PEO-STRI-14-W097
STOC II-15-KOP-0001
Enclosure 1: SOW
Amendment 0001
24 July 2015

Statement of Work
For
Live, Virtual, Constructive – Integrating Architecture (LVC-IA) Enhanced Capability (EC)

U.S. Army Program Executive Office for
Simulation, Training, and Instrumentation (PEO STRI)
12350 Research Parkway
Orlando, FL 32826-3276

PEO-STRI-14-W097
STOC II-15-KOP-0001
24 July 2015

Prepared by the:

Product Manager Warrior Training Integration (PM WTI)

X TRAN.HOANG.OANH.T.1232216553 Digitally signed by TRAN.HOANG.OANH.T.1232216553 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USA, cn=TRAN.HOANG.OANH.T.1232216553 Date: 2015.07.29 13:45:13 -04'00'

Prepared by:
Chief Engineer

Ms. Oanh Tran, PM ITE LVC-IA

X

Approval:
APM

Mr. Richard A. Link, PM ITE LVC-IA

PEO-STRI-14-W097
STOC II-15-KOP-0001
24 July 2015

VERSION	DOCUMENT DATE	REVISION / CHANGE DESCRIPTION	PAGES AFFECTED
1.0	24 July 2015	Final RFP Pkg	All

TABLE OF CONTENTS

1. SCOPE 1
1.1 BACKGROUND 1
2. APPLICABLE DOCUMENTS 2
2.1 DEPARTMENT OF DEFENSE DOCUMENTS 2
2.2 AVAILABILITY OF DEPARTMENT OF DEFENSE DOCUMENTS 3
2.3 OTHER GOVERNMENT DOCUMENTS 3
2.4 AVAILABILITY OF GOVERNMENT DOCUMENTS 4
3. REQUIREMENTS 4
3.1 PROGRAM MANAGEMENT 4
3.1.1 INTEGRATED MASTER PLAN (IMP) 5
3.1.2 INTEGRATED MASTER SCHEDULE (IMS) 5
3.1.3 FINANCIAL MANAGEMENT 5
3.1.4 EARNED VALUE MANAGEMENT 6
3.1.4.1 SUBCONTRACTOR MANAGEMENT 6
3.1.5 INTEGRATED BASELINE REVIEW (IBR) 7
3.1.6 INTEGRATED PRODUCT TEAMS (IPTs) 7
3.1.6.1 IPT MEETINGS 8
3.1.6.2 CONFIGURATION MANAGEMENT 8
3.1.6.3 CONFIGURATION CHANGE MANAGEMENT 8
3.1.6.4 SOFTWARE CONFIGURATION MANAGEMENT 9
3.1.6.5 ENGINEERING CHANGE PROPOSAL 9
3.1.7 TECHNICAL PERFORMANCE MEASURES (TPM) 9
3.1.8 RISK MANAGEMENT 9
3.1.9 MANAGEMENT AND TECHNICAL REVIEWS 10
3.1.9.1 START OF WORK MEETING 11
3.1.9.2 POST AWARD CONFERENCE 11
3.1.9.3 PROGRAM MANAGEMENT REVEWS (PMRs) 11
3.1.9.4 TECHNICAL REVIEWS 11
3.1.9.5 TECHNICAL INTERCHANGE MEETINGS (TIMs) 12
3.1.10 INTEGRATED DIGITAL ENVIRONMENT (IDE) 12
3.1.10.1 THE IDE DEVELOPMENT AND INSTALLATION 13
3.1.10.2 IDE ADMINISTRATION 13
3.1.10.3 IDE DATA MANAGEMENT 14
3.1.10.4 IDE DATABASE MANAGEMENT 14
3.1.10.5 LVC-IA WEB PORTAL 14
3.1.10.6 DEVELOPMENT ENVIRONMENT CYBERSECURITY ACCREDITATION 14

3.1.11 ANTITERRORISM (AT)/OPERATIONS SECURITY (OPSEC) 15
3.1.11.1 AT LEVEL 1 TRAINING 15
3.1.11.2 ACCESS AND GENERAL PROTECTION POLICY AND PROCEDURES FOR CONTRACTOR REQUIREING COMMON ACCESS CARD (CAC) 15
3.1.11.3 AT AWARENESS TRAINING FOR US BASED CONTRACTOR PERSONNEL TRAVELING OVERSEAS 16
3.1.11.4 iWATCH TRAINING 16
3.1.11.5 ARMY TRAINING CERTIFICATION TRACKING SYSTEM (ATCTS) REGISTRATION FOR CONTRACTOR EMPLOYEES WHO REQUIRE ACCESS TO GOVERNMENT INFORMATION SYSTEMS 16
3.1.11.6 OPSEC PROGRAM 16
3.1.11.7 REQUIREMENT FOR OPSEC TRAINING 16
3.1.11.8 CYBERSECURITY/INFORMATION TECHNOLOGY (IT) TRAINING 16
3.1.11.9 CYBERSECURITY/IT CERTIFICATION 17
3.1.11.10 PERFORMANCE OR DELIVERY IN A FOREIGN COUNTRY 17
3.1.11.11 HANDLING OR ACCESS TO CLASSIFIED INFORMATION 17
3.1.11.12 THREAT AWARENESS REPORTING PROGRAM 17
3.2 SYSTEMS ENGINEERING 17
3.2.1 SYSTEM DESIGN 18
3.2.1.1 SYSTEM DEFINITION STAGE 19
3.2.1.2 PRELIMINARY DESIGN STAGE 19
3.2.1.3 DETAILED DESIGN STAGE 20
3.2.1.4 ASSEMBLY, INTEGRATION AND TEST STAGE 21
3.2.1.5 OPEN SYSTEMS DESIGN APPROACH AND GOALS 22
3.2.2 HARDWARE ENGINEERING 23
3.2.3 SOFTWARE ENGINEERING 24
3.2.3.1 SOFTWARE REQUIREMENTS AND ARCHITECTURE DEVELOPMENT AND REVIEW 25
3.2.3.2 SOFTWARE DESIGN AND IMPLEMENTATION 25
3.2.3.3 SOFTWARE DEVELOPMENT TEST 26
3.2.3.4 TECHNOLOGY REFRESH 26
3.2.3.5 TECHNOLOGY DEVELOPMENT AND INSERTION 27
3.2.3.6 MODIFICATION/SYSTEM UPGRADES 27
3.2.4 HARDWARE AND SOFTWARE INTEGRATION 27
3.2.5 CYBERSECURITY 28
3.2.5.1 CYBERSCURITY ARTIFACTS 29

3.2.5.2 INFORMATION ASSURANCE VULNERABILITY MANAGEMENT 29
3.2.5.3 RMF ASSESS ONLY PROCESS 31
3.2.5.4 HOST-BASED SECURITY SYSTEM (HBSS) 31
3.2.6 SPECIALTY ENGINEERING 31
3.2.6.1 RELIABILITY, AVAILABILITY, AND MAINTAINABILITY (RAM) 31
3.2.6.2 SAFETY ENGINEERING 32
3.2.6.3 SAFETY ASSESSMENT 32
3.2.6.4 QUALITY ASSURANCE 32
3.2.6.4.1 TEST DISCREPANCIES 33
3.2.6.4.2 DISCREPANCY PROCESSING 33
3.2.6.4.3 TEST DISCREPANCY PRIORITY 33
3.2.7 DESIGN REVIEWS 33
3.2.7.1 SYSTEMS REQUIREMENTS REVIEW (SRR) 34
3.2.7.2 ENGINEERING DESIGN REVIEW (EDR) 34
3.2.7.3 CRITICAL DESIGN REVIEW (CDR) 35
3.2.7.4 PRODUCT DEFINITION DATA (PDD) 35
3.3 LOGISTICS 36
3.3.1 LOGISTICS SUPPORT ANALYSIS 36
3.3.2 SUPPORTABILITY ANALYSIS AND LOGISTICS MANAGEMENT INFORMATION 36
3.3.3 TECHNICAL PUBLICATIONS 37
3.3.4 ITEM UNIQUE IDENTIFICATION (IUID) 37
3.3.5 TRAINING PRODUCTS 38
3.3.5.1 NEW EQUIPMENT TRAINING (NET) 38
3.3.5.2 INSTRUCTOR/OPERATOR TRAINING 38
3.3.5.3 MAINTENANCE TRAINING 39
3.3.6 INTERIM CONTRACTOR SUPPORT 39
3.3.7 SOFTWARE SUPPORT 39
3.3.8 SITE SUPPORT 39
3.3.9 CUSTOMER SUPPORT SERVICES 40
3.3.10 TRANSITION PLANNING 40
3.4 INTEGRATED TESTING 40
3.4.1 TEST READINESS REVIEW (TRR) 41
3.4.2 SYSTEM MEASUREMENT PERFORMANCE (SMP) EVENT 42
3.4.3 GOVERNMENT ACCEPTANCE TEST (GAT) 43
3.4.4 PRODUCTION AND FIELDING READINESS REVIEW 43
3.4.4.1 EQUIPMENT RECORD 44

3.4.5 **FIRST USE ASSESSMENT (FUA)** 44
3.5 **SITE ACTIVATION** 44
3.5.1 **INSTALLATION PROGRAM** 45
3.5.2 **INSTALLATION SPARES** 45
3.5.3 **ON-SITE ACCEPTANCE TEST** 45
3.6 **SYSTEM TECHNICAL SUPPORT** 45
3.6.1 **POST DEPLOYMENT SOFTWARE SUPPORT** 46
3.6.1.1 **HELP DESK SUPPORT** 46
3.6.1.2 **PROBLEM TROUBLE REPORT (PTR) PROCESS** 47
3.6.1.3 **PRODUCTION & DEPLOYMENT PROCESS** 49
3.6.1.4 **MAINTAINER/OPERATOR UPGRADE & TECHNICAL REFRESH TRAINING** 49
3.7 **INTELLECTUAL PROPERTY AND DATA RIGHTS** 49
4. **ACRONYM LIST** 50

PEO-STRI-14-W097
STOC II-15-KOP-0001
24 July 2015

1. SCOPE

This Statement of Work (SOW) defines the effort required for designing, developing, integrating, testing, managing, documenting, delivering, and Post Deployment Software Support (PDSS) of the Live, Virtual, Constructive Integrating Architecture (LVC-IA) Enhanced Capability (EC).

LVC-IA increment 1 provides the interoperability and integration tools within the Modeling and Simulations (M&S) community to Train as you Operate within the Live, Virtual, Constructive Integrated Training Environment (LVC-ITE) for Brigade commanders, battle staffs and individual soldiers on tactical-level collective tasks. The LVC-IA capability integrates Mission Command (MC) applications and systems and supports the Common Operating Environment (COE) by virtualizing the system operating in the Cloud.

The LVC-IA will provide the Army a significantly wider range of capabilities among the Mission Training Complex (MTC) to maximize data initialization and integration effects of multiple simulation architectures and enable LVC collective non-distributed and distributed training. The LVC-IA will populate a single Common Operating Picture with friendly, enemy, neutral, and noncombatant entities from the participating Live, Virtual and Constructive Training Aids, Devices, Simulators and Simulations (TADSS). LVC-IA is the key enabler for the interoperability and linkage of the LVC-ITE.

The LVC-IA will provide a standardized set of common protocols, specifications, standards, processes, and interfaces for data management across the training environments within the LVC-IA family of systems and consistent with the geospatial foundation of mission command systems.

LVC-IA will incorporate future systems and capabilities, including emerging technologies, facilitating a building block approach that integrates and updates the LVC training environment. This strategy supports an evolutionary development approach that provides opportunities to leverage commercial developments for fielding expanded capabilities.

1.1 BACKGROUND

In FY10, a small-business competition was conducted using the Simulation and Training Omnibus Contract (STOC II) Lot II contracting vehicle. As a result, the LVC-IA program awarded contract W900KK-09-D-0532, Delivery Order 0002, with contract period of performance of 30 Jun 10 – 29 Jun 15, consisting of a two (2) year base and three (3) one year option periods. This contract was structured for development in accordance with an approved Capability Development Document (CDD) in an evolutionary manner with 4 pre-planned increments. Upon completion of version 1, the resulting Capability Production Document (CPD) replaced the multi-increment evolutionary model with a single increment, multi-version model

where subsequent versions, based on the requirements provided by the LVC-IA Requirements Oversight Board, will provide enhanced LVC-IA capabilities. With each version, the contract provided for fielding and training version capability to the designated Basis Of Issue Plan (BOIP) sites and Post Deployment Software Support (PDSS) for all currently fielded versions.

