ORDER FOR SUPPLIES OR SERVICES

PAGE 1 OF 57

1. CONTRACT/PURCH ORDER/ AGREEMENT NO.	2 DELIVERY ORDER/ CALL NO	3 DATE OF ORDER/CALL (YYYYMMMDD)	4 REQ / PURCH REQUEST NO	5 PRIORITY
GS00Q14OADU341	N6893619F0020	2018 Oct 16	1300748386	

6. ISSUED BY CODE N68936
CDR NAWCWD CODE 254500E
ATTN: (b)(6)
(b)(6)
429 E BOWEN RD STOP 4015
CHINA LAKE CA 93555

7. ADMINISTERED BY *(if other than 6)* CODE S0107A
DCMA HUNTSVILLE
1040 RESEARCH BLVD SUITE 100
MADISON AL 35758-2040

8. DELIVERY FOB
[X] DESTINATION
[ ] OTHER
(See Schedule if other)

9. CONTRACTOR CODE 2B360 FACILITY
NAME AND ADDRESS
WYLE LABORATORIES, INC.
(b)(6)
345 BOB HEATH DR
HUNTSVILLE AL 35806-2842

10 DELIVER TO FOB POINT BY (Date) *(YYYYMMMDD)*
SEE SCHEDULE

11. MARK IF BUSINESS IS
[ ] SMALL
[ ] SMALL DISADVANTAGED
[ ] WOMEN-OWNED

12. DISCOUNT TERMS

13. MAIL INVOICES TO THE ADDRESS IN BLOCK
See Item 15

14. SHIP TO CODE N68936
CDR NAWCWD CODE 491G00E
(b)(6)
575 I AVE, SUITE 1
BUILDING (b)(6) ROOM (b)(6)
POINT MUGU CA 93042-5049

15. PAYMENT WILL BE MADE BY CODE HQ0338
DFAS - COLUMBUS CENTER
SOUTH ENTITLEMENT OPERATIONS
P O BOX 182317
COLUMBUS OH 43218-2264

MARK ALL PACKAGES AND PAPERS WITH IDENTIFICATION NUMBERS IN BLOCKS 1 AND 2.

16. TYPE OF ORDER			
	DELIVERY/ CALL	X	This delivery order/call is issued on another Government agency or in accordance with and subject to terms and conditions of above numbered contract
	PURCHASE		Reference your quote dated Furnish the following on terms specified herein. REF:

ACCEPTANCE. THE CONTRACTOR HEREBY ACCEPTS THE OFFER REPRESENTED BY THE NUMBERED PURCHASE ORDER AS IT MAY PREVIOUSLY HAVE BEEN OR IS NOW MODIFIED, SUBJECT TO ALL OF THE TERMS AND CONDITIONS SET FORTH, AND AGREES TO PERFORM THE SAME.

NAME OF CONTRACTOR | SIGNATURE | TYPED NAME AND TITLE | DATE SIGNED *(YYYYMMMDD)*

[X] If this box is marked, supplier must sign Acceptance and return the following number of copies: 1

17. ACCOUNTING AND APPROPRIATION DATA/ LOCAL USE
See Schedule

18. ITEM NO.	19. SCHEDULE OF SUPPLIES/ SERVICES	20. QUANTITY ORDERED/ ACCEPTED*	21. UNIT	22. UNIT PRICE	23. AMOUNT
	SEE SCHEDULE				

* *If quantity accepted by the Government is same as quantity ordered, indicate by X. If different, enter actual quantity accepted below quantity ordered and encircle.*

24. UNITED STATES OF AMERICA
TEL: (b)(6)
EMAIL: (b)(6) j@navy.mil
BY: (b)(6) (b)(6)
CONTRACTING / ORDERING OFFICER

25. TOTAL $3,326,187.65
26. DIFFERENCES

27a. QUANTITY IN COLUMN 20 HAS BEEN
[ ] INSPECTED [ ] RECEIVED [ ] ACCEPTED, AND CONFORMS TO THE CONTRACT EXCEPT AS NOTED

b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE | c. DATE *(YYYYMMMDD)* | d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE

f. TELEPHONE NUMBER | g. E-MAIL ADDRESS

28. SHIP NO | 29. DO VOUCHER NO. | 30. INITIALS

[ ] PARTIAL [ ] FINAL

31. PAYMENT
[ ] COMPLETE [ ] PARTIAL [ ] FINAL

32. PAID BY

33. AMOUNT VERIFIED CORRECT FOR

34. CHECK NUMBER

35. BILL OF LADING NO.

36. I certify this account is correct and proper for payment.
a. DATE *(YYYYMMMDD)* | b. SIGNATURE AND TITLE OF CERTIFYING OFFICER

37. RECEIVED AT	38. RECEIVED BY	39. DATE RECEIVED *(YYYYMMMDD)*	40. TOTAL CONTAINERS	41. S/R ACCOUNT NO.	42. S/R VOUCHER NO.

Section C - Descriptions and Specifications

STATEMENT OF WORK

STATEMENT OF WORK (SOW)
AIRBORNE ELECTRONIC ATTACK (AEA)
ELECTRONIC TACTICAL INFORMATION REPORT AND MANAGEMENT SYSTEMS (ETIRMS)
DEVELOPMENT
JANUARY 2018

1.0 BACKGROUND AND SCOPE

The AEA/EA-6B Integrated Product Team (IPT), NAWCWPNS has been tasked by multiple sponsors, including Naval Air (NAVAIR) Systems Command (PMA-231, PMA-234, PMA-262, PMA-265, PMA-281, PMA-290, and PMA-299), with providing software development, testing, and engineering support for all existing and future configurations of the ETIRMS software system. Additionally, under Foreign Military Sales (FMS) cases, a modified version of the ETIRMS software systems will be developed for the Royal Australian Air Force (RAAF), Royal Australian Navy (RAN), Kuwait, Norway, and the United Kingdom.

