ORDER FOR SUPPLIES OR SERVICES

PAGE 1 OF 50

1 CONTRACT/PURCH ORDER/ AGREEMENT NO	2 DELIVERY ORDER/ CALL NO	3 DATE OF ORDER/CALL (YYYYMMMDD)	4 REQ / PURCH REQUEST NO	5 PRIORITY
GS00Q14OADU336	N6893619F0179	2018 Dec 20	1300668715-0001	

6 ISSUED BY CODE N68936
CDR NAWCWD CODE 254500E
(b) (6)
575 I. AVE., BLDG 36, SUITE 1116
PT. MUGU CA 93042-5049

7 ADMINISTERED BY *(if other than 6)* CODE S2206A
DCMA BOSTON
495 SUMMER
BOSTON MA 02210-2138

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

9 CONTRACTOR CODE 4A457 FACILITY
NAME AND ADDRESS
ENGILITY CORP.
(b) (6)
35 NEW ENGLAND BUSINESS CENTER DR STE 200
ANDOVER MA 01810-1071

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 36, ROOM 1303
POINT MUGU CA 93042-5049

15 PAYMENT WILL BE MADE BY CODE HQ0337
DFAS - COLUMBUS CENTER
NORTH ENTITLEMENT OPERATIONS
PO BOX 182266
COLUMBUS OH 43218-2266

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)
BY: (b) (6) (b) (6)
CONTRACTING / ORDERING OFFICER

25 TOTAL $2,773,670.44
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

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

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

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)
SEA HAWK ESM EMITTER LIBRARY DEVELOPMENT (SHEELD)
SEVERABLE
July 2018

1.0 BACKGROUND AND SCOPE

The AEA/EA-6B Integrated Product Team (IPT), Naval Air Warfare Center Weapons Division (NAWCWD) has been tasked by multiple sponsors which includes Naval Air Systems Command (PMA-299, PMA-231, PMA-234, PMA-265 and Joint Program Office (JPO) with providing software development and engineering support for all existing and future configurations of the SHEELD software systems as well as data development for AN/ALQ-217 Electronic Support Measures (ESM) System for E-2 HAWKEYE Aircraft, for AN/ALQ-210 ESM system for MH-60R SEAHAWK Helicopter, Jammer Techniques Optimization (JATO) and for F-35 Aircraft Mission System. Capability support includes Royal Australian, Royal Saudi, other Foreign Military Sales (FMS) variants, cooperative development (co-dev) projects, and other advanced electronic attack derivatives. This effort is severable.

The scope of this SOW consists of developing and testing support for the AN/ALQ-210, AN/ALQ-217 ESM Mission Data Libraries (MDLs) and producing mission planning software for MH-60R, E-2C/D and F-35 Aircrafts.

2.0 APPLICABLE DOCUMENTS

The following documents are applicable to this SOW.

2.1 Military Standards

Identifier	Document Name	Date
ANSI/EIA-649-B	Configuration Management Standard	6/17/2011
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
ANSI/EIA-748-C	Earned Value Management Systems	4/29/2014

2.2 Instructions and Guides

Identifier	Document Name	Date
NAVAIR 00-25-100	Technical Manual Program	12/30/2006
NAVAIR 00-25-300-B	Technical Directives System	1/1/2009
NAVAIR 4355.19E	NAVAIR System Engineering Guide	2/6/2015
NAWCWD 5500.1	Command Security Program Regulation	2/13/2012
NAVAIR 01-85ADC-1	EA-6B NATOPS Flight Manual	8/15/2000
4.2.0.0P4	Defense Information Infrastructure - Common Operating Environment (DII-COE) Specifications 1.4	
264A502-00 Rev 6	Lockheed Martin System Integration (LMSI) Emitter Definition File (EDF) User's Manual (264A502-00 Rev 6)	11/3/2012
266A921-04 Rev B	LMSI Baseline Scan Tune (BST) User's Manual	10/10/215
47 CFR 300.1	Manual of Regulations and Procedures for Federal Radio Frequency Management	5/1/2014
DoDI 5000.02	Operation of the Defense Acquisition System	1/7/2015
HKT-CMP-1501	HAWKTool Configuration Management Plan (CMP-0601) (located at Classified AEA Network, SHEELD Product SharePoint website)	1/19/2016
HKT-CS-1501	HAWKTool Software Coding Standards (Draft) (located at Classified AEA Network, SHEELD Product SharePoint website)	3/16/2013
HKT-DBDD-1501	HAWKTool Database Design Document (Draft) (located at Classified AEA Network, SHEELD Product SharePoint website)	4/21/2016
HKT-FRD-1501	HAWKTool Functional Requirements Document (Draft) (located at Classified AEA Network, SHEELD Product SharePoint website)	8/27/2015
HKT-OUM-1501	HAWKTool On-Line Help (Draft) (located at Classified AEA Network, SHEELD Product SharePoint website)	6/23/2017
HKT-SDP-1501	HAWKTool Software Development Plans (SDPs) (Draft) (located at Classified AEA Network, SHEELD Product SharePoint website)	7/2/2016
HKT-SRD-1501	HAWKTool Software Requirement Specifications (SRS) (Draft) (located at Classified AEA Network, SHEELD Product SharePoint website)	12/10/2014
HKT-SSS-1501	HAWKTool System/Segment Specification (SSS) (Draft) (located at Classified AEA Network, SHEELD Product SharePoint website)	1/9/2014
HKT-UM-1501	HAWKTool User's Manual (Draft) (located at Classified AEA Network, SHEELD Product SharePoint website)	7/23/2017
MP-FA18-ICD-10-001	F/A-18 Hl2 Mission Initialization Files Interface Control Document (ICD)	9/13/2012
NWP 3-22.5-EA6B	EA-6B Tactical Manual (TACMAN)	
Version 4.1	JMPS Technical Rules (located at Classified AEA Network, ETIRMS Product SharePoint website)	10/8/2009
	AEA IPT Processes and Procedures, (located at: https://share.navair.navy.mil/aeaipt/Pages/IPTHome.aspx)	5/1/2015