Version 1.0 facilitates the interoperability between Training Aids Devices Simulators Simulation (TADSS) with Mission Command System. The TADSS Core Systems include: Live Environment - Home Station Instrumentation Training System (HITS); Virtual Environment-Close Combat Tactical Trainer (CCTT), Aviation Combined Arms Tactical Trainer (AVCATT); Constructive Environment - Joint Land Component Constructive Training Capability-Entity Resolution Federation (JLCCTC-ERF) and Gaming Environment – Virtual BattleSpace 3 (VBS3).

Version 2.0, will incorporate additional system capabilities and emerging technologies including: SIPRNET connection; Bi-Directional Mission Command (MC) Cross Domain Solution rule sets; Distributed operations; Increased entity counts; and Dismounted Soldier Training System (DSTS) through CCTT. Due to the variability in the timing of DSTS requirements definition, DSTS is at risk of not making it into V2 and potentially moving into a later version.

2. APPLICABLE DOCUMENTS

Applicable documents supporting work to be performed under this SOW are listed below. In the event of a conflict between documents referenced herein and the contents of this SOW, the contents of the SOW shall be the governing requirement.

2.1 DEPARTMENT OF DEFENSE DOCUMENTS

CNSSI 1253	Security Categorization and Controls Selection for National Security Systems (NSS) and National Security Information (NSI)
DFARS clause 252.225-7043	Antiterrorism/Force Protection for Defense Contractors Outside the US
DFARS 252.234-7001 /7002	Note of Earned Value Management System (Apr 2008) Earned Value Management System (EVMS) (May 2011)
DFARS 252.239.7001	Information Assurance Contractor Training and Certification
DOD 8570.01-M	Information Assurance Workforce Improvement Program
DODI 5000.64	Accountability and Management of DOD Equipment and Other Accountable Property
DODM 5200.01	Information Security Program, Volumes 1 thru 4
DODI 5220.22	National Industrial Security Program (NISP)

DODI 8500.01	Cybersecurity
DODI 8510.01	Risk Management Framework (RMF) for DOD Information Technology (IT) (March 12, 2014)
DODI 8580.1	Information Assurance (IA) in the Defense Acquisition System
DODAF v1.5	Department Of Defense Architecture Framework (DODAF) (23 Apr 2007)
FAR 52.204-2	Security Requirements
FAR 52.204-9	Personal Identity Verification of Contractor Personnel

2.2 AVAILABILITY OF DEPARTMENT OF DEFENSE DOCUMENTS

Copies are available on the WWW at URL: https://assist.dla.mil/online/start/
Copies are available on the WWW at URL: http://www.dtic.mil/whs/directives/

2.3 OTHER GOVERNMENT DOCUMENTS

AR 25-2	Information Assurance
AR 25-1	Army Information Technology
AR 25-30	Army Publishing Program
AR 380-5	Department of the Army Information Security Program
AR 380-53	Communications Security Monitoring
AR 381-12	Military Intelligence Threat Awareness and Reporting Program
AR 525-13	Antiterrorism
AR 530-1	Operations Security (OPSEC)
COE DC CE	COE DC CE Architecture Compliance Checklist, (V2.0.2, dated 1 June 14)
CSPAR	PEO STRI Policy on the Use of Common Standards, Products, Architectures and/or Repositories (CSPAR)
GFE	Government Furnished Equipment (GFE)
LVC-IA CDD	LVC-IA Capability Development Document (CDD) (23 Sep 2009)
LVC-IA CPD	LVC-IA Capability Production Document (CPD) (14 Nov 2012); and Memorandum, U.S. Army Combined Arms Center - Training (CAC-T), Subject: Live Virtual Constructive – Integrating Architecture (LVC-IA) Version 3 Requirements (Feb 2015)
MIL-STD-130N	Identification Marking of US Military Property, paragraph 5.2
MIL-STD-882E	Standard Practice For System Safety
MIL-STD-31000A	Technical Data Packages (TDP)

MIL-STD-40051-1/-2B	Manuals, Technical; Operation and Maintenance Instructions for Training Devices Preparation of Digital Technical Information for Page-Based Technical Manuals
NIST SP 800-53	National Institute of Standards and Technology Special Publication, Security and Privacy Controls for Federal Information Systems and Organizations
SAE-GEIA-STD-0007	Logistics Product Data
SOP 70-1	PEO STRI Standard Operating Procedure
W900KK-09-D-0532 D.O. 0002	Live, Virtual, Constructive – Integrating Architecture (LVC-IA) and Infrastructure

2.4 AVAILABILITY OF GOVERNMENT DOCUMENTS

Copies of the other documents are available from PEO STRI (PM ITE-WTI), 12350 Research Parkway, Orlando, FL 32826-3275. ATTN: Ms. jacqueline.e.bushway.civ@mail.mil

3. REQUIREMENTS

It is anticipated that this LVC-IA EC effort will include Versions V3 and V4 development (2 year development cycle each); V3 and V4 integration & test, Government Acceptance Test (GAT) and First Use Assessment (FUA) for each version; PDSS/Site Support/Spares for V2.x to V4.x throughout the contract period of performance as each version is fielded; fielding version upgrades from V l.x to V2.x, V2.x to V3.x, and V3.x to V4.x at each of the 14 sites (11 continental United States (CONUS) and 3 outside continental United States (OCONUS)) at an estimated two year cycle for each upgrade; and potentially one site activation. Technical refresh will occur once every 5 years (3 sites/year); however, in FY17-19 the program will provide this refresh as part of version 2.0 fielding. These efforts will be concurrent activities that will require continued production and fielding/upgrades of the LVC-IA systems to the remaining BOIP sites.

LVC-IA (1 system each) BOIP site locations include:
FY12: Ft. Hood, TX
FY13: Ft. Bliss, TX; Ft. Campbell, KY; Ft. Drum, NY; Camp Casey, Korea
FY14: Ft. Stewart, GA; Ft. Riley, KS; Ft. Carson, CO; Schofield Barracks, HI
FY15: Ft. Bragg, NC; Joint Base Lewis-McCord, WA
FY16: USARAK; Ft Benning, GA (Center of Excellence); Ft. Polk, LA

3.1 PROGRAM MANAGEMENT

The Contractor shall provide the overall management and administrative effort necessary to ensure that the requirements of this contract are accomplished for the contract period of performance. The Contractor shall plan, implement, and maintain a life cycle cost (LCC)

management process to minimize the system cost and use LCC to conduct trade studies, evaluate design and support alternatives, and select the resource support requirements. The Contractor shall define and monitor metrics and technical performance measures (TPMs) to evaluate the performance of each critical technical and management process and conformance of the evolving products with contract requirements and objectives including cost requirements and objectives.

(DI-MGMT-80227) Contractor's Progress, Status, and Management Report
Ref: CDRL B001

3.1.1 INTEGRATED MASTER PLAN (IMP)

The Contractor shall implement, manage to, update, and maintain the contract IMP. The Contractor shall develop the system in accordance with the IMP. The IMP shall be used throughout the contract as a management tool to assess progress and determine success in achieving program requirements. The Contractor shall report on work in progress in accordance with the IMP at each program review, at selected technical reviews and at government discretion. The IMP shall depict the contract work breakdown structure.

3.1.2 INTEGRATED MASTER SCHEDULE (IMS)

The Contractor shall develop, implement, manage to, update, and maintain the contract IMS. All contract schedule information delivered or presented at program reviews shall originate from the IMS, shall be traceable to the IMP, and shall contain all critical events and exit criteria, accomplishments, predecessors and successors events, and their dependencies. The IMS shall address total program activities including activities performed by major Subcontractors. The Contractor shall develop the logic resource loaded network that accurately portrays the sequence and relationship of activities defining the total development and production program. These activities shall be keyed to the Contract Work Breakdown Structure (CWBS). The activities time and cost data shall be updated to reflect accomplished activities and any changes in activity time and cost estimates. The Contractor shall conduct critical path analysis of the tasks and identify problem areas and corrective actions required to eliminate or reduce schedule impacts.

(DI-MGMT-81861) Integrated Program Management Report (IPMR): IMS
Ref: CDRL B002

3.1.3 FINANCIAL MANAGEMENT

The Contractor shall plan, budget, schedule, and control the resources allocated to meet the requirements of the contract. The Contractor shall document and track the status of all appropriated funds associated with the contract to include payments, cancellations and invoices against each contract line item and subline item. The Contractor shall extend the government-provided Program Work Breakdown Structure to lower levels in the Contractor's CWBS. It defines the lower level components of what is to be procured and includes all the product

elements (hardware, software, data, or services), which are defined by the Contractor and the Contractor's responsibility.

The extended CWBS shall serve as the framework for contract planning, budgeting, and reporting of cost and schedule status. The Contractor shall identify major elements of subcontracted work in the extended CWBS. The Contractor may propose changes to the CWBS to enhance its effectiveness in satisfying program objectives. The Contractor shall continually update an integrated database during contract performance with pertinent records and data that underlie and support the cost and schedule data reported.

(DI-MGMT-81468) Contract Funds Status Report (CFSR)
Ref: CDRL B003
(DI-MGMT-81651) Contract Invoicing and Payment Report (CIPR)
Ref: CDRL B004
(DI-MGMT 81861) Integrated Program Management Report (IPMR): CWBS
Ref: CDRL B002

3.1.4 EARNED VALUE MANAGEMENT

The Contractor shall implement an Earned Value Management System (EVMS) in accordance with DFARS 234.201. The Contractor shall integrate cost, schedule, and performance management information. The Contractor shall develop, implement, maintain and use an EVMS that complies with Industry Guidelines ANSI/EIA-748 and meets contractual requirements. The Contractor shall document the integrated cost and schedule status of work progress on the contract and related technical performance with cost and schedule accomplishment using procedures for planning work, controlling costs and measuring performance based on ANSI/EIA-748. The Contractor shall incorporate and integrate performance information reported by Subcontractors into the Contractor's EVMS. The Contractor shall be responsible for reviewing and assuring the validity of all Subcontractors reporting.

DI-MGMT-81861 Integrated Program Management Report (IPMR): CPR
Ref: CDRL B002

3.1.4.1 SUBCONTRACTOR MANAGEMENT

The Contractor shall maintain the capability to manage Subcontractors in accordance with the Subcontractor Management Plan. The Contractor shall integrate Subcontractors into program Integrated Product Teams and program management and tracking systems such as management information systems. The Contractor shall ensure the requirements of this contract and subsequent delivery orders are applied to all subcontracts and associate contracts.

3.1.5 INTEGRATED BASELINE REVIEW (IBR)

The Contractor shall conduct IBRs in order to perform an assessment of the Performance Measurement Baseline (PMB) for the program. The initial IBR shall be conducted within 90 days of contract award and subsequent IBRs shall be conducted as required due to changes in the PMB due to modifications or restructuring to facilitate and maintain a mutual understanding of:

- The scope of the PMB consistent with authorizing documents;
- Management control processes;
- Risks in the PMB associated with cost, schedules, and resources; and
- Corrective actions where necessary.

Completion of the IBR shall result in the assessment of risk within the PMB and the degree to which the following have been established:

a. Technical scope of work is fully included and is consistent with authorizing documents.
b. Key project schedule milestones are identified and supporting schedules reflect a logical flow to accomplish the work.
c. Resources (budget, facilities, personnel, skills) are available and are adequate for the assigned tasks.
d. Tasks are planned and can be measured objectively relative to the technical progress.
e. Rationales underlying the PMB are reasonable.
f. Management processes support successful execution of the project.

The PMB shall be placed under configuration control with changes authorized only upon mutual agreement of the government and the Contractor.

3.1.6 INTEGRATED PRODUCT TEAMS (IPTs)

The Contractor shall implement and maintain an IPT structure for the duration of the contract. IPTs bring together functions that have a stake in the performance of a product or process and concurrently make decisions affecting that product or process (e.g., Requirements Analysis, Market Research, Design, Development, Integration, Test, Evaluation, and Peer Reviews). The Contractor shall apply IPTs at various levels ranging from the overall project structure to specific groups functioning across existing project units. Each IPT shall consist of Government and Contractor personnel and have Government and Contractor co-chairs. With Government input, Contractor shall define and document composition, structure, roles, and responsibilities of each IPT. Each IPT shall maintain a membership list. Each IPT shall be empowered to make critical life cycle decisions regarding each product or process within their purview.