The scope of this SOW consists of providing software development, testing, and engineering support for all existing and future configurations of the ETIRMS software system for customers that may include but are not limited to the United States Navy (USN), Commonwealth of Australia, Kuwait, Norway, and the United Kingdom.

2.0 APPLICABLE DOCUMENTS

The following documents are applicable to this SOW.

Military Standards

Identifier	Document Name	Date
ANSI/EIA-649-B	Configuration Management Standard	6/17/2011
ANSI/EIA-748-C	Earned Value Management Systems	4/29/2014
DoD-STD-2167A	Defense System Software Development	2/5/1994
GEIA-STD-0007B	Logistics Product Data Handbook	2/10/2014
MIL-STD-498	Software Development and Documentation (still valid for legacy system)	5/27/1998
MIL-STD-961E	Defense and Program-Unique Specifications Format and Content	4/1/2008
MIL-STD-1679A	Software Development	10/22/1983
MIL-HDBK-61A	Configuration Management Handbook	2/7/2001

2.0 Instructions and Guides

Identifier	Document Name	Date
DoDI 5000.02	Operation of the Defense Acquisition System	1/7/2015
NAVAIR 00-25-300-B	Technical Directives System	1/1/2009
NAVAIR 00-25-100	Technical Manual Program	12/30/2006
NAVAIR 4355.19E	NAVAIR System Engineering Guide	2/6/2005
NAVAIRINST 4355.19D	Systems Engineering Technical Review Process	1/1/2008
NAWCWD 5500.1	Command Security Program Regulation	2/13/2012
4.2.0.0P4	Defense Information Infrastructure - Common Operating Environment (DII-COE) Specifications 1.4	N/A
47 CFR 300.1	Manual of Regulations and Procedures for Federal Radio Frequency Management	5/1/2014
EA-18G0EWDS-DBDD-1816-91-000-01-T	EWDS Database Design Document (located at Classified AEA Network, ETIRMS Product SharePoint website)	4/20/2017
ETIRMS-H14-SDP	ETIRMS Software Development Plan (located at Classified AEA Network, ETIRMS Product SharePoint website)	4/1/2016
ETIRMS-MH60-UM-1601	ETIRMS User's Manual (located at Classified AEA Network, ETIRMS Product SharePoint website)	10/01/2016
ETIRMS-UPC-CMP-1601	ETIRMS Configuration Management Plan (located at Classified AEA Network, ETIRMS Product SharePoint website)	6/1/2016
ETIRMS-UPC-CS-1301	ETIRMS Software Coding Standards (located at Classified AEA Network, ETIRMS Product SharePoint website)	10/1/2013
ETIRMS-UPC-H16-SRS-1701	ETIRMS Software Requirements Specifications (SRSs) (located at Classified AEA Network, ETIRMS Product SharePoint website)	3/1/2017
ETIRMS-UPC-H16-SSS-1701	ETIRMS System/Segment Specification (SSS) (located at Classified AEA Network, ETIRMS Product SharePoint website)	3/1/2017
ETIRMS-UPC-H12-STP-1301	ETIRMS Test Plan (located at Classified AEA Network, ETIRMS Product SharePoint website)	9/1/2013
ETIRMS-UPC-PP-1501	ETIRMS Project Plan (located at Classified AEA Network, ETIRMS Product SharePoint website)	3/1/2015
ETIRMS-UPC-StCP-1601	ETIRMS Standards Compliance Plan (located at Classified AEA Network, ETIRMS Product SharePoint website)	1/22/2016
FRD-NavMPS-H12	ETIRMS Functional Requirements Document (located at Classified AEA Network, ETIRMS Product SharePoint website)	12/1/2014
N/A	Naval Systems Engineering Guide (located at https://nserc.nswc.navy.mil/nseg/default.aspx)	1/1/2004
N/A	AEA IPT Processes and Procedures (located at https://share.navair.navy.mil/aeaipt/Pages/IPTHome.aspx)	5/1/2015
N/A	Joint Mission Planning System (JMPS) Developer's Handbook Ver 1.2.4/1.3.5	10/8/2009
Version 4.1	JMPS Technical Rules (located at Classified AEA Network, ETIRMS Product SharePoint website)	10/8/2009

2.1 Industry Standards

Identifier	Document Name	Date
CMMI V1.3	Capability Maturity Model Integration (CMMI), Carnegie Mellon University	11/1/2010
IEEE 12207-2008	ISO/IEC/IEEE Standard for Systems and Software Engineering - Software Life Cycle Processes	1/31/2008

The Government will provide all necessary obsolete reference documents and those not generally available to the contractor as requested.

The Contractor shall not purchase IT equipment on behalf of NAVAIR in support of this order, which reports to PBIS-IT, without a NAVAIR Command Information Officer (CIO) approved NAV-IDAS ITPR.

