFI Estimated Delivery Date
1	Extract, Transform and Load Scripts	30 days after award
2	Extract, Transform and Load SAP Data Services Scripts	30 days after award
3	Extract, Transform and Load scripts or configuration data from other automated tools	30 days after award

11.2 Government Property (GP)

As defined in FAR Part 45, Government Property (GP) is property owned or leased by the Government which includes material, equipment, special tooling, special test equipment, and real property.

NOTE: NMCI computers will be assigned to a contractor. Prior to a NMCI computer being removed from a Government facility, the contractor employee shall possess at all times a Property Pass (OF-7) with each NMCI asset that will be authorized and signed by the COR or

other authorized Government personnel. Although NMCI assets are not tracked as GFP, the contractor shall separately track and report all NMCI assets assigned to all contractor employees for use on this TO. For reporting purposes, the contractor shall include a list of NMCI assets assigned to this TO (separate from the GFP inventory list) in the TO status report (CDRL A008).

Government Property includes both GFP and CAP. Government Property does not include intellectual property and software. The contractor shall have established property management procedures and an appropriate property management point of contact who shall work with the assigned Government Property Administrator (PA) to ensure their property management system is acceptable.

11.2.1 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, but is not limited to, 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).

The use of GFP on this TO is authorized in accordance with DFARS requirements. The contractor shall meet applicable FAR requirements for the use and charges of GFP. The contractor shall have the means to provide an effective and efficient stewardship of Government Property. NOTE: The contractor shall only receive items listed in the Consolidated GFP form and shall only take possession of items not in excess of the maximum promised quantity identified in the GFP form. If additional items or increased quantities are required, a modification to the TO must occur. A revised GFP form will be submitted in support of the modification, and the GFP form will be uploaded to EDAas an attachment to the TO modification. Previously uploaded GFP forms associated with the same task order will be retained in EDA as well. The following types of GFP are applicable on this TO:

11.2.1.1 Government Furnished Equipment (GFE)

GFE is Property, Plant and Equipment (PP&E) provided to the contractor. It consists of tangible items that are functionally complete for their intended purpose, durable, non-expendable, and needed for the performance of a contract. It is not intended for sale and does not ordinarily lose its identity or become a component part of another article when put into use. It does not include material, real property, special test equipment or special tooling. GFE will be provided to the contractor as identified on the Consolidated GFP form, Attachment 4..

GFE issued under this task order includes computers furnished to a contractor for use within a Government facility and are typically laptops (vs. a desktop) and are non-NMCI (utilizes the RDT&E network or is task-owned). Because these laptops are designed for portability and may be required away from Government facilities during performance of the contract; therefore, they shall be noted as GFP (per DoN direction).

11.2.2 Government Furnished Material (GFM)

No GFM will be provided on this TO.

11.2.3 Special Test Equipment (STE)

No STE will be provided on this TO

11.2.4 Special Tooling (ST)

No ST will be provided on this TO.

11.2.1 GFP REPORTING AND TRACKING

All GFP shall be tracked in the Contractor's Property Management System as required by FAR clause 52.245-1 and DFARS clause 252.245-7003. The contractor shall comply with the GFP reporting requirements of DFARS clause 252.211-7007. The primary and preferred means to do this is via electronic transfer transaction reporting in Invoicing, Receipt, Acceptance, and Property Transfer (iRAPT), an application within Wide Area Workflow (WAWF). This will automatically update the GFP records in the Item Unique Identification Registry's GFP Repository. Subsequent transactions affecting GFP custody must also be reported for serially-managed GFP items. As part of the TOSR (CDRL A008) requirements, the contractor shall provide a monthly GFP listing of items physically on-hand.

11.3 CONTRACTOR ACQUIRED PROPERTY (CAP)

No CAP is anticipated on this TO

11.4 GOVERNMENT PROPERTY MANAGEMENT

11.4.1 Contractor Property Management System

Pursuant to FAR clause 52.245-1 and DFARS clause 252.245-7003 & 252.211-7007, the contractor shall establish and maintain an acceptable property management system for both GFP and CAP that is subject to review and approval by the Contracting Officer and contract Government Property Administrator. The contractor's property management system shall adhere to the applicable prescribed requirements in FAR clause and include the required data elements in DFARS clause. The contractor shall ensure GFP in the possession of a subcontractor if applicable shall also be reported using the required data elements cited in DFARS clause.

11.4.2 Government Property Administrator

Pursuant to FAR Subpart 42.201 (Contract Administration Responsibilities), the contract property administrator under this contract is designated as Defense Contract Management Agency (DCMA). The contractor shall work with the designated contract property administrator to ensure compliance with the contract's property requirements.