Conference Agenda and Conference Minutes shall be available in the LVC-IA Web Portal.

3.1.6.1 IPT MEETINGS

The Contractor shall coordinate and host, or participate in IPT meetings to be conducted throughout the contract period of performance. IPT meetings shall provide a forum for maintaining a continuous interchange of ideas and issues including snapshot data of Deficiency Reports status (open, closed, working, etc.) for current requirement analysis, design and test events, as agreed to by the Contractor and Government, and to identify and resolve potential problem areas. Each IPT shall publish an agenda before each meeting. Each IPT shall record and maintain meeting minutes. Meeting minutes shall be shared across IPTs.

Conference Agenda and Conference Minutes shall be available in the LVC-IA Web Portal.

3.1.6.2 CONFIGURATION MANAGEMENT

The Contractor shall use an automated internal configuration management process to monitor, update, and control all configuration documentation, physical media, and physical parts representing or comprising the system configuration items. The Contractor shall plan and implement an automated configuration management function to perform configuration control, configuration identification, audits, and status accounting in a system-engineering environment. The Contractor shall develop, maintain, and update configuration management procedures and processes for control of all hardware and software baselines. The process shall allow simultaneous access to the common product data model coupled with the ability to coordinate and update immediate changes to the product definition data. The configuration management process must handle all levels of product and process integration to build and support the product as well as manage the sequence of significant events.

(DI-CMAN-80858B) Contractor's Configuration Management Plan
Ref: CDRL A00I

3.1.6.3 CONFIGURATION CHANGE MANAGEMENT

The Contractor shall establish a systematic and measurable configuration change management process for managing product configuration changes and variances. Once the system requirements have been approved by an authorized management activity, the Contractor shall effect changes to the baseline requirements only after the proposed change has been approved using the change process. The Contractor shall:

a. Document and uniquely identify each change.
b. Classify requested changes to aid in determining the levels of review and approval.
c. Clearly and completely document request for change.
d. Consider the technical, support, schedule, and cost impacts of a requested change before making a judgment to approve the change for implementation and incorporation in the system and its documentation.

e. Determine potential effects of a change and coordinate impacts with the impacted areas of responsibility.
f. Determine the effectivity for each change and identify which units of the system are to be changed and which units will be included in a retrofit.
g. Verify implementation of a change to ensure consistency between the system, its documentation, and its support elements.
h. Document variances, when authorized by the appropriate level of authority.

3.1.6.4 SOFTWARE CONFIGURATION MANAGEMENT

The Contractor shall establish and document a software configuration management process. The Contractor's software configuration management plan may be incorporated into the software development process plans or may be a separate configuration management plan.

(DI-CMAN-80858B) Contractor's Configuration Management Plan
Ref: CDRL A00I

3.1.6.5 ENGINEERING CHANGE PROPOSAL

The Contractor shall document and the IPT shall review all changes to established baselines and all changes to the requirements (other than the functional baseline), including changes to the SOW, the CDRL, and the general provisions of the contract.

3.1.7 TECHNICAL PERFORMANCE MEASURES (TPM)

The Contractor shall select technical performance parameters that reflect key indicators of program success. TPM parameter inter-relationships shall be depicted through construction of tiered dependency trees similar to the specification tree. Each parameter shall be correlated with a specific CWBS element. Parameters to be reported at each management review shall be selected from the total parameters tracked and shall be identified in the integrated master plan. As the design and development activity progresses, the achievement to data shall be tracked continually for each of the selected technical performance parameters. If the data falls outside the tolerance band a new profile or current estimate shall be developed immediately. The current estimate shall be determined from the "achievement to date" and the remaining time and budget. An analysis shall be accomplished on the variation to determine the causes and to assess the impact on higher level parameters, on interface requirements, and on system cost effectiveness. For performance in excess of requirements, opportunities for reallocation of requirements and resources shall be assessed.

3.1.8 RISK MANAGEMENT

The Contractor shall prepare, implement and maintain a risk management process that includes identification, analysis, mitigation planning, mitigation plan implementation and tracking. The

Contractor shall develop and implement cybersecurity risk management, which will include security safeguards. These safeguards shall include but are not limited to local policy and guidance, identifies threats, problems and requirements, and adequately plan for the required resources. The Contractor's risk management process shall measure future uncertainties in achieving program goals within defined cost, schedule, and performance constraints. The cybersecurity risk shall be addressed across the risk management process and can be addressed in multiple areas.
The Contractor shall develop, submit, and maintain a Risk Management Plan as part of the Systems Engineering Management Plan (SEMP) to document Risk Management procedures and processes. The Contractor shall execute Risk Management in accordance with (IAW) the Risk Management Plan.

The Contractor shall:

a. Identify and document moderate and high-risk items for each risk assessment area.
b. Identify and implement risk handling approaches and track over time each moderate and high-risk item.
c. Develop risk tree with risk triggers and mitigation paths for each high risk item.
d. Document risk issues that have been successfully resolved and schedule each open item into the program IMS.
e. Develop and deliver to the Government mitigation plans to identify the recommended critical path for contract completion and the appropriate risk handling approach to lower the level of uncertainty identified.

(DI-MISC-80711A) Scientific and Technical Reports: Risk Management Report
Ref: CDRL A003
(DI-SESS-81785) Systems Engineering Management Plan (SEMP)
Ref: CDRL A00C

3.1.9 MANAGEMENT AND TECHNICAL REVIEWS

The Contractor shall conduct periodic program reviews at their own or government facilities. The Contractor is responsible for providing visibility on the progress, performance, and status of major Subcontractors. The Contractor shall be responsible for documenting, coordinate resolution and track action items until closure. The Contractor shall be responsible for generating minutes of all meetings/reviews and provide them to the Government.

Conference Agenda and Conference Minutes shall be available in the LVC-IA Web Portal.

3.1.9.1 START OF WORK MEETING

A start of work meeting shall be held at PEO STRI after contract award. The start of work meeting shall be limited to the Contractor's key team members identified in the proposal, and the emphasis will be on top level management of the program, agreement on metrics that will be used as management indicators during the program and partnering approach to implement.

3.1.9.2 POST AWARD CONFERENCE

A post award conference shall be held at the Contractor's facility at a mutually agreed to date after the start of work meeting. The conference shall introduce the key IPT participants, identify points of contact and discuss both parties understanding of the scope of work and other contract issues.

3.1.9.3 PROGRAM MANAGEMENT REVEWS (PMRs)

Program Management Reviews shall be conducted at the Government facilities with an initial PMR to be held no more than 90 days after contract award and on a date mutually agreed to by the Procuring Contracting Officer and Contractor. PMRs shall include status of design documentation, hardware and software design status, risk and problem identification, subcontract management, data collection and modeling, logistics planning, financial data and test planning. Program Reviews shall also address provisioning, training and technical publications status. The Contractor is responsible for providing visibility on the progress, performance, and status of major Subcontractors. The Contractor shall also be responsible for generating minutes of the meetings and provide them to the Government. The Contractor shall document action items, coordinate resolution and track action items until closure.

Conference Agenda and Conference Minutes shall be available in the LVC-IA Web Portal.

3.1.9.4 TECHNICAL REVIEWS

The Contractor shall conduct reviews, to include requirements and design reviews (system, subsystem, test readiness, production readiness), for the purpose of assessing technical progress. The design reviews shall be conducted at the completion of each application of the system-engineering phase. Each review shall accomplish the following:

a. Assess the system requirements and allocations to ensure that requirements are unambiguous, consistent, complete, feasible, verifiable, and traceable to top-level system requirements. (System Requirements Review).
b. Present the risks associated with a continued development effort.
c. Assess the life cycle processes and infrastructure necessary for product sustainment throughout the system life cycle.
d. Identify resources (cost and schedule) required for continued development.

e. Determine whether to proceed with the next application of the systems engineering process, to discontinue development, or to take corrective actions before proceeding with the development effort. (Readiness Reviews).
f. The Contractor shall support technical interchange meetings (TIMs) to address specific topics or issues, address status of development or test activities between management reviews, address the functions of an established working group, or coordinate and provide guidance for engineering data or technical publications.

Trade-off analysis and verification results should be available during design reviews in order to substantiate design decisions. Component, subsystem, and system functional- and design-configuration audits shall be performed to ensure that supporting documentation has been satisfactorily completed, that qualification tests for each specification requirement have been completed and all requirements satisfied or products comply with final drawings.

Conference Agenda and Conference Minutes shall be available in the LVC-IA Web Portal.

3.1.9.5 TECHNICAL INTERCHANGE MEETINGS (TIMs)

The Contractor shall conduct and participate in technical interchange meetings to be held at both Contractor and Government facilities. The specific locations, dates, and duration of the meetings shall be as specified in the IMS. The meetings shall be co-chaired by a Government and Contractor representative. The Contractor shall be prepared to explain the reasoning, assumption, and methodologies in arriving at particular conclusions, recommendations, or alternatives in the accomplishment of the tasks required by the contract. The Contractor shall prepare drawings and other data, as required, to aid in the presentations. The Contractor shall have all the required personnel and resources present. The Contractor shall make available facilities for Government only meetings. These Government meeting facilities shall include direct internet access for Government personnel laptops. The Contractor shall ensure cell phone access throughout the Contractor's meeting facility. The Contractor shall prepare the meeting agenda and document the meeting results. Except where noted herein, meetings shall be considered fulfilled when all of the following items are completed:

- A formal review meeting has been conducted
- All action items requiring Contractor response have been documented and posted in the LVC-IA Web Portal.

3.1.10 INTEGRATED DIGITAL ENVIRONMENT (IDE)

The Contractor shall establish, maintain and manage an interactive, online, protected, and access controlled IDE, such that the Government and Contractor team members can exchange program information. The Contractor shall include software applications and database services for the generation, integration, storage, indexing, distribution, simultaneous on-line sharing of digital data among all government and Contractor team members, and delivery of technical data

products with associated Contractors, Subcontractors and Government organizations. The IDE shall provide program personnel complete visibility into the system at every stage of development, regardless of data location. The Contractor shall ensure that everyone associated with this project has access to information they need to properly perform their duties.

3.1.10.1 THE IDE DEVELOPMENT AND INSTALLATION

The Contractor shall provide an IDE with the following capabilities:

a. Ability to capture information as it's created.
b. Ability to manage product and program management structures.
c. Real-time information sharing and work flow implementation.
d. Team access to the most current information.
e. Ability to assign rules regarding information access.
f. Common information architecture that is distributed geographically.
g. Electronic notification of changes to program and product information.
h. Ability to present a single interface to the entirety of your and your Subcontractors' data creation activities.
i. Ability to recover from unexpected loss of program data due to environmental disasters, operator error, equipment failure, and hostile intruders.
j. Ability to provide access to program data using standards defined in section 2.3 of the Joint Technical Architecture-Army, or through an open systems approach.

3.1.10.2 IDE ADMINISTRATION

The Contractor shall provide a Web based electronic data management system to facilitate the electronic data interchange of non-classified data. Except where noted specifically on the DD Form 1423, the Contractor shall provide this service for items on the data accession list, management data, and technical data generated and maintained in digital format. The Contractor shall provide the Government and Contractor team members with the capabilities for on-line review, comment, acceptance and approval of deliverable data. The Contractor shall include these comments, approvals and acceptances in the database as well as mechanisms to establish appropriate audit trails to identify the sources of these additions and to maintain configuration control. The Contractor shall develop and implement procedures for establishing and administering user accounts for the IDE. The Contractor shall provide users access to a help desk to solve user problems. The help desk shall be operational during the scheduled operation hours of the team. The Contractor shall maintain records of reported incidents and derive metrics from the data. The Contractor shall develop, maintain, and implement a user-training program to ensure users are able to operate within the IDE and understand their roles and responsibilities within the IDE processes.

3.1.10.3 IDE DATA MANAGEMENT

The Contractor shall establish, implement, and maintain a data management capability within the IDE for the integration, storage, access, management, delivery, and exchange of data furnished by the government or generated by any contract work effort including Subcontractors. The system shall be capable of maintaining a record and reporting the status of data accession and data deliveries for each unit delivered. The Contractor shall generate and maintain a master listing of all documents maintained in the training site libraries. The listing shall include all operations and maintenance publications, engineering drawings and specifications, software source code, software databases, training materials, and baseline description documents.