2.2 IT Requirements

2.4.1 Clinger-Cohen Act (CCA): The contractor shall conduct analysis of program/project needs, acquisition strategy and program artifacts to identify and capture specific factors required to satisfy the 11 elements of CCA compliance listed in DODI 5000.02, Enclosure 1, Table 9. Using Microsoft Word, the contractor shall prepare a CCA compliance matrix following the organization and appearance of Table 11 with additional separate columns for the display of artifact: titles, date(s) of approval, page number(s), and paragraph or section number(s). The right-hand column shall include an embedded object permitting the reader to open unclassified artifacts. The column shall identify classified artifacts and shall describe approved classified channels for access of classified artifacts. The contractor shall support the program manager during CCA compliance review and respond to reviewer comments if and when additional supporting information or revisions are required.

Updating approved CCA compliance packages: For updates of approved CCA compliance packages, the contractor shall conduct analysis of program/project needs, acquisition strategy and program artifacts to identify and to determine if each of the Eleven (11) elements of CCA has changed and if no change has occurred a notation stating "no change" shall be entered in the CCA compliance matrix. If changes have been found, the Contractor shall update the CCA compliance matrix to reflect the changes.

The contractor shall support the program manager during CCA compliance review and respond to reviewer comments if and when additional supporting information or revisions are required.

2.4.2 Cybersecurity: The contractor shall conduct investigation and analysis of acquisition program artifacts such as but not limited to Initial Capabilities Document (ICD), Capability Description Document (CDD), Capability Production Document (CPD), Navy urgent operational need (UON) and Marine Corps urgent universal need statement (UUNS), joint urgent operational needs (JUONs), threat assessments and acquisition strategies (AS). Knowledge gained from this analysis shall be used when developing the Cybersecurity Strategy (CS) needed to steer and inform the program's development of a Security Plan (SP) in accordance with DoDI 8510.01, of 12 March 2014

As a minimum, hardware, firmware, software, documentation (data deliverables) and/or IT services delivered by this contract shall be in compliance with the following References:

a. DoDI 8500.01 Cybersecurity, 14 March 2014
b. DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), 12 March 2014, Incorporating Change 1, May 24, 2016.
c. Committee on National Security Systems Instruction 1253, "Security Categorization and Control Selection for National Security Systems," March 27, 2014, as amended.
d. DoDD 8140.01, Cyberspace Workforce Management, 11 August 2015.
e. DoD 8570.01-M Information Assurance Workforce Improvement Program, 15 August 2004, Certified Current as of 10 November 2015.

The contractor shall conduct investigation and perform analysis including; criticality analysis, threat assessment and vulnerability assessments. All findings and recommendations shall be reported to the

Government in technical reviews and submitted as written reports or documents as listed in Contract Data Requirements Lists. The contractor shall support Government efforts needed for Information systems (IS) (enclaves or major applications), Platform Information Technology (PIT) or PIT systems to successfully categorize the system, achieve favorable assessment for selection, implementation and testing of security controls and authorization (approval to operate) before use or interconnection in an operating environment in accordance with references (a), (b) and (c). This includes IT that is standalone and IT that is connected to other systems, networks or enclaves. Information systems (enclaves or major applications), PIT or PIT systems delivered prior to award of this contract but included in the performance of this contract may have been delivered in compliance with Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) and as such shall require transition to Risk Management Framework cybersecurity compliance. Transition planning proposed or performed under this contract shall be in compliance with reference (b) Enclosure 8, Figure 2 and all hardware, firmware and software deliverables shall be capable of receiving Authorization to Operate in accordance with reference (b).

Information technology services shall only be performed by personnel who are qualified and certified in accordance with reference (d). Personnel proposed and/or used in the performance of this contract as certified personnel shall be limited to those whose specifically assigned duties and responsibilities require certification.

All Cybersecurity shall be in compliance with the following listed instructions:

a. DoDI 8582.01, Security Of Unclassified DoD Information On Non-DoD Information Systems, 06 May 2012
b. Chairman of the Joint Chiefs of Staff Instruction CJCSI 3170.01I (series), Joint Capabilities Integration and Development System (JCIDS), 23 January 2015.
c. CJCSI 6211.02D, Defense Information System Network (DISN): Policy and Responsibilities, 24 Jan 2012 (Current as of 4 Aug 2015).
d. CJCSI 6251.01D, Narrowband Satellite Communications Requirements, 30 Nov 2012.
e. CJCSI 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND), 09 Feb 2011, certified current 9 Jun 2015.
f. Chairman of the Joint Chiefs of Staff Manual CJCSM 6510.01B – Cyber Incident Handling Program, 10 July 2012 (Current as of 18 Dec 2014).
g. Navy Ports Protocols, and Services (NPPS) Manual, Version 1.5, 16 November 2010.
h. Defense Acquisition Guidebook – Chapter 7, Acquiring Information Technology, Including National Security Systems, Section 7.5, Information Assurance (IA).
i. DoD 5220.22-M, National Industrial Security Program Operating Manual, February 28, 2006 (NISPOM) Incorporating Change 2 May 18, 2016.
j. DoD 8570.01-M, Information Assurance Workforce Improvement Program, 19 Dec 2005, (Incorporating Change 3, 24 Jan 2012).
k. DoDD 8000.01, Management of the Department of Defense Information Enterprise, 17 March 2016.
l. DoDD 8100.02, Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG), 14 April 2004, Certified Current, 23 April 2007.
m. DoDD 8140.01, Cyberspace Workforce Management, 11 August 2015.
n. DoDI 8330.01, Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), 21 May 2014.
o. DoDI8500.01, Cybersecurity, 14 March 2014.
p. DoDI 8520.02, Public Key Infrastructure (PKI) and Public Key (PK) Enabling, 24 May 2011.
q. DoDI 8551.01, Ports, Protocols, and Services Management (PPSM), 28 May 2014
r. DoDI 8580.1, Information Assurance (IA) in the Defense Acquisition System, 9 July 2004.