11.4.3 Government Property Records

Pursuant to *FAR clause 52.245-1 & DFARS clause 252.211-7007*, contractors and any subcontractors, if applicable, shall be responsible for establishing and maintaining records of Government Property in their possession – this includes GFP and CAP. The contractor shall ensure GFP and CAP records contain, at a minimum, the data elements as described in the FAR and GFP records also contain the data elements specified in the DFARS.

11.4.3.1 NMCI computers will be assigned to a contractor.

Prior to a NMCI computer being removed from a Government facility, the contractor employee shall possess at all times a Property Pass (OF-7) with each NMCI asset that will be authorized and signed by the COR or other authorized Government personnel. Although NMCI assets are not tracked as GFP, the contractor shall separately track and report all NMCI assets assigned to all contractor employees for use on this TO. For reporting purposes, the contractor shall include a list of NMCI assets assigned to this TO (separate from the GFP inventory list) in the TO status report (CDRL A008).

11.4.3.2 Requirement to Retain DD Form 1149

For all GFP items including laptops (identified on the Consolidated GFP form) removed from a Government facility, the contractor employee shall possess at all times a Government signed copy of the DD1149 specifying contract and applicable TO number, company name, model number, and serial number of the computer. For GFP laptops assigned to contractor employees, in addition to the signed DD1149, a contractor-generated property pass with the employee's name may be attached to validate possession in accordance with applicable company internal procedures.

11.5.1 Government Property Transferring Accountability

GFP cannot be transferred between contracts or task orders unless approval is obtained from the Contracting Officer, proper identification/tracking is maintained, and modifications are issued to both affected contracts and/or task orders. Contractor shall ensure they have all necessary documentation required for authorized transfer of property from one contract/task order to another. The contractor shall ensure transfer documentation specifies the type, quantity and acquisition cost of each item being transferred.

11.5.2 Government Property Lost or Damaged Items

Pursuant to Insert DFARS clause 252.245-7002,. The contractor shall promptly report to the COR and Contracting Officer all lost and/or damaged Government property. The requirements and procedures for reporting lost Government Property are specified in DFARS clause.

11.5.3 Government Property Inventory Disposition

When disposition instructions for GFP are contained in the accountable contract or on the supporting shipping documents (DD Form 1149), the Contractor shall initiate and submit an excess inventory listing to the Procuring Contracting Officer (PCO), via the activity Property Administrator.

Pursuant to *DFARS clause 252.245-7004,* when disposition instructions are not stipulated in the contract or supporting shipping document (DD Form 1149), an excess inventory listing is required that identifies GFP and, under cost reimbursement contracts, CAP. The contractor shall submit the list to the COR and PCO, via the activity Property Administrator, at which time disposition instructions will be provided by the Government. Note: If any Government Property is slated for demilitarization, mutilation, or destruction by the contractor, the event shall be witnessed and verified by the COR or the designated Government personnel.

When GFP and CAP are specific to a single task order, the contractor shall include a final inventory reporting list in the TO Closeout Report (CDRL A009). At the time of the contractor's regular annual inventory, the contractor shall provide the PCO, via the assigned Property Administrator, a copy of the physical inventory listing. All contractor personnel shall be responsible for following the company's internal inventory management procedures and correcting any problems noted by the Government Property Administrator.

11.5.4 Government Property Performance Evaluation

Non-compliance with the contract's Government Property terms and conditions will negatively affect the contractor's annual Contractor Performance Assessment Reporting System (CPARS) rating.

11.6 TRANSPORTATION OF EQUIPMENT/MATERIAL

No transportation of equipment/material is required by the contractor on this TO.

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 the respective task orders under this contract. 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.

12.1.1 Performance at government facilities

In addition to complying to clause 5252.223-9200 Occupational Safety and Health Requirements, the 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 contracting officer.

13.0 TRAVEL

13.1 LOCATIONS

The contractor shall ensure all travel is performed pursuant to clause 5252.231-9200. For planning purposes, the contractor shall provide adequate personnel to support the travel requirements listed below. The proposed estimated travel cost cannot exceed the not-to-exceed (NTE) value cited in the applicable pricing model. Travel estimates are in accordance with the latest Joint Travel Regulations (JTR) for DoD Civilian Personnel. Note: During the request for proposal (RFP) phase, a contractor may propose an alternate Travel value less than the NTE value in the pricing model, but the proposal must contain substantiating information validating the cost differential; if no validation is provided, the proposal material cost will be adjusted to government proposed NTE value.