2.3 Industry Standards

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

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

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

2.4 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 who are 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 Program Management

The contractor shall provide recommendations on metric collection and analysis plans, procedures, and forms for measuring and analyzing software processes. The contractor shall develop, collect and analyze metric data. This includes: development of plans, procedures and forms for the collection of metrics. Potential metrics for collection include: earned value, software development and integration man-hours, software complexity, central processing unit (CPU) throughput, and input/output (I/O) throughput. Upon Government approval, the contractor shall implement and maintain software metrics developed. The results of the metrics support shall be reported in the Contractor's Progress, Status and Management Report. (CDRL A002)

3.1.1 The contractor shall host/attend meetings regarding various subjects related to the TO requirements. Meetings will be held at Government and contractor’s facilities, and may include engineering briefings conducted at various unclassified and classified DoD test ranges and facilities and contractor facilities. The contractor shall attend engineering and software design reviews and software acceptance testing program reviews, and other technical reviews and meetings for the purpose of gathering data required to develop and deliver the systems and software engineering efforts, as stated herein. The contractor shall also participate in Technical Coordination Meetings (TCMs), status meetings, Deficiency Change Review Boards (DCRBs) and other program reviews to support the tasks within this SOW. The times/dates for meetings to be hosted by the contractor will be provided at least two weeks prior to event, to the contractor via email. The contractor shall provide recommendations and conclusions based on evaluation of data acquired. (CDRL A004)

3.1.2 The contractor shall, upon written Government approval, develop technical, engineering, and presentation graphics, and other visual aid requirements, to reflect the status of assigned tasks under this SOW. (CDRL A004)

3.1.3 The contractor shall develop and maintain plans, milestone charts, perform reviews, conduct analyses, complete evaluations and make recommendations, which will provide the technical and scientific evidence necessary to facilitate program development decisions. (CDRL A001)

3.1.4 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 (Summary). In addition, the contractor shall provide task execution highlights and labor expenditure reporting. (CDRLs A002 and A003)

3.1.4.1 The contractor shall provide highlights and status reporting. (CDRL A002)

3.1.4.2 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 A003)

3.1.4.3 The contractor shall develop and deliver a report that provides 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 report to the Contracting Officer's Representative (COR) and the Navy Technical Representative. (CDRL A002)

3.2 Systems/Software/Test Engineering

The contractor shall provide systems engineering support in accordance with the NAVAIR Systems Engineering Guide and Systems Engineering Process as specified under section 2.0. Systems engineering shall include planning, analysis, design, development, fabrication of new and existing EW laboratories, prototyping, procurement, integration, test, evaluation, operation, repair, maintenance, upgrade, and documentation the system software and firmware.

3.2.1 SHEELD is planning to change programming languages, but this has not been decided yet. The contractor shall develop SHEELD software using C#, Visual Basic or selected programming languages under Windows operating, mobile or Web/Services, build data and test Mission Data Libraries (MDLs) in support the AN/ALQ-210 and AN/ALQ-217 ESM. The contractor shall provide software development and configuration management support for the SHEELD software application in accordance with IPT and government specifications, analyze requirements, produce preliminary and detail design as well as maintain and produce code and data for the SHEELD application. The contractor shall provide testing support for build tests (under Joint Mission Planning System or any other framework environment), Independent Verification and Evaluation (IV&V), Development Test and Evaluation (DT&E), and Operational Test and Verification at specific test sites. Specific test sites will be provided to the contractor via electronic mail two weeks prior to occurrence. Testing support includes: developing and updating test procedures and test plans, Software Change Procedure (SCP) verification in accordance with operational requirements which are defined in the Mission Requirements Specification (MRS), troubleshooting, analyzing, and recommending corrective actions and upon government approval, integrate the corrective action. The data test environment is established under a receiver hot-bench to which signals of interest are tested against a simulated threat injection. The contractor shall provide the results of the analysis in written problem investigation reports or identify problem in the form of computer Software Problem Report (SPR). The results of field testing shall be reported in a Trip Report. (CDRLs A001, A005 and A006)