s. DoDI 8581.01, Information Assurance (IA) Policy for Space Systems Used by the Department of Defense, 8 June 2010.
t. DON CIO Memo 02-10, Department of the Navy Chief Information Officer Memorandum 02-10 Information Assurance Policy Update for Platform Information Technology, 26 April 2010.
u. DON letter 5239 NAVAIR 726/2322 of 18 Feb 09, NAVAIR Data at Rest Policy.
v. Federal Information Processing Standards Publications (FIPS PUB)-199, February 2004.
w. Committee on National Security Systems Policy CNSSP No. 11, 10 June 2013.
x. Office of the Chief of Naval Operations OPNAV INST 5239.1C, Navy Information Assurance (IA) Program, 20 Aug 08.
y. SECNAV M-5239.1, Department of the Navy Information Assurance Program; Information Assurance Manual, November 2005.
z. SECNAVINST 5230.15, Information Management/Information Technology Policy for Fielding of Commercial Off the Shelf Software, 10 April 2009.
aa. SECNAVINST 5239.3C, Department of the Navy Cybersecurity Policy, 2 May 2016.
bb. SECNAVINST 5239.19, Department of the Navy Computer Network Incident Response and Reporting Requirements, 18 March 2008.
cc. The National Security Act of 1947.
dd. Title 40/Clinger-Cohen Act.
ee. Title 44/ Federal Information Security Management Act.
ff. National Institute of Standards and Technology Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4, April 2013 (Updated 22 Jan 2015).

All IT procured on behalf of this contract shall meet all DoD/DON and NAVAIR cybersecurity polices. Failure to follow these policies will result in denied access to NMCI, One Net, Integrated Shipboard Network System (ISNS) and other DON, DoD and Joint Networks. These cybersecurity policies are standard across the Department and ensure cybersecurity compatibility and interoperability.

IT systems and or networks operated by contractors pursuant to a NAVAIR contract, regardless of the level of data processed, shall be operated in accordance with the NISPOM.

Approved contractor-owned equipment shall be permitted connections to NAVAIR/DoD networks in order to carry out the performance of this contract. All Contractor-owned hardware and/or software shall meet DoDI 8500.1 Cybersecurity (CS), is subject to validation scanning and must be approved by the NAVAIR site CS Manager prior to connection.

The following specific criteria must be met before the contractor can be connected to any DoD or NAVAIR network in support of this contract. Requirements include:

a. Network Vulnerability Scanning. NAVAIR Deputy CIO for Information Assurance maintains authorized auditing tools and shall provide for firewall/port scans, device discovery scan, vulnerability assessment, and other requirements as required to ensure secure interoperability with DoD networks. The contractor shall be responsible for the remediation of any equipment that fails these audits prior to the connection of the system to the networks; Results of approvals shall be documented via Memorandum of Agreement with the Facility Security officer and the Defense Security Service Representative for that contractor.

b. Extent of Validation Scanning. To prevent scanning of corporate assets, all such networks, equipment and connections shall be physically segregated from any government/contractor corporate networks that are not in direct support of DoD contracts.

c. Circuit Provisioning. Any circuit or connection between NAVAIR and/or DoD site and the contractor site shall be provisioned via the Defense information Security Agency and comply

with CJCSI 6211.02D, Defense Information System Network (DISN): Policy and Responsibilities, 24 Jan 2012.

d. Servicing Systems from a Remote Contractor Site. Remote Access Service connections that allow off-station operation and/or administration of contractor owned systems, located at any NAVAIR facility or site, shall not be permitted, with the exception of those systems connecting to the Command via the Outreach Services identified in Section 6, Enterprise Architecture.

e. Memorandum of Agreement and Inter-connection Agreements. A Cybersecurity Memorandum of Agreement (MOA) between the contractor owning the equipment and AIR-7.2.6 shall be developed and signed before the equipment can be connected to NAVAIR networks. Failure to comply with the signed MOA shall be grounds for disconnection from the network.

2.4.3 Enterprise Architecture

a. Contractor Networks and Connections. Contractor-owned and operated networks are prohibited on NAVAIR facilities or sites in support of this contract. The contractor may access non-Government, external IP space via the NAVAIR-provided Virtual Private Network (VPN) Outreach service or NAVAIR CIO approved Internet Protocol (IP) service.

b. Architecture Compliance. The contractor shall ensure all IT solutions, including database solutions, comply with the appropriate NAE Enterprise Architecture, and are verified by the NAVAIR Enterprise Architect (AIR-7.2.3) prior to build out.

c. Disclosure of pre-existing networks, circuits or connections. All networks, circuits or connections between the contractor and NAVAIR sites related to previous contracts shall be identified in the Memorandum of Agreement (MOA). Failure to comply and subsequent discovery of an unregistered network, circuit or connection shall be grounds for immediate disconnection.

3.0 REQUIREMENTS

3.1 General Engineering Support

In support of this effort, the contractor shall utilize the IPT's development system, software baselines, databases, processes and procedures, as referenced in Section 2.