Base Year, Project 1

# Trips	# People	# Days/Nights	From (Location)	To (Location)
2	1	5/4	Charleston, SC	San Diego, CA

Option 1, Project 1

# Trips	# People	# Days/Nights	From (Location)	To (Location)
2	1	5/4	Charleston, SC	San Diego, CA

Option 2, Project 1

# Trips	# People	# Days/Nights	From (Location)	To (Location)
2	1	5/4	Charleston, SC	San Diego, CA

Option 3, Project 1

# Trips	# People	# Days/Nights	From (Location)	To (Location)
2	1	5/4	Charleston, SC	San Diego, CA

Option 4, Project 1

# Trips	# People	# Days/Nights	From (Location)	To (Location)
2	1	5/4	Charleston, SC	San Diego, CA

Note: Travel specifically to Iraq or Afghanistan shall not be performed under this contract.

14.0 COR DESIGNATION

The Contracting Officer Representative (COR) for this task order is [redacted]

15.0 TRANSPORTATION OF EQUIPMENT/MATERIAL

Transportation of equipment and/or material is applicable for the noted GFP and is the responsibility of the contractor; the cost shall be included in the proposal.

Government-furnished Property (GFP), GFP may be technically refreshed (replaced) anytime on a three to five year cycle to meet information assurance or sustainment requirements.

16.0 ACCEPTANCE PLAN

Inspection and acceptance is performed by the COR on all services, data, and non-data deliverables in accordance with the Quality Assurance Surveillance Plan (QASP), Attachment 1.

17.0 OTHER CONDITIONS/REQUIREMENTS

The contractor shall meet all the general operating requirements listed below:

a. The contractor personnel shall be familiar with all documents listed in TO PWS Paragraph 3.0, and adhere to the applicable portions of each document in the performance of these tasks.

b. All communications (written or oral) with accrediting officials shall be by the SSC Atlantic

c. Personnel unless prior authorization is granted in writing from SSC Atlantic COR.

d. The contractor's working hours shall conform to the normal work hours of the site. The contractor may request, in writing, deviations in work hours if required in advance. SSC Atlantic COR will review the requests and approval will be granted if acceptable to site personnel.

e. Contractor personnel shall wear an appropriate nametag indicating the company and employee name while working on site.

f. Contractor vehicles shall be properly identified.

17.1 DATA RIGHTS

The Government has unlimited rights to all documents/material produced under this contract. All documents and materials, to include the source codes of any software, produced under this contract shall be Government owned and are the property of the Government with all rights and privileges of ownership/copyright belonging exclusively to the Government. These documents and materials may not be used or sold by the contractor without written permission from the Contracting Officer. All materials supplied to the Government shall be the sole property of the Government and may not be used for any other purpose. This right does not abrogate any other Government rights.

17.2 CYBERSECURITY WORKFORCE DESIGNATION

This task order requires contractor personnel to perform cybersecurity functions.

Pursuant to DFAR clause 252.239-7001, DoDD 8140.01 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 SPAWARNote 5239.3B prior to accessing DoD information systems. This applies to sections 3.2, 3.3, 3.5 and 3.6 and their subsections.

The contractor shall be responsible for tracking and reporting cybersecurity personnel, also known as Cyber Security Workforce (CSWF). See PWS Para 5.2.1.3 for CSWF Report reporting requirements. Although the minimum frequency of reporting is monthly, the COR may require additional updates at any time.

Pursuant to DoD 8570.01-M Information Assurance Workforce Improvement Program Manual, the cybersecurity workforce 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. All labor categories (to be determined at time of task order award) providing system administration and extract-transform and load operations shall meet the IA Designator Level II as a Primary Duty. The following Labor Categories shall meet the IA Designator, IA Level/Position, and have the estimated Primary/Additional/Embedded hours performing IA duties:

Table 1: Cybersecurity Workforce Requirements

Project / Labor Category	Quantity Personnel	IA Designator (Note1)	IA Level/Position (Note2)	IA Duty Hours (Note3)	IA Cert (Note4)	OS/OE or Trng Cert (Note5)
1 / Computer Systems Analyst III (SCA 14103)	(1)	IAT	Level 2	Primary	Security+	Server+ or Linux
2 / Computer Systems Analyst II (SCA 14102)	(1)	IAT	Level 2	Primary	Security+	Server+ or Linux

Notes:

1: (select one) IAT, IAM, IASAE, CNDSP

2: (select one) Level 1, Level 2, Level 3, CND-A, CND-IS, CND-IR, CND-AU, CND-SPM

3: (select one) Primary (≥25 hrs), Additional (15-24 hrs), Embedded (1-14 hrs)

4: (select one) SSCP, GSEC, Security+, SCNP, CISA, GSE, SCNA, CISSP

5: If not specified: Windows, Linux or Server +

17.3 PRIVACY ACT REQUIREMENTS

Data Warehouse Business Intelligence System (DWBIS) and its successor business intelligence systems shall each be considered a System of Records while performing work under this Task Order.

17.3.1 Privacy Act Notification

In accordance with FAR clause 52.224-1:

The Contractor shall be required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the Privacy Act of 1974, Public Law 93579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties.