3.1.10.4 IDE DATABASE MANAGEMENT

The Contractor shall develop and maintain a technical information validation process to validate the adequacy and accuracy of the technical data contained within the IDE. The Contractor shall initially populate and then update operation and maintenance or engineering libraries to reflect the latest as modified configuration. These libraries shall consist of the courseware, technical publications, product definition data, software and hardware configuration and programming data required to operate and maintain a training site. The Contractor shall perform an audit of technical publications and product definition data 120 days prior to expiration of this contract and make any changes necessary to each library so that a complete set of documentation exist at each site in usable condition with the latest revisions incorporated.

3.1.10.5 LVC-IA WEB PORTAL

The Contractor shall develop and manage the LVC-IA Web Portal. All CDRLs and non-CDRL deliverables such as Equipment Inventory, Help Desk tickets, PTRs and PTR tracking, any meeting minutes, Peer Design Review notes, Risk Management tracking, TPM, and a repository of all project related documentation such as requirements, design, test, fielding, and training, shall be available in the LVC-IA Web Portal to all users approved by the Government for access. The LVC-IA Web Portal shall comply with all applicable DOD cybersecurity requirements.

3.1.10.6 DEVELOPMENT ENVIRONMENT CYBERSECURITY ACCREDITATION

The Contractor shall produce all components of the Risk Management Framework (RMF) Assess and Authorize (A&A) package with regard to all Information Technology (IT) assets and cybersecurity-enabled products for the LVC-IA Development Environment, to include the Joint Development Integration Facility (JDIF), located at 12000 Research Parkway, Suite 382, Orlando, FL 32826, and PDSS facility locations. The Contractor shall comply with the cybersecurity process in accordance with the most current standard for the effort being performed per DODI 8510.01 (RMF). The Contractor shall identify all cybersecurity requirements and include them in the design, acquisition, installation, integration and testing, operation, upgrade or replacement of all components of LVC-IA. The Contractor shall ensure that the security requirements and procedures are met in accordance with all required DOD and

Army regulations per the classification of the data being processed. For Sensitive data processing only (e.g. JDIF Dev Env) Confidentiality, Integrity and Availability (CIA) levels are Low-Low-Low, for Classified processing, the applicable CIA levels are High-Low-Low.

3.1.11 ANTITERRORISM (AT)/OPERATIONS SECURITY (OPSEC)

3.1.11.1 AT LEVEL 1 TRAINING

All Contractor employees, to include Subcontractor employees, requiring access Army installations, facilities and controlled access areas shall complete AT Level I awareness training in accordance with AR381-12 within thirty (30) calendar days after contract start date or effective date of incorporation of this requirement into the contract, whichever is applicable. The Contractor shall submit certificates of completion for each affected Contractor employee and Subcontractor employee, to the COR or to the contracting officer, if a COR is not assigned, within thirty (30) calendar days after completion of training by all employees and Subcontractor personnel. AT level I awareness training is available at the following website: https://atlevel1.dtic.mil/at.

3.1.11.2 ACCESS AND GENERAL PROTECTION POLICY AND PROCEDURES FOR CONTRACTOR REQUIREING COMMON ACCESS CARD (CAC)

Contractor and all associated Subcontractors employees shall provide all information required for background checks to meet installation access requirements to be accomplished by installation Provost Marshal Office, Director of Emergency Services or Security Office. Contractor workforce must comply with all personal identity verification requirements (FAR clause 52.204-9, Personal Identity Verification of Contractor Personnel) as directed by DOD, HQDA and/or local policy. In addition to the changes otherwise authorized by the changes clause of this contract, should the Force Protection Condition at any individual facility or installation change, the Government may require changes in Contractor security matters or processes.

Before CAC issuance, the Contractor employee requires, at a minimum, a favorably adjudicated National Agency Check with Inquiries (NACI) or an equivalent or higher investigation in accordance with Army Directive 2014-05. The Contractor employee will be issued a CAC only if duties involve one of the following: (1) Both physical access to a DOD facility and access, via logon, to DOD networks on-site or remotely; (2) Remote access, via logon, to a DOD network using DOD -approved remote access procedures; or (3) Physical access to multiple DOD facilities or multiple non- DOD federally controlled facilities on behalf of the DOD on a recurring basis for a period of 6 months or more. At the discretion of the sponsoring activity, an initial CAC may be issued based on a favorable review of the FBI fingerprint check and a successfully scheduled NACI at the Office of Personnel Management.

3.1.11.3 AT AWARENESS TRAINING FOR US BASED CONTRACTOR PERSONNEL TRAVELING OVERSEAS

All US based Contractor employees and associated Subcontractor employees must take Government provided Area Of Responsibility specific AT awareness training as directed by AR 525-13. Specific Area Of Responsibility training content is directed by the combatant commander with the unit AT Office being the local point of contact.

3.1.11.4 iWATCH TRAINING

The Contractor and all associated Subcontractors shall brief all employees on the local iWATCH program (training standards provided by the requiring activity AT Office). This local developed training will be used to inform employees of the types of behavior to watch for and instruct employees to report suspicious activity to the COR. This training shall be completed within 30 calendar days of contract award and within thirty (30) calendar days of new employees commencing performance with the results reported to the COR no later than sixty (60) calendar days after contract award.

3.1.11.5 ARMY TRAINING CERTIFICATION TRACKING SYSTEM (ATCTS) REGISTRATION FOR CONTRACTOR EMPLOYEES WHO REQUIRE ACCESS TO GOVERNMENT INFORMATION SYSTEMS

All Contractor employees with access to a Government information system must be registered in the ATCTS at commencement of services, and must successfully complete the DOD Information Assurance Awareness prior to access to the IS and then annually thereafter.

3.1.11.6 OPSEC PROGRAM

The Contractor shall develop an OPSEC Standing Operating Procedure (SOP)/Plan within 90 calendar days of contract award, to be reviewed and approved by the responsible Government OPSEC officer. This plan will include a process to identify critical information, where it is located, who is responsible for it, how to protect it and why it needs to be protected. The Contractor shall implement OPSEC measures as ordered by the commander. In addition, the Contractor shall have an identified certified Level II OPSEC coordinator per AR 530-1.

3.1.11.7 REQUIREMENT FOR OPSEC TRAINING

Per AR 530-1, Operations Security, new Contractor employees must complete Level I OPSEC training within thirty (30) calendar days of their reporting for duty. All Contractor employees must complete annual OPSEC awareness training.

3.1.11.8 CYBERSECURITY/INFORMATION TECHNOLOGY (IT) TRAINING

All Contractor employees and associated Subcontractor employees must complete the DOD cybersecurity awareness training before issuance of network access and annually thereafter. All

Contractor employees working cybersecurity/IT functions must comply with DOD and Army training requirements in DODD 8570.01, DOD 8570.01-M and AR 25-2 within six (6) months of employment.

3.1.11.9 CYBERSECURITY/IT CERTIFICATION

Per DOD 8570.01-M , DFARS 252.239.7001 and AR 25-2, the Contractor employees supporting cybersecurity/IT functions shall be appropriately certified upon contract award. The baseline certification as stipulated in DOD 8570.01-M must be completed upon contract award.

3.1.11.10 PERFORMANCE OR DELIVERY IN A FOREIGN COUNTRY

The Contractor shall comply with DFARS clause 252.225-7043, Antiterrorism/Force Protection for Defense Contractors Outside the US. Non-local national Contractor personnel must comply with theater clearance requirements.

3.1.11.11 HANDLING OR ACCESS TO CLASSIFIED INFORMATION

Contractor shall comply with FAR 52.204-2, Security Requirements. This clause involves access to information classified "Confidential," "Secret," or "Top Secret". The Contractor shall comply with (1) The Security Agreement (DD Form 441), including the National Industrial Security Program Operating Manual (DOD 5220.22-M) and (2) any revisions to DOD 5220.22-M.

3.1.11.12 THREAT AWARENESS REPORTING PROGRAM

For all Contractors with security clearances, per AR 381-12 Threat Awareness and Reporting Program (TARP), Contractor employees must receive annual TARP training by a counterintelligence agent or other trainer as specified in 2-4b.

3.2 SYSTEMS ENGINEERING

The Contractor shall implement a systems engineering process that will transform all system and cybersecurity requirements into a set of lower level performance requirements that define the system. Contractor shall ensure the successful integration of cybersecurity specifications into the system design, development, production and maintenance and ensure security engineering trades do not impact the ability of the system to meet fundamental mission requirements. The process shall accomplish planning, identify and allocate functional requirements, identify participation in trade studies, provide inputs to documentation, and include design reviews. The systems engineering effort shall integrate all elements of a multifunctional engineering effort to meet system requirements. The Contractor shall ensure the timely integration of engineering specialties such as reliability, maintainability, security engineering, logistics engineering, human factors engineering, safety, value engineering, standardization, and transportability into design and development. The Contractor shall develop and complete all planned IMS tasks for each

milestone. The Contractor shall as part of the systems engineering effort, develop, update and maintain the SEMP as a living document. The Contractor shall use the SEMP to identify and assure control of the overall technical management process.

The Contractor shall perform data management across the LVC-IA Family of Systems (FoS). The Contractor shall lead the analysis with the Core Systems to determine the interactions, entities, munitions, obstacles and supported data elements. As part of their systems engineering processes, the Contractor shall implement a methodology to align the data that is required for integration, testing, fielding and exercise preparation activities.

(DI-SESS-81785) Systems Engineering Management Plan (SEMP)
Ref: CDRL A00C

3.2.1 SYSTEM DESIGN

The Contractor shall assess the extent to which LVC-IA CPD capabilities have been addressed through current initiatives. The Contractor shall anticipate and assess the impact, including those affecting cybersecurity, of external changes on the LVC-IA FoS and constituent systems. The Contractor shall understand the systems that contribute to the FoS and their relationships and shall develop a detailed architecture for LVC-IA. The Contractor shall develop a design for the LVC-IA FoS that acts as a persistent framework for evaluating new FoS requirements and materiel solution options.

The Contractor shall maximize government off the shelf (GOTS) component availability and support an open source, evolutionary development approach. The Contractor shall perform trade studies to help determine currently available training capabilities for potential integration reuse. This will include both commercial-off-the-shelf (COTS) and Government-owned capabilities.

The design concept shall incorporate a modular open systems approach which shall be based on an engineering and business strategy to choose specifications and standards adopted by industry best practices and standards bodies for selected system interfaces, products, practices and tools. Selected designs and specifications shall be based on performance, cost, industry acceptance, long term availability and supportability, and upgrade potential. This effort shall be developed in an IPT environment that facilitates frequent, convenient, and collaborative face to face interchanges with the Government team.

(DI-MGMT-81644A) DOD Architecture Framework Documentation
Ref: CDRL A001

3.2.1.1 SYSTEM DEFINITION STAGE

The Contractor shall translate LVC-IA CPD requirements into FoS capabilities. Once the program and system requirements are identified, documented, and coordinated with the LVC-IA team, the requirements need to be placed under change control so proposed changes can be carefully managed. The Contractor shall define the functions, performance characteristics and environment for LVC-IA to meet the requirements of the CPD. The Contractor shall complete the system, product, and subsystem interface requirements and definition; establish a system baseline; and complete technical reviews. The documentation generated during system definition shall be used to guide subsystem development. The technical reviews shall evaluate the maturity of the system development and the readiness to progress to subsystem definition.

The system definition shall be reviewed to ensure that:

a. The design is sufficiently mature to meet systems engineering criteria.
b. System functional requirements and system non-functional requirements (e.g., performance, design goals (e.g., modular open system approach) are identified.
c. System-level risks have been adequately addressed to justify continued development.
d. Trade-study data are adequate to substantiate that system requirements are achievable.
e. Interface requirements between human and products or subsystems have been identified, including performance, workloads, design constraints, and usability.
f. Selected cybersecurity products that are NIAP-validated or on the DOD Unified Capabilities Approved Products List (https://aplits.disa.mil/processAPList.do).
g. Decisions made in arriving at the system definition configuration are well supported by analysis, test, and other technical data.