3.1.1 Reports: The contractor shall support the reporting of programmatic planning, tracking and monitoring progress, status and cost reports. The contractor shall develop, update, deliver and maintain the following reports: Progress, Status and Management, Financial and Cost Graphs, and Contract Summary Reports. In addition, the contractor shall provide task execution highlights and labor expenditure reporting. (CDRLs A002 and A003)

3.1.1.1 The contractor shall provide bi-weekly highlights and status reporting. (CDRL A002)

3.1.1.2 An Expense Status Report shall be provided monthly and shall include the estimated cost, funds authorized to date, total to date funding, total estimated spending, percentage of funds expended, weekly burn rate, stop work date, and period of performance end date. (CDRL A002)

3.1.1.3 The contractor shall develop and deliver a weekly report that provides a by-person and by-work breakdown structure (WBS) task breakout of the hours and burdened cost expended for the respective reporting period and cumulative to date. In addition, the weekly report shall provide a percentage complete of each WBS task that will be input into the Government's earned value tracking system. The contractor shall electronically deliver the weekly report to the Contracting Officer's Representative (COR) and the

Navy Technical Representative. The contractor shall enter hours into the Government SharePoint EVM website. (CDRL A002)

3.1.2 The contractor shall attend and participate in engineering meetings: Technical Interface Meetings (TIM), Preliminary Design Reviews (PDR), Critical Design Reviews (CDR), Integration Readiness Reviews (IRR), Construction Readiness Reviews (CRR), Build Readiness Reviews (BRR), Operational Systems Review Board (OSRB), Technical Review Board (TRB), Deficiency Change Review Board (DCRB), working group meetings, peer reviews, test readiness reviews, test events, etc. If travel is involved, the times/dates for meetings will be provided at least two weeks prior to event to the contractor via electronic mail. The contractor shall provide recommendations and conclusions based on meeting discussions and materials. (CDRL A002)

3.1.3 The contractor shall support engineering, status, and managerial meetings by preparing slides or input to slides. The contractor will be tasked via electronic mail. (CDRL A004)

3.1.4 The contractor shall attend engineering and software design reviews, software acceptance testing program reviews, and other technical reviews and meetings for the purpose of gathering data required to develop and deliver the ETIRMS testing support as stated herein. The times/dates for meetings will be provided at least two weeks prior to event to the contractor via electronic mail. The contractor shall provide recommendations and conclusions based on evaluation of data acquired. (CDRL A002)

3.2 Software Requirements

3.2.1 The contractor shall identify, analyze, and develop new requirements, and modify and delete existing requirements, that will be imposed on the ETIRMS software component, as needed by the Government. The contractor shall analyze the requirements for appropriate decomposition, allocation, and traceability; document the results; and submit the results for peer review in accordance with the IPT's approved requirements analysis process. The requirements shall address functionality, performance, and interfaces. These requirements shall be documented in the Functional Requirements Document (FRD), System/Subsystem Specification (SSS), Software Requirements Specification (SRS), user stories, and acceptance criteria. (CDRLs A007 and A008)

3.2.2 The contractor shall support requirements analysis by: (1) conducting studies and analyses to develop system concepts, including functionality and performance requirements for existing, upgraded, and new systems; (2) identifying life cycle support requirements; (3) defining interface requirements; and (4) preparing requirement and functional baseline specifications, plans and documents (CDRLs A001, A005, A007 and A008)

3.2.3 The contractor shall identify conflicting, not testable, ambiguous requirements affecting software functions, as well as inadequate software data requirements. (CDRLs A006 and A007)

3.3 Software Design

The contractor shall produce preliminary and detailed design based upon the requirements. The contractor shall develop a top-level and lower level design for each Computer Software Configuration Item (CSCI). The contractor shall participate in software design reviews. A detailed design of each CSCI shall be generated and documented. The design shall be documented using project templates and the unified modeling language (UML). (CDRLs A001 and A005)

3.3.1 The contractor shall evaluate testability of computer program design in development.

3.4 Software Code

The contractor shall create new code, and modify and delete existing code in order to implement new functionality and correct software defects. The code changes will be in compliance with new and modified software design. Coding assignments will be done via electronic mail or other electronic means (e.g., Microsoft SharePoint, Microsoft Team Foundation Server). All code will be in compliance with the coding standards. Code shall be peer reviewed in accordance with existing processes. (CDRL A006)

3.4.1 The contractor shall provide all current executable code, and all source code, libraries and files required to generate the executable code, and (as applicable) interface and version description documentation. Software languages may include "C", C++, Visual Basic, C-Sharp, Java, and JavaScript. Software frameworks may include .NET and JMPS. The software delivered shall meet or exceed established defect criteria, and must be loadable and able to run on the applicable system. (CDRL A006)

3.4.2 The contractor shall use the configuration management tool (Rational ClearCase, Microsoft Team Foundation Server) to check out code and check it back in.

3.5 Software Cybersecurity

The contractor shall ensure that all software code that is created under this TO is scanned for cyber security requirements utilizing a Government provided source code scanning application/tool (example, HP Fortify). The chosen tool will include the ability to provide audit reports to the current version of the Government provided Application Security and Development Security Technical Implementation Guide (STIG). The tool will have the ability to identify the root cause of software security vulnerabilities in the source code and generate an accurate risk ranked list of issues with detailed action on how to rectify those vulnerabilities at the "Line of Code Level". The contractor shall submit the results of this scan to the Government as an artifact in support of the delivered software. (CDRL A00A)

3.6 Database Development

The contractor shall create new databases and maintain existing databases. The databases shall be done in Microsoft SQL Server, Microsoft Access, or other database management systems (DBMS). The database contents shall be retrieved via queries, views, and stored procedures developed by the contractor. (CDRL A006)

3.7 Configuration Management

The contractor shall use Rational ClearCase and Microsoft Team Foundation Server to perform configuration management of the source code, build scripts, InstallShield projects, databases, and create the final working software product for test and delivery. The contractor shall develop build reports and software version descriptions (SVDs). The contractor shall produce source lines of code (SLOC) counts for the purposes of metrics and presentations. The contractor shall manage software baselines, identify baselines for developers to modify, and incorporate submitted software changes. (CDRL A001)

3.8 Installation

The contractor shall create installation packages for software and databases. The contractor shall check the InstallShield Project files in to the configuration management tool(s). (CDRL A006)

3.9 Virtual Machines

The contractor shall support the creation of virtual machines (VMs) and the maintenance and dissemination of the VMs.