17.3.2 Privacy Act

In accordance with clause 52.224-2:

(a) The Contractor shall:

(1) Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the task order specifically identifies

(i) The systems of records; and

(ii)The design, development, or operation work that the contractor is to perform;

(2) Include the Privacy Act notification contained in this task order in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the design, development, or operation of a system of records on individuals that is subject to the Act; and

(3) Include this clause, including this subparagraph (3), in all subcontracts awarded under this task order which requires the design, development, or operation of such a system of records.

(b) In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a system of records on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a system of records on individuals to accomplish an agency function. For purposes of the Act, when the task order is for the operation of a system of records on individuals to accomplish an agency function, the Contractor and any employee of the Contractor is considered to be an employee of the agency.

(c) For Systems of Record,

(1) Operation of a system of records, as used in this clause, means performance of any of the activities associated with maintaining the system of records, including the collection, use, and dissemination of records.

(2) Record, as used in this clause, means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and that contains the person's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint or voiceprint or a photograph.

(3) System of records on individuals, as used in this clause means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

17.4 HANDLING PERSONALLY IDENTIFYING INFORMATION (PII)

Work under this task order requires access to Personally Identifying Information (PII) as defined under the Privacy Act. This information may not be discussed or disclosed to unauthorized persons as required by paragraph 8.2.4 of this task order.

17.5 Non-Disclosure Agreement (NDA) Requirements

All persons performing work that requires access to Government data designated UNLASSIFIED / SENSITIVE, is Procurement Sensitive or subject to Privacy Act shall be required to sign Agency provided nondisclosure agreements prior to being authorized access to any sensitive data.

The Contractor shall appoint an officer within the Company who is authorized to bind the Company to the terms of the signed non-disclosure agreements executed by each employee or subcontractor (Attachment).

As a condition to receiving access to sensitive data, the Contractor shall:

(a) Prior to having access to proprietary data, obtain the agreement of the applicable person or entity to permit access by the Contractor to such data.

(b) Use the data solely for the purpose of performing duties under this Task Order.

(c) Not discuss with, disclose, release, reproduce or otherwise provide or make available the data, or any portion thereof, to any employee of the contractor unless and until each person and the appointed officer of the Company has executed a copy of the individual non-disclosure agreement.

(d) Not discuss with, disclose, release, reproduce or otherwise provide or make available the data, or any portion thereof, to any non-Government person or entity (including, but not limited to any subcontractor, joint venture, affiliate, successor or assignee of the contractor), unless the KO (and any contractor claiming the data is proprietary) have given prior written approval, and the person receiving the data has executed an individual non-disclosure agreement.

(e) Establish safeguards to protect such data or software from unauthorized use or disclosure.

(f) Indoctrinate its personnel who will have access to the data as to the restrictions under which access is granted. Any other use, disclosure, release or reproduction is unauthorized and may result in substantial criminal, civil and/or administrative penalties to the contractor or to the individual who violates this special task order requirement or non-disclosure agreement.

(g) Apply appropriate restrictive legends on any copies and reproductions made of all or any part of the data and any data that is derived from, based upon, incorporate, include or refer to the data. When the Contractor's need for such data ends, the data shall be returned promptly (within ten (10) business days) to the appropriate Government program personnel. However, the obligation not to discuss, disclose, release, reproduce or otherwise provide or make available such data, or any portion thereof, shall continue, even after completion of this contract/order. Any actual or suspected unauthorized use, disclosure, release, or reproduction of such data or violation of this agreement, of which the company or any employee is or may become aware, will be reported promptly (within one (1) business day) to the contractor's program manager, who will inform the KO within five (5) business days of receiving the report.

17.6 EXTENDED WORK WEEK

Work under this order will be done during normal working hours when practical. However, due to operational requirements, schedules, and the availability of required resources and/or downtime of those resources, extended hours including weekend work may be required.

Approval from the COR is required prior to any extended work week performance.

17.7 CONTRACT ORGANIZATIONAL CONFLICT OF INTEREST (OCI)

Due to the type of work performed, there are organizational conflict of interest clauses that are applicable to this task order. The contractor shall follow the restrictions as cited in clause 5252.209-9203.

In accordance with clause 5252.209-9203 of this task order, the Contractor shall submit an organizational conflict of interest mitigation plan (CDRL A017) that is acceptable to the Government before being authorized access to sensitive or proprietary data under this Task Order.

17.8 FUNDING ALLOCATION

This TO 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 TO award. Unless otherwise advised, the contractor shall itemize all summary of work and financial information in the TOSR CDRL by each TO funding CLIN. The ability of the contractor to perform adequate billing and accounting will be reflected in the contractor's annual Government Contractor Performance Assessment Report (CPAR) rating.

LIST OF ATTACHMENTS

See Section J.