(DI-IPSC-81431A) System/Subsystem Specification (SSS)
Ref: CDRL A002
(DI-IPSC-81434A) Interface Requirements Specification (IRS)
Ref: CDRL A00L

3.2.1.2 PRELIMINARY DESIGN STAGE

The Contractor shall initiate subsystem design and create subsystem-level definition and design-to baselines to guide component development. The Contractor shall ensure that the design considerations include systems functional requirements and the Software Requirement Specification (SRS). The Contractor shall ensure that functional design considerations integrate cybersecurity functional requirements and that these requirements are included throughout the development process. The Contractor shall decompose identified subsystem functions into lower-level functions and allocate functional and performance requirements to component-level functional and physical architectures. Each preliminary subsystem requirements and verification definition and preliminary design-to baseline shall be evolved into a subsystem requirement and

verification definition and design-to baseline. Preliminary component requirements and verification definition and build-to baselines shall be defined for the components and the subsystem being developed. Final subsystem definition shall include identification of recommended components and interfaces; resolution of subsystem-level risks; assessment of component risks; and design for quality factors to include producibility, verifiability, usability, cybersecurity, supportability, trainability and disposability for each subsystem. Subsystem reviews shall be completed for each subsystem at the completion of its preliminary design stage. The results of the evaluation shall be documented. The purpose of each review is to assure that:

a. The subsystem definition is sufficiently mature to meet systems engineering criteria.
b. The subsystem functional requirements are identified in the subsystem design and are traceable to the system functional and the SRS requirements.
c. Component allocations and preliminary component specifications are reasonable and provide a sound subsystem concept.
d. Subsystem risks have been assessed and mitigated to a level appropriate to continue development.
e. Trade-study data are adequate to substantiate that subsystem requirements are achievable.
f. Human system interfaces are identified and described in the subsystem design and are traceable to design requirements.
g. Decisions made in arriving at the subsystem configuration definition are well supported by analysis and technical data.
h. Security engineering processes are integrated into the design to achieve an integrated secure solution.

Conference Agenda and Conference Minutes shall be made available in the LVC-IA Web Portal.

(DI-CMAN-81248A) Interface Control Document (ICD)
Ref: CDRL A00G
(DI-IPSC-81431A) System/Subsystem Specification (SSS)
Ref: CDRL A002
(DI-IPSC-81433A) Software Requirements Specification (SRS)
Ref: CDRL A00B
(DI-MISC-80711A) Scientific and Technical Reports: Engineering Design Review Report
Ref: CDRL A003

3.2.1.3 DETAILED DESIGN STAGE

The Contractor shall complete subsystem design down to the lowest component level, and create a component requirements and verification definition and build-to product baseline for each component. Final component definition shall include identification of recommended parts and interfaces; resolution of component-level risks and for each component, down to the lowest sub-component, the design for quality factors to include producibility, verifiability, usability,

cybersecurity, supportability, trainability and disposability. Component reviews shall be completed for each component at the completion of the detailed design stage. The Contractor shall integrate security engineering processes into the design to achieve an integrated secure solution. The results of the evaluation shall be documented. The purpose of this review shall be to ensure that:

a. Each detailed component definition is sufficiently mature to meet measure of effectiveness and measure of performance criteria.
b. Component specifications are reasonable and provide a sound component concept.
c. Component and related life cycle process risks have been assessed and mitigated to a level appropriate to support the fabrication, assembly, integration and test phases.
d. Trade-study data are adequate to substantiate that detailed component requirements are achievable.
e. Human system interfaces are identified and described in the detailed design and are traceable to design requirements.
f. The detailed software design is described in terms of the satisfaction of functional and non-functional systems requirements.
g. Decisions made in arriving at the detailed component definition configuration are well supported by analysis and technical data.
h. Security engineering processes are integrated into the design to achieve an integrated secure solution.

Conference Agenda and Conference Minutes shall be available in the LVC-IA Web Portal.

(DI-MISC-80711A) Scientific and Technical Reports: Critical Design Review Report
Ref: CDRL A003
(DI-IPSC-81432A) System/Subsystem Design Description
Ref: CDRL A004
(DI-CMAN-81248A) Interface Control Document (ICD)
Ref: CDRL A00G
(DI-IPSC-81431A) System/Subsystem Specification (SSS)
Ref: CDRL A002
(DI-IPSC-81433A) Software Requirements Specification (SRS)
Ref: CDRL A00B

3.2.1.4 ASSEMBLY, INTEGRATION AND TEST STAGE

The Contractor shall resolve product deficiencies when specifications for the system, product, subsystem, assembly, or component are not met, as determined by inspection, analysis, demonstration, or test. The Contractor shall verify that the products designed satisfy specifications. The Contractor shall integrate security engineering processes into the design to achieve an integrated secure solution. Functional configuration audit (FCA) shall be completed

to verify that products have achieved requirements as demonstrated during GAT; that they satisfy the characteristics as specified in specifications, interface specifications, and other baseline documentation; and that test plans and procedures were complied with. The results of the audit shall be documented.

3.2.1.5 OPEN SYSTEMS DESIGN APPROACH AND GOALS

The Contractor shall define, document, and follow an open systems approach for using modular design, standards-based interfaces, and widely-supported consensus-based standards. The Contractor shall develop (as part of the SEMP), maintain, and use an Open System Management Plan (OSMP), to support this approach and shall demonstrate compliance with that plan during all design reviews. As part of an OSMP, the Contractor shall identify in a listing contained in its proposal to the Government all Commercial-Off-the-Shelf/Non-development Item (COTS/NDI) components, their functionality and proposed use in the system, and provide copies of license agreements related to the use of these components for Government approval prior to use. In satisfying the Government's requirements, the following system architecture approach characteristics shall be utilized:

a. Open Architecture – The Contractor shall develop and maintain an architecture that incorporates appropriate considerations for reconfigurability, portability, maintainability, technology insertion, vendor independence, reusability, scalability, interoperability, upgradeability, and long-term supportability.

b. Modular, Open Design – The Contractor shall develop an architecture that is layered and modular and uses standards-based COTS/NDI hardware, operating systems, and middleware that all utilize either non-proprietary or non-vendor-unique key module or component interfaces. The Contractor's design approach shall be applied to all subsystems and components.

c. Inter-component Dependencies – The Contractor's design approach shall result in a layered system design, maximizing software independence from the hardware, thereby facilitating technology refresh. The design shall be optimized at the lowest component level to minimize inter-component dependencies. The layered design shall also isolate the application software layers from the infrastructure software (such as the operating system) to enhance portability and to facilitate technology refresh.

d. Treatment of Proprietary or Vendor-Unique Elements – The Contractor shall explain the use of proprietary, vendor-unique or closed components or interfaces. When interfaces, hardware, firmware, or modules that are proprietary or vendor-unique are required, the Contractor shall demonstrate to the Government that those proprietary elements do not preclude or hinder other component or module developers from interfacing with or otherwise developing, replacing, or upgrading open parts of the system.

e. Reuse of Pre-existing or Common Items – The Contractor shall reuse pre-existing or common items unless a determination is made to not reuse. Exceptions to reuse of pre-existing items must be accompanied by justification, such as cost (both of adoption and life cycle support), schedule, functional and non-functional performance, etc. The general objective of these efforts shall be the development of a common system and/or common elements or components which meet the performance requirements of the various DOD or Service platform missions, where commonality offers the greatest technical and cost benefits.

f. Third-Party Development – The Contractor shall address how it will provide to the Government information needed to support third-party development and delivery of competitive alternatives of designs for software or other components or modules on an ongoing basis. The Contractor shall provide a list of those proprietary, vendor-unique elements that it requests be exempt from this review.

g. Life Cycle Management and Open Systems – The Contractor's architecture shall provide for insertion of COTS into the system and demonstrate that COTS, reusable NDI, and other components are logistically supported throughout the life cycle.

h. The Contractor's architectural approach shall support LVC-IA migration to a Data Center/Cloud (DC/C) environment so that training sites can utilize the LVC-IA from a centrally managed location and minimize hardware footprint. The Contractor's architectural approach shall be based on an evolutionary path which starts with LVC-IA supporting a cloud enabled implementation model and culminates with LVC-IA supporting a cloud optimized model. The Contractor will not be responsible for developing the DC/C infrastructure which will ultimately host the LVC-IA, but shall be responsible for developing LVC-IA DC/C architecture that conforms with the latest COE DC CE Architecture Compliance Checklist, (V2.0.2, dated 1 June 14). The Army will ultimately provide the DC/C infrastructure for LVC-IA, but until then the Contractor will be responsible for identifying a DC/C infrastructure to demonstrate and test the LVC-IA cloud enabled and optimized capabilities until the Army's DC/C infrastructure is fully operational.

(DI-SESS-81785) Systems Engineering Management Plan
Ref:A00C

3.2.2 HARDWARE ENGINEERING

The Contractor shall integrate and assemble the system hardware that satisfies the performance and cybersecurity requirements stated in the developed specifications. The Contractor shall conduct market surveillance and market investigations in order to maximize the use of

commercial and non-developmental items. The Contractor shall apply the systems engineering process during each level of system development (system, subsystem, and component). Through each of the following design stages, information generated shall be documented in an integrated database. The proposed solution shall be documented and provided to the Government for acquisition through the Computer Hardware Enterprise Software and Solutions (CHESS) program. Additionally, the Contractor shall comply with DOD Unified Capabilities Approved Products List (APL) for cybersecurity requirements.

The contractor shall demonstrate that mechanisms are in place to effectively monitor the supply chain for critical components, understands how supply chain risk can be introduced through those components, and has implemented or plans to implement countermeasures to mitigate such risks.

3.2.3 SOFTWARE ENGINEERING

The Contractor shall define a software development approach appropriate for the computer software effort to be performed under this solicitation; this approach shall be documented in a Software Development Plan (SDP). The Contractor shall follow this SDP for all computer software to be developed or maintained under this effort. The SDP shall define the Contractor's proposed life cycle model and the processes used as a part of that model. The level of detail shall be sufficient to define all software development processes, activities, and tasks to be conducted. Information provided must include, at a minimum, specific standards, methods, tools, actions, strategies, and responsibilities associated with development and qualification.The Contractor shall provide sufficient evidence that the producing software development organizations have software management and development processes documented. The design process shall incorporate features that promote assessment of open source software products, ease of operation, cybersecurity, ease of software maintenance, ease of future updates and modifications, data void work around, and also any smart designs that can justify a reduction in the amount of documentation. Computer programs and computer data system shall be fully integrated in accordance with the system specification. The Contractor shall conduct market surveillance and market investigations, in order to maximize the use of open source software, commercial software and non-developmental software. The Contractor shall maintain a software Controlled Development Environment that complies with the NIST SP 800-53 Revision 3. The Contractor shall employ well-defined security policy models, structured, disciplined, and rigorous hardware and software development techniques, and sound system/security engineering principles. The contractor shall develop a set of secure coding standards and secure design features drawing upon the "top 10 secure coding practices" (SEI CERT Coding Standards, 2011, `https://www.securecoding.cert.org/confluence/display/seccode/Top+10+Secure+Coding+Practices`).

(DI-IPSC-81427A) Software Development Plan
Ref: CDRL A00M

3.2.3.1 SOFTWARE REQUIREMENTS AND ARCHITECTURE DEVELOPMENT AND REVIEW

The Contractor shall develop software requirements and architecture in accordance with the industry software development process plan best practices and standards. All analysis and results shall be documented in an integrated database. The Contractor shall define and record the operational concept for the system, and define and record the architectural design of the system (identifying the components of the system, their interfaces, and a concept of execution among them) and the traceability between the system components and system requirements. Based upon analysis of system requirements, system design, and other considerations, the Contractor shall define and record the software requirements to be met by each software item, the methods to be used to ensure that each requirement has been met, and the traceability between the software item requirements and system requirements. The Contractor shall evaluate the cybersecurity requirements to assess any impacts on developed software and provide potential solutions, if applicable. The Contractor shall use modeling and simulation as appropriate for architecture validation. In addition, the Contractor shall determine if existing open source software products are capable of meeting any operational capabilities, perform a detailed software reuse evaluation, and document the results of the analysis. The Contractor shall conduct architecture evaluations, including stakeholders external to the Contractor's organization, for each software build.