3.10 Software Test

The contractor shall provide testing support for build tests, Independent Verification and Validation (IV&V), Developmental Test and Evaluation (DT&E), and Operational Test and Verification at the appropriate test site.

3.10.1 The contractor shall develop and update test procedures based upon requirement changes and establish the traceability of requirements to test procedures. The contractor shall participate in test procedure peer reviews. (CDRL A00A)

3.10.2 The contractor shall support the development and update of the Software Test Plan (STP). (CDRL A009)

3.10.3 The contractor shall test the software. The contractor shall verify the software by conducting independent testing, code analysis, algorithm analysis, and review of the test procedures and results. The contractor shall conduct software verification as specified under the STP, including problem reporting, tracking, and correction. Software portions may include functional areas to be verified, including critical to safety, security, equipment selection, mission critical performance, development schedule, software reuse, sustainability, reliability, and supportability. (CDRLs A001, A005, and A00B)

3.10.4 The contractor shall provide the results of the test analysis in written problem investigation reports, or identify problems in the form of computer Software Problem Reports (SPRs), discrepancy reports (DRs), defect reports, software anomaly reports (SARs), and test metrics. The contractor shall enter these software defect reports into the Government tracking system and update status throughout the investigation and resolution process. (CDRL A00B)

3.10.5 The contractor shall test ETIRMS software in accordance with IPT and Government specifications. (CDRL A009)

3.10.6 The contractor shall support lab, ground, and flight integration and test events by developing and updating integration and test plans and procedures; verifying system engineering requirements; and troubleshooting, analyzing, recommending, and incorporating corrective actions. (CDRLs A001, A00A and A00B)

3.11 User Documentation

The contractor shall support the maintenance and/or creation of the user's manual, system administrator's user manual, training material (slides, videos, etc), and certification letters. The contractor shall generate a compiled help manual (CHM) from the user's manual. (CDRLs A004 and A005)

3.11.1 The contractor shall provide redlined change pages for specifications and user documentation impacted by each engineering solution. The contractor shall provide current user documentation for installation, operation, and maintenance. (CDRL A005)

4.0 PERSONNEL QUALIFICATIONS.

The contractor shall be responsible for employing personnel having at least the minimum level of education and training, experience, and security clearance, as stated under each key labor category specified herein.

4.1 **Key Personnel** are those who will be performing in Key Labor Categories specified below.

4.2 College Degree:

All degrees shall be obtained from an "accredited college or university" as recognized by the U.S. Department of Education. This includes Associates, Bachelor's, Master's, or Doctorate degrees.

4.3 Degree Majors:

All labor category degree major requirements are specified below.

4.4 Experience and Education Level Definitions:

JUNIOR: A Junior level person within a labor category has less than 3 years' experience and a BA/BS degree. A Junior level person is responsible for assisting more senior positions and/or performing functional duties under the oversight of more senior positions.

JOURNEYMAN: A Journeyman level person within a labor category has 3 to 10 years of experience and a BA/BS degree. A Journeyman level person typically performs all functional duties independently.

SENIOR: A Senior level person within a labor category has over 10 years of experience and a MA/MS degree. A Senior level person typically works on high-visibility or mission critical aspects of a given program and performs all functional duties independently. A Senior level person may oversee the efforts of less senior staff and/or be responsible for the efforts of all staff assigned to a specific job.

Additionally, the following qualification substitution chart provides standard experience/education substitutions:

Bachelor's Degree	6 years' additional work experience may be substituted for a Bachelor's Degree	Associate's Degree plus 4 years' additional work experience may be substituted for a Bachelor's Degree
Master's Degree	Bachelor's Degree plus 4 years additional work experience may be substituted for a Master's	

"Years of experience" shall mean full, productive years of participation.

Productive years" shall mean 52 weeks of work reduced by reasonable amounts of time for holidays, annual and sick leave.

If participation was part-time, or if less than one-half of the standard work week was spent performing qualifying functions, the actual time spent performing qualifying functions may be accumulated to arrive at full years of experience.

Contractor personnel must have performed these functions for at least five years within the last five years.