[END OF PWS]

5252.237-9600 PERSONNEL QUALIFICATIONS (MINIMUM) (JAN 1992)

(a) Personnel assigned to or utilized by the Contractor in the performance of this task order shall, as a minimum, meet the experience, educational, 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 the contract, 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. 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.

Labor Categories and Minimum Requirements

1. Program Manager

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

Experience: Fifteen (15) years of technical experience in support of Information technology services and cyber security, to include: Equipment Support, System Support, and Programmatic Support. Eight (8) years of Program Management experience, to include: [redacted]chnology Assessments, Systems Design, Systems Analysis, Programmatic Support, Acquisition Planning, and Budget Planning. Five (5) years as manager for information technology services in a DoD Cybersecurity environment. Note: Experience may be concurrent. Knowledge of Federal Acquisition Regulation (FAR) and DoD procurement policies and procedures.

2. Project Manager

Education: BS degree in Physical Sciences, Mathematics, Management Information Systems, or Business or other IT or Cyber related fields.

Experience: Ten (10) years of direct work experience with information technology services and cyber security. Eight (8) years of direct work experience, to include: Design, Development, Production, Installation, and Test & Evaluation of enterprise IT and cyber security. Four (4) years as manager of enterprise IT, cyber security, or data center management in a DoD Cybersecurity environment, to include: Supervising Project Personnel, Scheduling Work, Writing Proposals and Preparing Bids, and Equipment and Material Logistics Control. Note: Experience may be concurrent. Knowledge of Federal Acquisition Regulation (FAR) and DoD procurement policies and procedures.

3. Computer Systems Analyst III (SCA 14103) (Extract, Transform and Load (ETL) Lead) (Key)

Clearance: Candidates MUST be eligible for a Public Trust clearance within the Department of Defense.

Cybersecurity Workforce: Candidates MUST be certified as IT Level 2, IAT Level 2

Education: Technical Training in information technology and cyber security

Ten (10) years of hands-on experience as a programmer, data analyst or computer script writer in a multi-user production environment, with five (5) years of experience managing daily schedules and processes to lead a production team charged to perform data extract, transformation, validation and load operations for business systems to meet production schedules. Recognized expert for daily operations.

4. Computer Systems Analyst III (SCA 14103) (Extract, Transform and Load (ETL) Operator)

Clearance: Candidates MUST be eligible for a Public Trust clearance within the Department of Defense.

Cybersecurity Workforce: Candidates MUST be certified as IT Level 2, IAT Level 2

Education: Technical Training in information technology and cyber security

Three (3) years of hands-on experience as a programmer, data analyst or computer script writer in a multi-user production environment.

5252.237-9601 KEY PERSONNEL (VARIATION)

(a) The offeror agrees to assign to this task order task order those key personnel listed in paragraph (d) below. No substitutions shall be made except in accordance with this clause.

(b) The offeror agrees that during the first 180 days of the task order task order performance period no personnel substitutions will be permitted unless such substitutions are necessitated by an individual's sudden illness, death or termination of employment. In any of these events, the contractor shall promptly notify the Contracting Officer and provide the information required by paragraph (c) below. After the initial 180 day period, all proposed substitutions must be submitted in writing, no more than thirty (30) in advance of the proposed substitutions to the contracting officer. The contractor shall provide any substitution requests in accordance with paragraph (c) below.

(c) All requests for approval of substitutions under this task order must be in writing and a detailed explanation of the circumstances necessitating the proposed substitutions. They must contain a complete resume for the proposed substitute or addition, and any other information requested by the Contracting Officer or needed by him to approve or disapprove the proposed substitutions. All substitutions proposed during the duration of this task order must have qualifications of the person being replaced. The Contracting Officer or his authorized representative will evaluate such requests and promptly notify the contractor of his approval or disapproval thereof in writing.

(d) List of Key Personnel

#	NAME	Labor Category	Effective Date
1	Extract, Transform and Load (ETL) Automation Lead	Computer Systems Analyst III (SCA 14103)	On Award

After task order award, the contractor shall be responsible for tracking and maintaining the Key Personnel list which is part of the monthly Task Order Status Report.

(e) If the Contracting Officer determines that suitable and timely replacement of key personnel who have been reassigned, terminated or have otherwise become unavailable for the task order work is not reasonably forthcoming or that the resultant reduction of productive effort would be so substantial as to impair the successful completion of the task order or the service order, the task order may be terminated by the Contracting Officer for default or for the convenience of the Government, as appropriate. In addition, if the Contractor is found at fault for the condition, the Contracting Officer may elect to equitably decrease the task order price or fixed fee to compensate the Government for any resultant delay, loss or damage. The contractor's ability to manage, provide, and/or maintain sufficient key personnel will be evaluated in the annual government Contractor Performance Assessment Report (CPAR) rating.