(DI-SESS-81771) Reuse Management Report
Ref: CDRL A005
(DI-IPSC-81431A) System/Subsystem Specification (SSS)
Ref: CDRL A002

3.2.3.2 SOFTWARE DESIGN AND IMPLEMENTATION

The Contractor shall design software, develop executable code, perform unit testing, and integrate software components (with each other and with hardware components) to meet system requirements. Software design includes not only design to requirements, but selection of existing software products including open source software to meet system requirements, and iterating the requirements to allow use of existing products when indicated by cost as an independent variable or schedule as an independent variable trades. Products that perform cybersecurity functions are considered cybersecurity or cybersecurity-enabled IT products and shall be selected from the DOD Unified Capabilities Approved Product List and configured in accordance with DOD -approved security configuration guidelines. These include databases which must comply with the DISA database Security Technical Implementation Guide (STIG).

(DI-CMAN-81248A) Interface Control Document (ICD)
Ref: CDRL A00G
(DI-MCCR-80700) Computer Software Product End Items (CSPEI)

Ref: CDRL A009
(DI-IPSC-81441A) Software Product Specification (SPS)
Ref: CDRL A006
(DI-IPSC-81442A) Software Version Description (SVD)
Ref: CDRL A00E

3.2.3.3 SOFTWARE DEVELOPMENT TEST

The Contractor shall establish and execute a software item qualification test program consisting of program or module and cycle or system levels of testing. For each software item, the Contractor shall determine if that item warrants a verification effort and the degree of organizational independence of that effort needed. If the item warrants an independent verification effort, a qualified organization responsible for conducting the verification shall be selected. The Contractor shall document the life cycle activities for each software item subject to verification, the required verification tasks for each life cycle activity, and related resources, responsibilities, and schedule. The Contractor shall establish test cases (in terms of inputs, expected results, and evaluation criteria) and establish traceability between the test case and the system requirements, detailed procedures for conducting the test, and test data for testing the software corresponding to each software item. The Contractor shall test the software corresponding to each software item. The testing shall be in accordance with the unit test cases and procedures. The Contractor shall analyze the results of item testing and shall record the test and analysis results. Prior to the start of final test, the Contractor shall upgrade the COTS products to the latest versions approved by the system software configuration control board. The Contractor shall conduct a software item test readiness review prior to initiating the formal qualification test.

(DI-IPSC-81440A) Software Test Report
Ref: CDRL A007
(DI-NDTI-80566A) Test Plan
Ref: CDRL A00D
(DI-NDTI-80603A) Test Procedure: Software Development Test
Ref: CDRL A00F
(DI-NDTI-80809B) Test/Inspection Report: Software Development Test
Ref: CDRL A00H

3.2.3.4 TECHNOLOGY REFRESH

The Contractor shall provide a detailed description of how their proposed system will allow for rapid and affordable technology insertion and refresh. The Contractor shall describe how the proposed system will allow incremental systems improvement through upgrades of individual hardware or software modules with newer modular components. At a minimum, the description shall address how the Contractor's architectural approach will support this requirement including how components from third-party providers and other potential reuse sources shall be included.

3.2.3.5 TECHNOLOGY DEVELOPMENT AND INSERTION

The Contractor shall identify, develop and integrate new technologies, as well as, support, mature and integrate research initiatives currently in development through collaborative initiatives between PEO STRI - PM ITE and other organizations that will benefit the PM ITE portfolio utilizing the PM ITE collaborative technology lab. These research initiatives include, but not limited to, Enterprise After Action Review (EAAR); Enterprise Scenario Generation Tool Suite (ESGTS); Live-Synthetic Training, Test and Evaluation Enterprise Architecture (LS TTE EA) and ITE Cloud Computing. The goal is to provide a base set of proven capabilities and solutions that can help reduce cost, schedule and performance risk on development programs, to include LVC-IA and ITE core systems.

The PM ITE collaborative technology lab is a PM ITE resource utilized to perform analysis/research tasks associated with potential technology solutions to be transitioned to Programs of Record. LVC-IA is a key component of the technology lab and is utilized to provide an underlying architecture supporting Integrated Training Environment (ITE) interoperability and component enhancement efforts. The Contractor shall provide "site support" to the efforts of the technology lab (e.g. Software, cybersecurity updates and patches to the LVC-IA baseline, installation, and training).

The Contractor shall maximize the open architecture design to support system upgrades, concurrency/technology insertions, ease of software/configuration changes, and the ability to modify interfaces that support future changes.

DI-MISC-80711A, Scientific and Technical Reports
Ref: CDRL A003

3.2.3.6 MODIFICATION/SYSTEM UPGRADES

The Contactor shall perform replacement or modification of components for reasons other than obsolescence including Pre-Planned Product Improvement (P3I), modification, conversion, reconfiguration, retrofit, and technology insertion to increase the performance capability of the system.

3.2.4 HARDWARE AND SOFTWARE INTEGRATION

The Contractor shall perform all activities to integrate and assemble the hardware and software to achieve a fully functional and accreditable system, with all support systems, that performs and operates in accordance with the system specification and Contractor generated specifications. The Contractor shall verify the complete integration of the hardware and software of each hardware and software subsystem and the overall system through the utilization of formalized test procedures. A system level production approval review shall be completed to demonstrate that the total system has been verified to satisfy specification and baseline requirements for each

system level, and to confirm readiness for production, distribution, operations, support, training, continuing improvement, and disposal. The review shall ensure that:

a. Issues for the component, assemblies, subsystem, products and life cycle process and services are resolved.
b. Test procedures for components, assemblies, and products were completed and were accurate.
c. The system and products were confirmed ready for functional and cybersecurity testing and accreditation.
d. Tests were conducted in accordance with established procedures.
e. An audit trail from design reviews, held after detailed design, is established with changes substantiated, and all component, subsystem, and system products meet specification requirements.
f. Risk-handling procedures are satisfactory for production.
g. Evolutionary development requirements and plans have been refined.
h. Planning is complete and procedures, resources, and other requisite people, products, and processes are available (or programmed to be available) to initiate production, distribution, operations, support, training, disposal, and evolutionary development (if any).

3.2.5 CYBERSECURITY

The Contractor shall develop and maintain an information assurance and cybersecurity process to guide management and design actions, document decisions, specify and track cybersecurity requirements, document certification efforts, identify possible solutions, and maintain operational systems security. The Contractor shall establish or adopt standards for managing information assurance and cybersecurity requirements and capabilities and an information system (IS) security engineering approach that emphasizes purposeful design or configuration of security solutions. All cybersecurity and cybersecurity-enabled products shall be securely configured IAW DOD -approved security configuration guidelines. The Contractor shall obtain STIGs and review each STIG for potential inclusion into the system configuration and document their assessment, with the Government reviewing any non-compliant STIG items to determine course of action. As part of the system design and component selection process, cybersecurity shall be considered as a requirement for all systems used to enter, process, store, display, or transmit information. Cybersecurity shall be achieved through the acquisition and appropriate implementation of evaluated or validated GOTS or COTS IA and cybersecurity-enabled Information Technology products. All COTS cybersecurity products and cybersecurity-enabled products shall be certified compliant with National Security Telecommunications and Information Systems Security Policy Number 11 (NSTISSP-11) by labs accredited under the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme or National Institute of Standards and Technology (NIST) Federal Information Processing Standards Cryptographic Module Validation Program. Similarly, GOTS

cybersecurityproducts or cybersecurity-enabled products employed by the system shall be evaluated by the National Security Agency (NSA) or in accordance with NSA approved processes. The Contractor shall perform manual scans and provide the scans to the Government at least monthly to ensure the system is Federal Information Security Management Act (FISMA) compliant.

(DI-MISC-80711A) Scientific and Technical Reports: Cybersecurity **Report**
Ref: CDRL A003

3.2.5.1 CYBERSCURITY ARTIFACTS

The Contractor shall support the Government in the RMF A&A effort. The Contractor shall support Government cybersecurity, Assess & Auhtorize, and Connectivity or Interconnectivity activities as required, including providing A&A documentation, upon request, in a format acceptable to DOD cybersecurity and A&A activities. The Contractor shall comply with the cybersecurity process in accordance with the most current standard for the effort being performed per DODI 8500.01 & DODI 8510.01 (RMF). The Contractor shall document the following A&A artifacts:

a. RMF Controls Self-Assessment
b. Information Security Plan
c. System Identification Profile
d. Configuration Management Plan
e. Memorandum of Understanding or Agreement
f. Tenant Security Plan
g. Continuity of Operation Plan
h. Artifacts associated with the implementation of cybersecurity controls

The Contractor shall produce all components of the A&A package necessary to certify and accredit the LVC-IA system. The Contractor shall ensure that the security requirements and procedures are met in accordance with all required DOD and Army regulation per the CIA of High-Low-Low levels, agreed upon for the system.

(DI-MISC-80508B) Technical Report – Study/Services (RMF Package)
Ref: CDRL A00A

3.2.5.2 INFORMATION ASSURANCE VULNERABILITY MANAGEMENT

As part of the Information Assurance Vulnerability Management (IAVM), the Contractor shall document the incorporated and unincorporated Information Assurance Vulnerability Alerts, Information Assurance Vulnerability Bulletins, and Information Assurance Vulnerability Technical Advisories, as required. The IAVM plan shall include but is not limited to identifying

and assessing potential threats to determine risks. It also involves developing and implementing controls, countermeasures, or solutions. The Contractor shall monitor the system for compliance and success, while evaluating and refining the IAVM plan as necessary. The Contractor shall incorporate all applicable DOD and Department of the Army Information Assurance Vulnerability Management messages issued on behalf of the Department of Army G3, CIO/G6 and Joint Task Force-Global Network Operations.

The Contractor shall report all Information Assurance Vulnerability Alerts (IAVAs), STIGs and Bulletins within a system Plan of Action and Milestone (POA&M) at least monthly, or more frequent if directed by the local Authorizing Official (AO), and provide a list outlining which were implemented, those not implemented and why they were not and how mitigated if mitigation required. The Contractor shall provide justification (i.e., describe the specific negative impact the IAVA and STIG incorporation would have on the system operation) for all non-implemented IAVAs and STIGs, and they shall have Government concurrence. The Contractor shall provide a comprehensive and up to date software scan using current Army Best Business Practices for scanning and remediation every month. The Contractor shall comply with the following:

a. IAVAs

- The Contractor shall apply Exploit category A IAVAs within 14 days of notification.
- The Contractor shall apply Exploit category B IAVAs within 14 days, when possible, or within 30 days if a system level POA&M to mitigate is provided.
- The Contractor shall monitor all update requirements including but not limited to (vendor sites, mailing lists, third party sources, vulnerability scans and US Army Network Enterprise Technology Command (NETCOM) SharePoint site for Information Assurance Vulnerability Messages.) The Contractor shall make mitigation, patching, upgrade or modification recommendations and provide a POA&M for all requirements that cannot be fulfilled on time, in a format approved by the PEO for each update requirement. The Contractor shall treat the POA&M as specified in the system's security classification guide (SCG) and provide a digital copy to the Government via a method approved by the Government. The Contractor shall provide a comprehensive and up to date software scan using current Army Best Business Practices for scanning and remediation every month.
- For the Standalone accredited Development Environment, the Contractor shall incorporate all applicable IAVA by their documented suspense date. The Contractor shall provide justification for each unincorporated IAVM message (i.e., describe the specific negative impact the IAVA message incorporation would have on the system operation).

b. STIGs

- Contractor shall implement STIGs within 30 days from release of a new DISA STIG. Where an update cannot be technically applied due to system functionality, that STIG item shall be documented in the system POAM with appropriate mitigations. If an update

cannot be applied within 30 days the Contractor shall provide a milestone schedule in the POAM item for application for Government approval.

c. Design Considerations

- The Contractor shall develop a cyber resilient system by ensuring IAVAs and STIGs can be applied individually without the need to re-image the system, and not only update IAVAs or STIGs during new capability updates.

3.2.5.3 RMF ASSESS ONLY PROCESS

Contractor shall ensure compliance with the policies and procedures for obtaining an Assess-Only certification in accordance with the DOD 8510.01 for any software application products that may be required to be fielded separately from the LVC-IA system (if any), that will be used directly or indirectly within Army Networks. The Contractor shall provide all applicable information to the LVC-IA program office for review.