4.5 Key Labor Qualifications:

The following chart lists the minimum education, experience, and security clearance requirements, the Bureau of Labor Statistics (BLS) Standard Occupational Classifications (SOCs), and the functional descriptions for each key labor category:

Key Labor Category	Level	BLS SOC Code	Functional Description	Security Clearance Required
Software	Journeyman	15-1133	Responsible for the detailed design, implementation, and testing of	SECRET

Engineer / Engineer IV			subsystems and system components. Able to build a wide variety of software subsystems and components efficiently and effectively, given only a requirements specification and constraints. Able to develop and sustain these subsystems and software components in complex, multi-vendor, multi-platform environments. Requires at least three (3) years of experience in software development and a BA/BS degree or higher in a "Relevant Engineering/Science Field".	
Systems Engineer/ Engineer V	Senior	15-1143	Has programmatic or technical leadership roles in an organization identifying, formulating, designing and/or testing practical solutions to engineering problems and guide the engineering development of modern complex systems; and to employ systems engineering methods and tools in the development of advanced complex systems, and when appropriate, conduct research in applied systems engineering to advance the field. Requires at least ten (10) years of experience in an engineering position, three (3) of which must be directly related to Naval systems, and a BA/BS degree or higher in a "Relevant Engineering/Science Field", Demonstrated knowledge in area of engineering expertise.	SECRET
Test Engineer/ Engineer IV	Journeyman	17-2011	Performs engineering duties testing software requirements analysis, software design evaluation, software test design, test procedure development and software test reporting. May recommend improvements in testing equipment and techniques. Requires over three (3) years of experience in an engineering position and a BA/BS degree or higher in "Relevant Engineering/Science Field".	SECRET
Computer Scientist,/ Engineer IV	Journeyman	15-1111	Works on high-visibility or mission critical aspects of a given program and performs all functional duties independently. May oversee the efforts of less senior staff and/or be responsible for the efforts of all staff assigned to a specific job. Requires over three (3) years of experience in software development and a BA/BS degree or higher in Computer Science or Mathematics.	SECRET

5.0 DELIVERABLES

Specific items of reports, test plans, procedures, technical support documents, meeting minutes, and progress reports will be provided in accordance with the applicable CDRLs.

CDRL	DESCRIPTION
A001	Scientific and Technical Reports
A002	Contractor's Progress, Status and Management Report
A003	Performance and Cost Report
A004	Presentation Materials
A005	Revision to Existing Government Documents
A006	Computer Software Product End Item Documentation*
A007	Software/Subsystem Specification (SSS)
A008	Software Requirements Specification (SRS)
A009	Software Test Plan (STP)
A00A	Acceptance Test Plan
A00B	Test/Inspection Report
A00C	PPIP

*100% Government purpose rights

6.0 SPECIAL CONSIDERATIONS

6.1 Travel:

During performance of the TO, the contractor may be required to perform local and non-local travel to support the tasking. The contractor shall submit a request for travel in support of this TO. Each request shall be submitted in advance (a minimum of one week) to the COR for approval.

Each travel request will minimally consist of:

- Date of Request
- TO number
- Employee(s)
- Date and duration of proposed travel
- Purpose of travel
- Destination
- Cost estimate (airfare, per diem, car rental, miscellaneous expenses)
- Total travel allowance on the TO
- Total travel cost expended to date
- Approval signatures

Upon completion of each trip, the contractor shall submit a trip report to the COR. (CDRL A001)

6.2 Access to Government Facilities:

During performance of this TO the contractor will require access to Government facilities. The contractor shall identify and request approval from the technical point of contact (POC), for each person expected to require access to a Government facility. The Government will furnish access to the ETIRMS Lab and other AEA/EA-6B laboratories on an as-needed basis during normal operating hours. The contractor shall provide a list to the ETIRMS manager of the personnel with the "need to know" for access to the ETIRMS Lab. Contractor personnel performing these tasks will require access to classified facilities, and must have appropriate clearances on file with the NAWCWPNS Security Office. The Government reserves the right to control the laboratory schedule and use of documentation required for performance of this contract.

6.3 Government Furnished Information:

The contractor will be allowed access to the AEA/EA-6B Engineering Document Data Center (EDDC) during normal operating hours. The contractor shall provide to the Government a list of personnel with "need to know" access to EDDC controlled data.

The Government will furnish access to ETIRMS documentation that shall include the following:

- FRD
- System/Segment Specification
- SRS
- Interface Design Specifications
- Interface Design Documents
- Software Development Document
- Data Base Design Document
- ETIRMS WBS

6.4 Place of Performance:

Approximately 95% of performance is expected to take place at Point Mugu, CA at a Government facility. The other 5% will take place at other Government installations identified in the RFP and contract. Support for these sites, including direct Fleet services that require SECRET clearance will be required.

6.5 Contract Work Environment:

The contractor shall execute the efforts described herein as a member of the AEA IPT. In support of this effort, the contractor shall utilize AEA IPT processes and procedures, including but not limited to IPT's development system, software baselines, software tools, and databases. The contractor shall interface with other Government and contractor team members, use existing NAWCWD special AEA laboratory hardware and facilities, and access NAWCWD test aircraft located at VX-31 China Lake, CA and VX-23 Patuxent River, MD, on an as needed basis.

6.6 NMCI:

Any tools developed that will be hosted by NMCI or run on NMCI workstations will be certified for NMCI and comply with NMCI policy. Additionally, any servers supporting this effort will be transitioned to meet the requirements of the current NAVAIR Server Consolidation effort.

7.0 MATERIAL AND PURCHASING:

The contractor may be required to purchase incidental material in support of this TO. The contractor must obtain prior approval from the COR for any purchases valued over $3,500. The contractor must obtain COR concurrence and Contracting Officer approval prior to any purchases valued over $25,000. To receive approval for purchases the contractor will submit a consent package providing a description, price, evidence of adequate price competition, or if unavailable, a justification for a single source and determination that the price is fair and reasonable. These requirements apply to all contractor purchases.

8.0 QUALITY SURVEILLANCE AND PERFORMANCE STANDARDS:

A Surveillance Activity Checklist (SAC) will be used by the Government to perform surveillance. A copy of the SAC is provided as an attachment in Section J, for informational purposes only.