(f) To request personnel be added to a labor category, the offeror shall employ the procedures outlined in paragraph (c) above. Adding personnel will only be permitted in the event of an indefinite quantity contract, where the Government has issued a delivery order for labor hours that would exceed a normal forty hour week if performed only by the number of employees originally proposed.

(End of clause)

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 COR.

CLAUSES INCORPORATED BY REFERENCE

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:

7000	3/27/2018 - 3/26/2019
7001	3/27/2018 - 3/26/2019
7100	3/27/2019 - 3/26/2020
7101	3/27/2019 - 3/26/2020
9000	3/27/2018 - 3/26/2019
9100	3/27/2019 - 3/26/2020

CLIN - DELIVERIES OR PERFORMANCE

Base Year: Date of award through one year thereafter.

Option Years: Date of Option Exercise through twelve months thereafter.

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".

CLAUSES INCORPORATED BY REFERENCE

52.242-15 Alt I Stop-Work Order (Aug 1989) - Alternate I APR 1984

SECTION G CONTRACT ADMINISTRATION DATA

The SPAWAR Atlantic Ombudsman is [redacted].

252.204-0002 LINE ITEM SPECIFIC: SEQUENTIAL ACRN ORDER. (SEP 2009)

The payment office shall make payment in sequential ACRN order within the line item, exhausting all funds in the previous ACRN before paying from the next ACRN using the following sequential order: Alpha/Alpha; Alpha/numeric; numeric/alpha; and numeric/numeric.

SUBJECT TO CHANGE PRIOR TO TASK ORDER AWARD

(End of clause)

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:

Cost Type Orders - Cost Voucher

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

N65236

(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	S1103A
Inspect By DoDAAC	N65236
Ship To Code	N65236
Ship From Code	N/A
Mark For Code	N65236
Service Approver(DoDAAC)	S1103A
Service Acceptor (DoDAAC)	N/A
Accept at Other DoDAAC	N/A
LPO DoDAAC	N65236
DCAA Auditor DoDAAC	HAA632
Other DoDAAC(s)	N/A

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

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

[redacted]

(g) WAWF point of contact.

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

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

5252.201-9201 Designation of Contracting officer's Representative (Mar 2006)

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

CONTRACTING OFFICER REPRESENTATIVE

Name: [redacted]

Code: [redacted]

Phone Number: [redacted]

E-mail: [redacted]

(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.

5252.216-9210 TYPE OF CONTRACT (DEC 1999)

This is a Cost-Plus-Fixed-Fee, Level of Effort and Cost task order.

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 task order basis, and to submit invoices reflecting costs incurred at that level. Invoices shall contain summaries of work charged during the period covered, as well as overall cumulative summaries by labor category for all work invoiced to date, by line item, task, or subtask.

(b) Where multiple lines of accounting are present, the ACRN preceding the accounting citation will be found in Section G, Accounting Data. 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, Electron Submission of Payment Requests, one copy of each invoice or voucher will be provided, at the time of submission to DCAA

(1) to the Contracting Officer's Representative or the Technical Representative of the Contracting Officer and

(2) to the Procuring Contracting Officer.

Accounting Data

SLINID	PR Number	Amount
700001	130064609100002	[redacted]

LLA :
AA 97X4930 NH3S 251 77777 0 050120 2F 000000 A00004448810
Standard Number: NWCF Overhead
ACRN: AA
PR#: 1300646091
NWA: 300000075062 0020
DOC: NWCF Overhead
Funds Expiration: 09/30/2018

900001 130064609100003 [redacted]
LLA :
AA 97X4930 NH3S 251 77777 0 050120 2F 000000 A00004448810
Standard Number: NWCF Overhead
ACRN: AA
PR#: 1300646091
NWA: 300000075062 0020
DOC: NWCF Overhead
Funds Expiration: 09/30/2018

BASE Funding [redacted]
Cumulative Funding [redacted]

MOD P00001

710001 130076685100001 [redacted]
LLA :
AB 97X4930 NH3S 251 77777 0 050120 2F 000000 A00004897921
Standard Number: NWCF OVHD
PR 1300766851
ACRN AB
Cost Code A00004897921
Funding Doc NWCF OVHD
Funding Expires 9-30-2019
NWA 300000075062 0010

910001 130076685100002 [redacted]
LLA :
AB 97X4930 NH3S 251 77777 0 050120 2F 000000 A00004897921
Standard Number: NWCF OVHD
PR 1300766851
ACRN AB
Cost Code A00004897921
Funding Doc NWCF OVHD
Funding Expires 9-30-2019
NWA 300000075062 0010

MOD P00001 Funding [redacted]
Cumulative Funding [redacted]

SECTION H SPECIAL CONTRACT REQUIREMENTS

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

In performing this task order, 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.