3.2.5.4 HOST-BASED SECURITY SYSTEM (HBSS)

The Contractor shall ensure HBSS compatibility and compliance are established for any system that touches the Army Network directly or indirectly or has the capability to connect, providing network administrators and security personnel with mechanisms to prevent, detect, track, report, and remediate malicious computer-related activities and incidents across all DOD networks and information systems in accordance with the Joint Task Force for Global Network Operations released Communications Tasking Order (CTO) 07-12 (Deployment of HBSS) mandating the deployment of HBSS on all Component Command, Service and Agency networks within DOD.

3.2.6 SPECIALTY ENGINEERING

3.2.6.1 RELIABILITY, AVAILABILITY, AND MAINTAINABILITY (RAM)

The Contractor shall conduct RAM analysis necessary to meet the LVC-IA CPD availability requirements, as well as cybersecurity availability requirements. The Contractor shall conduct analysis to identify assumptions, constraints, and definitions needed to determine the best approach for achieving satisfactory RAM in support of LVC-IA, as a functioning end-item, can be operated and maintained within the scope of the logistics support concept while attaining operational availability (Ao) requirements. The Contractor analysis shall also consider mission and logistics reliability requirements and the maintainability and integrated diagnostics requirements that address all aspects of system performance; ensuring system-level design and layout considerations are addressed to minimize unnecessary/untimely removal of LVC-IA components to perform proper maintenance.

3.2.6.2 SAFETY ENGINEERING

The Contractor shall develop and implement tasks and activities to identify, evaluate, and eliminate or control hazards throughout the systems life cycle. The Contractor shall ensure the safety of the system's design, operation, transportation, maintenance, support, and disposal. The Contractor shall conduct safety analyses, hazard identification and classification and hazards tracking integral to the system design effort. A hazard risk index including hazard severity and hazard probability levels shall be developed for all hazards.

3.2.6.3 SAFETY ASSESSMENT

The Contractor shall conduct safety analyses and identify and classification hazards as an integral part of the system design effort. The Contractor shall develop a hazard risk index including hazard severity and hazard probability levels for all hazards. The Contractor shall document information about each hazard. The Contractor shall ensure that safety of the design is achieved and that all system specific safety requirements are met. This shall include verifying any changes due to redesign. Once complete, the Contractor shall verify the safe design of the system and to determine the safety risk assumed prior to test or operation. The Contractor shall identify those software items or portions thereof whose failure could lead to violation of critical requirements and develop a strategy, including both test and analysis, to assure that the requirements, design, implementation, and operating procedures for the identified software minimize or eliminate the potential for such violations. The Contractor shall identify by type, and develop strategies for, the following types of critical requirements:

a. Safety-critical: Those software items or portions thereof whose failure could lead to a hazardous system state (one that could result in unintended death, injury, loss of property, or environmental harm).
b. Security-critical: Those software items or portions thereof whose failure could lead to a breach of system security.
c. Privacy protection-critical: Those software items or portions thereof whose failure could lead to a breach of system privacy protection.

(DI-SAFT-80102B) Safety Assessment Report (SAR)
Ref: CDRL A008

3.2.6.4 QUALITY ASSURANCE

The Contractor shall implement a quality assurance program to ensure the system requirements are met. Specifically, control and audit procedures that shall identify areas adversely affecting contract performance and the quality of deliverables. The Contractor shall implement a methodology for application and monitoring of corrective action which will ensure successful and timely problem resolution, process and outcome performance measurement, including

methods that identify and prevent deficiencies in the quality of services, Subcontractors, and teaming partners. The Contractor shall utilize a system to be used for recording, computing, and accessing performance measurement data. This performance data shall be provided to the Government as requested.

3.2.6.4.1 TEST DISCREPANCIES

The Contractor shall document all test discrepancies for Contractor conducted tests and track the failure analysis and corrective action for each test discrepancies until correction and regression test are successfully completed. The Contractor shall establish a suspense system to ensure timeliness of analysis and corrective action of each test discrepancy. The Contractor shall establish a process to receive test discrepancies from any IPT member and accomplish data entry. Upon correction of the test discrepancies, the Contractor shall test the system to ensure that the correction of the test discrepancies did not interfere with or alter the functionality of the system. Upon closeout of a discrepancy, the Contractor's process shall notify the government designated test director that an integrated database has been updated.

3.2.6.4.2 DISCREPANCY PROCESSING

The Contractor shall document a detailed description defining the changes made to the equipment, hardware, and software to correct each discrepancy. Each discrepancy correction that modifies or changes any baseline shall be documented and entered in the configuration management system. Discrepancies ready for recheck shall normally accumulate into sufficient quantities to permit at least eight hours of continuous testing.

3.2.6.4.3 TEST DISCREPANCY PRIORITY

The Contractor shall assign level of effort to test discrepancies based on the priority codes assigned by the test team, in accordance with the ground rules established by the IPT. The government reserves the right to make the final determination of the priority of any test discrepancy.

3.2.7 DESIGN REVIEWS

The Contractor shall conduct reviews, to include design reviews (system, subsystem, component, life cycle processes, test readiness, production approval and FCA, for the purpose of assessing technical progress. The Contractor shall address cost, schedule, and performance risks as appropriate during design reviews. The Contractor shall document the results of the review, including any resulting action items. Each review shall accomplish the following:

a. Assess the system requirements and allocations to ensure that requirements are unambiguous, consistent, complete, feasible, verifiable, and traceable to top-level system requirements.

b. Assess the design maturity based on technical development goals, IMS events and accomplishments, and empirical analysis and test data supporting progress to date.
c. Address the system security design.
d. Present the risks associated with a continued development effort.
e. Assess the life cycle processes and infrastructure necessary for product sustainment throughout the system life cycle.
f. Identify resources required for continued development;
g. Determine whether to proceed with the next application of the systems engineering process, to discontinue development, or to take corrective actions before proceeding with the development effort.

The Contractor shall conduct component, subsystem, and system design reviews for each level of development. Trade-off analysis and verification results should be available during design reviews in order to substantiate design decisions. Reviews may result in the need to iterate through the system engineering process to resolve identified deficiencies before progressing further into the development activity. The Contractor shall perform component, subsystem, and system functional- and design-configuration audits to ensure that supporting documentation are complete, and all requirements and products comply with specifications.

(DI-MISC-80711A) Scientific and Technical Reports: Design Review Report
Ref: CDRL A003

3.2.7.1 SYSTEMS REQUIREMENTS REVIEW (SRR)

The Contractor shall be responsible for planning, coordinating, and executing all activities associated with the SRR. All system and performance requirements derived from the CPD are defined/testable and consistent with cost, schedule, risk, technology readiness, and other system constraints. This review assesses the system performance requirements as captured in the system performance specification, and ensures that the system performance requirements are consistent with the system solution and available technologies.

3.2.7.2 ENGINEERING DESIGN REVIEW (EDR)

The Contractor shall be responsible for planning, coordinating, and executing all activities associated with the preliminary design. The Contractor shall provide the preliminary design by executing a series of Engineering Design Reviews (EDRs) structured in conjunction with the technical strategy. The EDRs will assess the system preliminary design as captured in performance specifications for each configuration item in the system (allocated baseline), and ensure that each function in the functional baseline has been allocated to one or more system configuration items. The EDRs ensure that the preliminary design is complete; the system can proceed into detailed design, and can meet the stated performance requirements within cost (program budget), schedule (program schedule), risk, and other system constraints. The EDRs

will substantiate to the Government that the hardware and software preliminary designs are complete, and the IPT is prepared to start detailed design and test procedure development.

3.2.7.3 CRITICAL DESIGN REVIEW (CDR)

The Contractor shall be responsible for planning, coordinating, and executing all activities associated with the CDR. The Critical Design Review (CDR) ensures that the system can proceed into system fabrication, demonstration, and test, and can meet the stated performance requirements within cost (program budget), schedule (program schedule), risk, and other system constraints. This review will assesses the system final design as captured in product specifications for each configuration item in the system (product baseline), and ensures that each product in the product baseline has been captured in the detailed design documentation. Product specifications for hardware must enable the fabrication of configuration items, and shall include product definition data. Product specifications for software (e.g. Software Design Documents) must enable coding of a Computer Software Configuration Item. Configuration items may consist of hardware and software elements.

The subsystem detailed designs shall be evaluated to determine whether they correctly and completely implement all system requirements allocated to the subsystem, and whether the traceability of final subsystem requirements to final system detail design is maintained. At this review the IPT shall also review the results of peer reviews on requirements and final detail design documentation, and ensure that latest estimates of cost (development, production, and support) are consistent with the detail design. A successful review is predicated on the IPT's determination that the subsystem requirements, subsystem detail design, results of peer reviews, and plans for testing form a satisfactory basis for proceeding into system fabrication, demonstration and test.

3.2.7.4 PRODUCT DEFINITION DATA (PDD)

The Contractor shall develop, produce, and maintain LVC-IA PDD that accurately depicts the final product and includes all the information necessary for maintaining and sustaining the system by a life cycle support Contractor. The PDD shall disclose complete design, logistics, training products, and manufacturing requirements, and the means of measuring compliance with LVC requirements. Piece part information (e.g. drawings, computer aided design files and Meta data, etc.) and associated lists shall provide the necessary engineering, manufacturing, and quality assurance requirement information necessary to maintain and sustain the system, without additional design engineering effort or recourse to the original design activity. The data shall be made available to the Government and shall be maintained by the Contractor to ensure that the information remains updated based on design changes for the life of the contract. For each high level component or assembly, the Contractor shall determine and document the functional requirements for the item, the environment in which it must operate, interface and interchangeability characteristics, and criteria for verifying compliance.

(DI-SESS-80776A) Technical Data Package
Ref: CDRL A00J
(DI-SESS-81000E) Product Drawings/Models and Associated Lists
Ref: CDRL A00K

3.3 LOGISTICS

The Contractor shall conduct engineering analyses to establish quantitative and qualitative supportability design guidelines. The Contractor shall conduct trade studies, evaluate design and support alternatives, and establish system supportability preliminary design configurations consistent with system readiness and availability and life cycle cost goals. The Contractor shall verify that the maintenance actions and support structure are aligned with the maintenance concept in accordance with government developed fielding plans.

3.3.1 LOGISTICS SUPPORT ANALYSIS

The Contractor shall identify support resources and infrastructure necessary for test and evaluation activities. The Contractor shall analyze, develop and define an optimized support infrastructure for production and deployment. The recommended support resources shall be sufficient to allow another Contractor with comparable skills to assume operation, maintenance, and support of the system and sustain the system availability requirement. The Contractor shall only use the form, fit, function, and interface requirements in the performance specifications for provisioning, training and maintenance planning.

3.3.2 SUPPORTABILITY ANALYSIS AND LOGISTICS MANAGEMENT INFORMATION

The Contractor shall conduct repair level analyses, develop diagnostic, preventative maintenance and repair procedures, conduct facilities analyses, refine hardware and software maintenance and support concepts, and identify support resource requirements including required spares and support equipment. Using Source Maintenance & Recoverability Codes, the Contractor shall develop a listing of which items should be repaired and which should be discarded and the level of maintenance at which the repair should be performed with the associated cost. The Contractor shall document the following in an inventory database:

a. All input data and their corresponding value and source of the data.
b. Operational scenario modeled, assumptions made, constraints assumed, and non-economic factors imposed.
c. Maintenance alternatives considered.
d. Analytical method and models used to perform the economic evaluations.
e. Discussion of the sensitivity evaluation performed and results obtained.

(DI-SESS-81758A) Logistics Product Data
Ref: CDRL C008
Refer to Annex to Exhibit A (Tailored Logistics Product Data Attribute Selection Sheet & Guidance.)
(DI-SESS-81759A) Logistics Product Data Summaries
Ref: CDRL C007
Refer to Annex to Exhibit A (Tailored Logistics Product Data Attribute Selection Sheet & Guidance.)

3.3.3 TECHNICAL PUBLICATIONS

The LVC-IA technical publications shall describe each operation and maintenance task in detail and in logical, systematic steps for the work to be accomplished. The Contractor shall develop and deliver a complete and exportable combined Operations and Maintenance Manual (O&M Manual) prior to the Test Readiness Review. The operations and maintenance instructions provided by the manual shall accurately provide the LVC-IA Operator/Maintainers with all of the information necessary to keep the equipment operational. It shall provide system and subsystem oriented instructions for installation, operation, maintenance and testing. All tools, test equipment and consumable items required to accomplish any maintenance or installation shall be identified as part of the O&M Manual. All Government Technical manuals and COTS manuals shall be reviewed to ensure changes, updates, and revisions reflect the components actually being installed. All publications shall reflect the configuration of fielded hardware as documented in the product baseline.