9.0 SECURITY:

9.1 The contractor shall provide personnel with the appropriate personnel security clearance levels for the work to be performed. Access to SECRET information is required in the performance of this contract and shall be in accordance with the DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), applicable DoD personnel security regulations, and DoD Contract Security Classification Specification (DD Form 254). The contractor shall maintain sufficiently cleared personnel to perform the tasks required by this SOW IAW the DD Form 254 and the contract. All contractor personnel shall possess the requisite security clearance, accesses, and need-to-know commensurate with the requirements of their positions.

Overarching contract security requirements, and Contractor access to classified information, shall be as specified in the basic DD Form 254 for this task order. All contractor personnel with access to unclassified IS, including e-mail, shall have at a minimum a favorable National Agency Check with Inquiries (NACI).

For Official Use Only information generated and/or provided under this contract shall be marked and safeguarded as specified in DoDM 5200.01, Information Security Program Manual (Volume 4) available at http://www.dtic.mil/whs/directives/corres/pdf/520001_vol4.pdf . Contractor shall not store or transmit CUI on personal IT systems or via personal e-mail. Unclassified e-mail containing any DoD CUI shall be encrypted. Prior to sending CUI to any non-Navy Marine Corps Internet (NMCI) addressees, the sender must first positively verify all recipients are authorized access to CUI and have need-to-know.

Non-NMCI recipients must have a DoD compliant Private Key Infrastructure (PKI) certificate that enables electronic transmission via unclassified networks while protecting the CUI with a digital signature and encryption.

9.2 Communications Security (COMSEC):

The contractor will require access to COMSEC at Government locations. U.S. cryptographic equipment inventory information, as well as the systems and manner in which each particular equipment is used, is for official use only. Publication or release of any related COMSEC information by any means, by the contractor, without prior written approval of the contracting officer is prohibited. The contractor must be a U.S. citizen, have a final Government security clearance with the appropriate personnel security background investigation for the level of classification involved, have strict need-to-know, have the appropriate COMSEC briefing before access is granted, and granted access only in conformance with procedures established for the particular type of COMSEC information involved. The contractor shall adhere to the DD Form 254 COMSEC security requirements, facility COMSEC material control and operating procedures, and all applicable COMSEC regulations, instructions, and policies. Prior approval from the Government Contracting Activity is required in order for a prime contractor to grant COMSEC access to a subcontractor.

9.3 Program Protection Plan (PPP):

A Program Protection Plan (PPP) and supporting annexes will be provided as Government Furnished Information (GFI). The contractor will follow guidance in the PPP and annexes for protection of Critical Program Information (CPI) identified in the PPP. The contractor will, as requested by the Government, provide input to updates of the PPP and associated annexes. Any modifications or deviations to the PPP or annexes will be made in writing by the Program Manager (PM). Requests for clarification of the PPP or annexes will be made by the contractor to the PM not later than thirty (30) days from receipt of the PPP, its annexes, or updates thereof.

9.4 Program Protection Implementation Plan (PPIP):

The Contractor shall develop (or update, as applicable) the PPIP to ensure effective and efficient protection of essential program information, technologies and systems, and in accordance with Operational Security (OPSEC) requirements which will include (at a minimum):

- The Security Management structure.
- The CPI physical locations under the Contractor's or subcontractors' control.
- The vulnerability of the CPI under the Contractor's or subcontractors' control to intelligence collection in the following areas: Human Intelligence (HUMINT); Open Source Intelligence (OSINT); Signals Intelligence (SIGINT); Imagery Intelligence (IMINT); Computer Network Operations (CNO).
- Countermeasures at each site where CPI is held, from the following security domains (as applicable): physical security; personnel security; telecom and network security; application/systems development; cryptography; security architectures; operational security network and IT access control.
- Any special handling procedures required for CPI, and procedures for recovering CPI in the event of a mishap. The Contractor shall address these procedures for all phases of the program, including (but not limited to): RDE&E; production; operations; maintenance; logistics; transportation; training; disposal.
- Procedures for ensuring compliance with U.S. Government export statutes and regulations.
- Procedures for public release of program information. (CDRL A00C)

9.4.1 The Contractor shall implement and maintain security procedures and controls to prevent unauthorized disclosure of controlled unclassified and classified information and to control distribution of controlled unclassified and classified information in accordance with the

National Industrial Security Program Operating Manual (NISPOM) and DoDM 5200.01, Information Security Manual. The DoD Contract Security Classification Specification, DD Form 254, defines program specific security requirements. All Contractor facilities shall provide an appropriate means of storage for controlled unclassified and classified documents, classified equipment and materials and other equipment and materials.

9.6 Public Release:

Disclosure of information is covered by DFARS 252.204-7000 Disclosure of Information, incorporated in Section I of the contract, notwithstanding subsection (a)(2), the contractor must seek specific approval for disclosure of controlled unclassified information even if the information already exists within the public domain.

CLAUSES INCORPORATED BY FULL TEXT

C-TXT-ECMRA REQUIRED ENTERPRISE-WIDE CONTRACTOR MANPOWER REPORTING APPLICATION (ECMRA) INFORMATION (NOV 2017)

The contractor shall report contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the ETIRMS requirement via a secure data collection site. 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) D, Automatic Data Processing and Telecommunications, IT and Telecom - Telecommunications Transmission (D304) and Internet (D322) ONLY.

(5) S, Utilities ONLY;

(6) V, Freight and Shipping ONLY.

The contractor is required to completely fill in all required data fields using the following web address "https://www.ecmra.mil."

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