3.3 Configuration Management (CM)

The contractor shall perform configuration management of the Computer Software Configuration Items (CSCIs) using IPT approved policies and processes. The contractor shall conduct CM life cycle management and planning, configuration identification, configuration control, status accounting, configuration verification and audits, and data management using IPT approved standards and processes with IPT approved CM tools including CM Synergy, Rational ClearQuest/ClearCase, DOORS, and Process Max. The contractor shall perform software CM functions including software merges, baseline updates, status accounting, ECP support, CDRL tracking, support CCB and milestone reviews, and conduct audits to ensure that the software and documentation baselines are comprised of the specified software modules, libraries, requirements, and support documentation. These actions will be assigned by the Project Software Manager, or designee, per the AEA IPT processes. The results of CM audits and activities shall be reported in the Contractor's Progress, Status and Management Report. (CDRLs A001 and A002)

4.0 PERSONNEL QUALIFICATIONS.

4.1 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.

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

4.3 **College Degree:** All degrees shall be obtained from an "accredited college or university" as recognized and approved by the U.S. Department of Education Database of Accredited Postsecondary Institutions and Programs as of award date. This includes Associates, Bachelor's, Master's, or Doctorate degrees.

4.4 **Degree Majors:** Degree/Major requirements per each labor category listed in 4.5 are specified below.

4.5 **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 six years within the last ten years in their applicable labor category.

4.6 **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
Program Manager	Journeyman	11-1021	Plan, direct, or coordinate activities in such fields as electronic data processing, information systems, systems analysis, and computer programming. Requires at least six (6) years of professional experience in the Defense acquisition, and three (3) years of experience in support of Navy Acquisition management. Experience with aircraft systems, hardware and software, configuration control, test and evaluation, systems integration, and systems supportability. Experience in initiating and maintaining technical direction within broad program objectives directly related to aircraft systems, hardware and software, configuration control, test and evaluation, systems integration, and systems supportability. Knowledgeable of acquisition policies and procedures. Demonstrated knowledge of and experience with the requirements of the DOD 5000 series. Demonstrated ability to work with large and diverse teams and the ability to effectively provide guidance, direction, and supervision in all areas of contracted effort such as program management, systems engineering, major system acquisitions, and financial management.	SECRET
Systems Engineer/ Engineer V	Senior	17-2011	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.	SECRET
Software Engineer/ Engineer IV	Journeyman	17-2199	Responsible for the detailed design, implementation, and testing of 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.	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	Technical Report – Study/Services

A002	Contractor's Progress, Status and Management Report
A003	Performance and Cost Report
A004	Presentation Agenda, Minutes, Materials
A005	Revision to Existing Government Documents
A006	Test/Inspection Report
A007	Program Protection Implementation Plan (PPIP)

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 (1) week) to the COR for approval. The estimated travel for the performance period of five (5) years is documented below:

Total estimated # of trips	Estimated # of days per trip	Estimated # of personnel per trip	From	To
10	4	1	Point Mugu, CA	Jacksonville, FL
10	5	1	Point Mugu, CA	San Diego, CA

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 may 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 Electronic Warfare Database Support (EWDS) Lab and other AEA/EA-6B laboratories on an as-needed basis during normal operating hours. The contractor shall provide a list to the EWDS Lab manager of the personnel with the "need to know" for access to the EWDS 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 task order.

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 AEA/EA-6B documentation that includes the following:

- System/Segment Specification
- Software Requirements Specification
- Interface Design Specifications
- Program Package Documents
- Interface Design Documents
- Software Development Specification

- Functional Operational Specifications
- Program Performance Specifications
- Data Base Design Specifications
- SHEELD WBS

6.3 Place of Performance: Approximately 94% of performance is expected to take place at Point Mugu, CA at a Government facility and 5% at the contractor's facility. The other 1% will take place at other Government installations identified in section 6.1. Support for these sites, including direct Fleet services that require SECRET clearance will be required.

6.4 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. Up to eight (8) workstations or Government spaces may be provided as required.

6.5 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, workstations or Government spaces will include a desk and access to a phone, fax machine, copier, and scanner, as required, including 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 $10,000. 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 A007)

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.

9.5 Public Release:

Disclosure of information is covered by DFARS 252.204-7000 Disclosure of Information and to be incorporated in Section I of the contract.

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 AEA IPT 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."