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 task order. The total level of effort for the performance of this task order shall be **22,480** (inclusive of base and option years) 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 **Zero (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, 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 task order shall be expended at an average rate of approximately **86** 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 Task Order 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 Task Order Contracting Officer, shall constitute a binding contract. The Contractor shall not accelerate any effort until receipt of such written approval by the Task Order Contracting Officer. Any agreement to accelerate will be formalized by contract modification.

(f) The Task Order 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 Task Order Contracting Officer, at its sole discretion, shall either (i) reduce the fee of this contract as follows:

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

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 Task Order 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 the 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.

* The Contracting Officer referred to, in paragraph (j), is the Task Order Contracting Officer.

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

(a) Definition.

“Confidential Business Information,” (Information) as used in this clause, is defined as all forms and types of financial, business, economic or other types of information other than technical data or computer software/computer software documentation, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if -- (1) the owner thereof has taken reasonable measures to keep such Information secret, and (2) the Information derives independent economic value, actual or potential from not being generally known to, and not being readily ascertainable through proper means by, the public.

Information does not include technical data, as that term is defined in DFARS 252.227-7013(a)(14), 252.227-7015(a)(4), and 252.227-7018(a)(19). Similarly, Information does not include computer software/computer software documentation, as those terms are defined in DFARS 252.227-7014(a)(4) and 252.227-7018(a)(4).

(b) The Space and Naval Warfare Systems Command (SPAWAR) may release to individuals employed by SPAWAR support contractors and their subcontractors Information submitted by the contractor or its subcontractors pursuant to the provisions of this contract. Information that would ordinarily be entitled to confidential treatment may be included in the Information released to these individuals.

Accordingly, by submission of a proposal or execution of this contract, the offeror or contractor and its subcontractors consent to a limited release of its Information, but only for purposes as described in paragraph (c) of this clause.

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

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

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

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

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

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

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

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

(5) Before releasing the Information to a non-Government person to perform the tasks described in paragraphs (c)(1) and (c)(2), SPAWAR shall provide the contractor a list of the company names to which access is being

granted, along with a Point of Contact for those entities.

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

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

5252.231-9200 REIMBURSEMENT OF TRAVEL COSTS (JAN 2006)--ALTERNATE II (SEP 2001)

(a) Contractor Request and Government Approval of Travel Any travel under this contract must be specifically requested in writing, by the contractor prior to incurring any travel costs. If this contract is a definite or indefinite delivery contract, then the written Government authorization will be by task/delivery orders issued by the Ordering Officer or by a modification to an issued task/delivery order. If this contract is not a definite or indefinite delivery contract, then the written Government authorization will be by written notice of approval from the Contracting Officer's Representative (COR). The request shall include as a minimum, the following:

(1) Contract number

(2) Date, time, and place of proposed travel

(3) Purpose of travel and how it relates to the contract

(4) Contractor's estimated cost of travel

(5) Name(s) of individual(s) traveling and;

(6) A breakdown of estimated travel and per diem charges.

The contractor shall submit the travel request in writing to the Contracting Officer's Representative (COR). The COR shall review and approve/disapprove (as appropriate) all travel requests submitted giving written notice of such approval or disapproval to the contractor.

(b) General

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

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

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

(iii) Standardized Regulations, (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem

Allowances in Foreign Areas" prescribed by the Department of State, for travel in areas not covered in the travel regulations cited in subparagraphs (b)(1)(i) and (b)(1)(ii) above.

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

(c) Per Diem

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

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

(3) Reimbursement to the contractor for per diem shall be limited to payments to employees not to exceed the authorized per diem and as authorized in writing by the Government per paragraph (a). Fractional parts of a day shall be payable on a prorated basis for purposes of billing for per diem charges attributed to subsistence on days of travel. The departure day from the Permanent Duty Station (PDS) and return day to the PDS shall be 75% of the applicable per diem rate. The contractor shall retain supporting documentation for per diem paid to employees as evidence of actual payments, as required by the FAR 52.216-7 "Allowable Cost and Payment" clause of the contract.

(d) Transportation

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

(2) The contractor agrees, in the performance of necessary travel, to use the lowest cost mode commensurate with the requirements of the mission and in accordance with good traffic management principles. When it is necessary to use air or rail travel, the contractor agrees to use coach, tourist class or similar accommodations to the extent consistent with the successful and economical accomplishment of the mission for which the travel is being performed. Documentation must be provided to substantiate non-availability of coach or tourist if business or first class is proposed to accomplish travel requirements.

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

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

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

(6) Definitions:

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

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

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

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

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

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

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

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

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

EXAMPLE 1: 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).Employee’s one way commuting distance to regular place of work is 7 miles. Employee drives from residence to an alternate

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

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 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. Employee’s one way commuting distance to regular place of work is 15 miles. Employee drives to regular place of work.

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: 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. Employee’s one way commuting distance to regular place of work is 12 miles. In the morning the employee drives to an

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: 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).Employee’s one way commuting distance to

regular place of work is 35 miles. Employee drives to the regular place of work (35

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: 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).Employee's one way commuting distance to regular place of work is 20 miles. Employee drives to the regular place of work (20

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.

5252.232-9104 ALLOTMENTOF FUNDS (JAN 2008)

a. This contract is incrementally funded with respect to both cost and fee. The amount(s) presently available and allotted to this contract for payment of fee for incrementally funded contract line item number/contract subline item number (CLIN/SLIN), subject to the clause entitled "FIXED FEE" (FAR 52.216-8) or "INCENTIVE FEE" (FAR 52.216-10), as appropriate, is specified below. The amount(s) presently available and allotted to this contract 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/SLINs covered thereby, and the period of performance for which it is estimated the allotted amount(s) will cover are as follows:

TO Ceiling	Funded Amount	Unfunded Amount	Period of Performance
$[redacted]	$[redacted]	$[redacted]	27 MAR 18 - 26 MAR 19
	$[redacted]	$[redacted]	27 MAR 19 - 26 MAR 20

b. The parties contemplate that the Government will allot additional amounts to this contract from time to time for the incrementally funded CLINs/SLINs by unilateral contract 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 _____are fully funded and performance under these CLINs/SLINs is subject to the clause of this 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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(g) 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.

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 performance information on defense contractors as required by FAR 42.1502 (Class Deviation 2013-O0018). The 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 https://www.cpars.gov/cparsfiles/pdfs/CPARS-Guidance.pdf.

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

SECTION I CONTRACT CLAUSES

CLAUSES INCORPORATED BY REFERENCE

52.219-6	**Notice of Total Small Business Set-Aside**	**NOV 2011**
252.211-7006	**Passive Radio Frequency Identification**	**JUN 2016**
252.246-7006	**Warranty Tracking of Serialized Items**	**MAR 2016**
52.251-1	**Government Supply Sources**	**APR 2012**

09RA 52.217-9 -- Option to Extend the Term of the Contract. (mar 2008)

(a) The Government may extend the term of this contract 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 contract expires. The preliminary notice does not commit the Government to an extension.

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

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

52.222-2 -- Payment for Overtime Premiums. (Jul 1990)

(a) The use of overtime is authorized under this contract if the overtime premium does not exceed __0__ or the overtime premium is paid for work –

(1) Necessary to cope with emergencies such as those resulting from accidents, natural disasters, breakdowns of production equipment, or occasional production bottlenecks of a sporadic nature;

(2) By indirect-labor employees such as those performing duties in connection with administration, protection, transportation, maintenance, standby plant protection, operation of utilities, or accounting;

(3) To perform tests, industrial processes, laboratory procedures, loading or unloading of transportation conveyances, and operations in flight or afloat that are continuous in nature and cannot reasonably be interrupted or completed otherwise; or

(4) That will result in lower overall costs to the Government.

(b) Any request for estimated overtime premiums that exceeds the amount specified above shall include all estimated overtime for contract completion and shall –

(1) Identify the work unit; e.g., department or section in which the requested overtime will be used, together with present workload, staffing, and other data of the affected unit sufficient to permit the Contracting Officer to evaluate the necessity for the overtime;

(2) Demonstrate the effect that denial of the request will have on the contract delivery or performance schedule;

(3) Identify the extent to which approval of overtime would affect the performance or payments in connection with other Government contracts, together with identification of each affected contract; and

(4) Provide reasons why the required work cannot be performed by using multishift operations or by employing

additional personnel.

* Insert either “zero” or the dollar amount agreed to during negotiations. The inserted figure does not apply to the exceptions in subparagraph (a)(1) through (a)(4) of the clause.

(End of Clause)

52.222-42 -- Statement of Equivalent Rates for Federal Hires (May 2014)

In compliance with the Service Contract Labor Standards statute and the regulations of the Secretary of Labor (29 CFR part 4), this clause identifies the classes of service employees expected to be employed under the contract and states the wages and fringe benefits payable to each if they were employed by the contracting agency subject to the provisions of 5 U.S.C. 5341 or 5332.

This Statement is for Information Only:
It is not a Wage Determination

EMPLOYEE CLASS	**MONETARY WAGE -- FRINGE BENEFITS**
COMPUTER SYSTEMS ANALYST III (SCA 14103)	$67.00

SECTION J LIST OF ATTACHMENTS

Attachment 1 - QASP

Attachment 2 - DD254

Attachment 3 - WD_15-4427rev6 - Charleston, SC

Attachment 4 - Gov SGFP Form

Exhbit A - DD1423 - CDRLs