(MIL-STD-40051-2B) Preparation of Digital Technical Information for Page-Based Technical Manuals (TMs)
Ref: CDRL C006
Refer to Annex to Exhibit C (Operator and Field Maintenance Manual Requirements Matrix, table A-II)
(DI-TMSS-80527C) Commercial Off-The-Shelf (COTS) Manual and Associated Supplemental Data
Ref: CDRL C003

3.3.4 ITEM UNIQUE IDENTIFICATION (IUID)

The Contractor shall coordinate among the IPT members to determine items requiring unique identification including embedded subassemblies, components and parts, and identify the unique identification (UID) to be used for each item. The Contractor shall provide unique item identification, or a DOD recognized unique identification equivalent, for all identified items delivered. UID marking design for each item shall be both machine readable and human readable in accordance with MIL-STD-130, paragraph 5.2.

(DI-MGMT-81804A) Item Unique Identification (IUID) Marking Activity, Validation and Verification
Ref: CDRL C004

3.3.5 TRAINING PRODUCTS

The Contractor shall design, develop and deliver a complete and exportable training support package that includes New Equipment, Instructor/Operator and Maintenance Training in accordance with SOW paragraphs below. The training support package shall integrate training products, materials, and other pertinent information necessary to train in an LVC environment. The Contractor shall design and develop the training support package using instructional systems design processes and deliver prior to the conduct of the Test Readiness Review.

(DI-ILSS-80872) Training Materials
Ref: CDRL C005

3.3.5.1 NEW EQUIPMENT TRAINING (NET)

The Contractor shall provide system operation and maintenance familiarization training through a combination of classroom, written instructions, and hands-on operation. The Contractor shall analyze, and prepare all training courseware including program of instruction, lesson plans, practical exercises, and a train-the-trainer package to accommodate new equipment training, sustainment training, and training of testers and evaluators. The Contractor shall conduct training for key test personnel prior to the Test Readiness Review (TRR) and in addition at each site as part of the installation for LVC-IA Operator/Maintainer personnel. The Contractor shall provide all related training and course materials to include O&M manuals, to each location at the beginning of each course.

3.3.5.2 INSTRUCTOR/OPERATOR TRAINING

The Contractor shall provide Instructor/Operator training that provides comprehensive training for instructors in the concepts, skills, and aptitude to efficiently coordinate and facilitate an LVC exercise. The course shall provide familiarization with operating techniques, functions, and controls to the extent necessary to facilitate their utilization in an LVC exercise. The course shall address the physical and functional descriptions and operation of the equipment including features, advantages, and configurations. The Contractor shall conduct training for key test personnel prior to the Test Readiness Review and in addition at each site installation for LVC-IA Operator/Maintainer personnel. The Contractor shall provide all related training and course materials to include O&M manuals to each location at the beginning of each course.

3.3.5.3 MAINTENANCE TRAINING

The Contractor shall provide Maintenance Training that provides comprehensive training for maintainers in the concepts, skills, and aptitude to efficiently maintain the LVC-IA system and all linkages. This course shall consist of instruction in troubleshooting and maintenance, diagnostics to fault isolation, calibration, adjustments, remove and replace procedures and the use of built in tests. At completion, personnel shall be capable of operating, maintaining and troubleshooting the LVC-IA system and associated networks to ensure network connectivity and successful operation of the LVC-IA system. The Contractor shall conduct training for maintenance personnel in support of each site installation. The Contractor shall provide all related training and course materials to include O&M manuals to each location at the beginning of each course.

3.3.6 INTERIM CONTRACTOR SUPPORT

The Contractor shall provide interim contract support (ICS) services at each fielding location. The Contractor shall maintain a high level of security awareness commensurable with the MAC and CL. All employees with access to a Contractor maintained or operated information system must complete cybersecurity training prior to be given access to the operational system. The Contractor shall implement the Army approved Information Assurance Vulnerability Management program during the ICS period and shall assist in compliance reporting.

The Contractor shall maintain a Help Desk 24/7 support capability to further assist the ICS Contractor in operation and maintenance of the LVC-IA system. Administrators shall meet the minimum requirements defined by paragraph 3-3 and 4-3 of AR 25-2.

3.3.7 SOFTWARE SUPPORT

The Contractor shall provide services to maintain and update system software for the duration of the interim contract support (ICS) effort. At the end of the ICS effort, the Contractor shall deliver, install, and check-out for proper operation a subset of the development software support environment to serve as the sole means to sustainment for the system software. The software support environment shall include all commercial, government-funded, and Contractor proprietary software, all necessary documentation/specifications, plus executing hardware with all applicable licenses necessary to enable the government to fully support all system software.

3.3.8 SITE SUPPORT

The Contractor shall provide three weeks of on-site support for approximately eight exercises per year to assist the Government's designated ICS Contractor representatives in the operation of LVC-IA during scheduled training exercise events on an as needed basis. The Contractor shall provide support and management of site logistical operations. In accomplishing this mission, the Contractor shall perform the administrative, operational, maintenance, supply, technical documentation change and revision program and other support functions required.

3.3.9 CUSTOMER SUPPORT SERVICES

The Contactor shall be prepared to perform LVC-IA EC related services to meet requirements of the LVC community to allow for a more efficient Integrated Training Environment capitalizing on technical investment plans, priorities and integrated investment strategies which promote coordination, cooperation, compatibility, interoperability and awareness while reducing duplication of effort.

3.3.10 TRANSITION PLANNING

A 60 day, phased in transition period will include at least one Version 2 software release fielding involving both incumbent and new Contractor participation, which will allow the successor Contractor to observe a fielding of Version 2. The incumbent Contractor will pack and ship the PDSS equipment. The Contractor's PDSS facility shall be up and running at the conclusion of the 60-day transition period, at a minimum for unclassified operations and storage. The PDSS facility shall be able to achieve accreditation at the SECRET level for operation and storage within one year of contract award. In the event the Contractor is unable to provide an accredited facility for operation and storage of existing SECRET PDSS equipment at contract award, the Government will provide space within the JDIF for storage of the SECRET equipment during the Contractor's PDSS facility accreditation.

For phase out, the incumbent Contractor shall provide support for the transfer of ICS responsibility to the government or another Contractor. Support shall include those services required to ensure the effective, efficient transfer of responsibility as well as technical data, tools and test equipment and repair and spare parts, in sufficient detail and coverage to enable other personnel with comparable skills to maintain the system. The transition effort shall include an analysis of all failures and maintenance actions undertaken during the interim support and revising technical publications subject to Government approval to reflect actual fielded experience. The support transfer shall include 100 percent of provisioned items.

3.4 INTEGRATED TESTING

The Contractor shall plan, coordinate, establish and implement a comprehensive test and evaluation (T&E) program to support the government Test and Evaluation Master Plan (TEMP) for the LVC-IA system. The Contractor shall implement a continuous integration, test and evaluation strategy in which integration events (IEs) gradually increase in size and functional capability as the system matures. LVC-IA integration activities shall include Integration Event (IE), Functional Verification Test (FVT), and a System Measurement Performance (SMP) Event that culminate with Government Acceptance Test (GAT). Each IE shall build upon the previous IE and increase system/application operational and technical capability. IEs support not only integration testing but also a verification process. FVT shall ensure that functionality integrated at IEs is operating as designed. The primary focus of FVT is to incrementally assess progress toward meeting all system level requirements. SMP shall introduce levels of loading on the

LVC-IA in order to observe and measure the performance. The goal of the event is to uncover performance bottlenecks, and to ensure that observation and data collection will support identification and correction of those bottlenecks.

The Contractor shall develop On-Site Acceptance Test (OSAT) Procedures to be used during site acceptance testing. The Contractor shall perform a preliminary inspection and test of the equipment to ensure it is functioning properly prior to shipping to the fielding site and retest the equipment after installation at the site.

System T&E refers to the test and evaluation activities which use the production hardware together with the software to validate that the system meets the operational and technical performance requirements as stated in the system specifications. System T&E includes all efforts associated with the design and production of models, specimens, fixtures and instrumentation in support of the T&E program. System test shall include a process to prepare the executable software, including any batch files, data files, or other software files needed to install and operate the software on a newly formatted (blank media) target computer. The Contractor shall develop step-by-step testing operations to be performed on items undergoing testing. The Contractor shall identify items to be tested, the test equipment and support required, the test conditions to be imposed, the parameters to be measured, and the pass and fail criteria against which the test results will be measured. The test planning and test procedures shall be structured to insure that the LVC-IA capability meets the requirements identified in the systems specification.

(DI-NDTI-80566A) Test Plan
Ref: CDRL A00D
(DI-IPSC-81442A) Software Version Description (SVD)
Ref: CDRL A00E
(DI-NDTI-80603A) Test Procedure: IE/FVT
Ref: CDRL A00F

3.4.1 TEST READINESS REVIEW (TRR)

The Contractor shall address the following key issues at the TRR prior to the start of formal GAT to ensure that the system and all test resources are ready to begin testing:

a. Test procedures comply with plans and descriptions, are adequate to accomplish test requirements and satisfy requirements for verification.
b. Pre-test predictions and informal tests indicate testing will confirm performance.
c. New or modified test equipment and facilities and procedure manuals required to accomplish planned test and evaluation, are available and satisfy the test requirements.
d. Data acquisition and reduction provisions are in place.
e. Technical publications are completed and validated.

The following documentation shall be reviewed during the TRR:

a. Evidence that a test management system as required under the contract is ready to accept the qualification tests and their results. Test management system is documentary evidence, as part of the contract, has developed a storage/retrieval of the project's qualification tests and their results.
b. Evidence that the requirements in the specification have been traced to qualification tests or tests on which the qualification tests rely.
c. A list of outstanding problem reports, both external and internal cross-referenced to the contracted deliverable end items or development hardware and software products.
d. Test requirements.
e. Requirements changes pending.
f. Design changes since the last design review.
g. Test constraints based on previous testing or test hardware limitations.
h. Test configuration (test article and instrumentation and support equipment).
i. Detailed test procedures.
j. Plans for collection, reduction and analysis of the test data.
k. Calibration plan and status.
l. Problem areas and their resolution.

Conference Agenda and Conference Minutes shall be available in the LVC-IA Web Portal.

3.4.2 SYSTEM MEASUREMENT PERFORMANCE (SMP) EVENT

The main purpose of the SMP event is to operate LVC-IA as a system and to observe and measure the performance of the system under load. In addition, the presumption is the event will uncover performance bottlenecks. The Contractor shall document the identification and correction of any bottlenecks.

The Government and the Contractor will collaborate but as a minimum, the SMP event shall collect the following metrics: Resource usage (Memory, CPU, Disk I/O); Distributed operations remote sites network traffic; Latency of conversion through each gateway; core systems interactions under required maximum loads.

(DI-NDTI-80603A) Test Procedure: SMP
Ref: CDRL A00F
(DI-NDTI-80809B) Test/Inspection Report: SMP
Ref: CDRL A00H

3.4.3 GOVERNMENT ACCEPTANCE TEST (GAT)

The Contractor shall plan, coordinate, establish and implement a comprehensive test and evaluation (T&E) program to support the government TEMP. The Contractor shall develop step-by-step testing operations to be performed on items undergoing developmental testing. The Contractor shall identify items to be tested, the test equipment and support required, the test conditions to be imposed, the parameters to be measured, and the pass and fail criteria against which the test results will be measured. The Contractor shall verify that the products designed satisfy system requirements and specifications. The Contractor shall conduct a GAT at the Government Integration facility and potentially two (2) CONUS remote sites to address the verification of approved LVC-IA System Level Requirements. Testing shall be conducted utilizing the FEDSUN network from the JDIF facility to connect to the core systems at their Contractor facilities. During Government acceptance test, the Contractor shall verify that the installed capability functions and operates properly to the baselined SSS requirements. Testing shall be conducted using portions of the acceptance test procedures selected by the Government. The main purpose of this GAT event is to verify the LVC-IA capability operates in the intended training environment on the home station infrastructure operated by the home station support staff. Any discrepancies/problems found during testing shall be corrected and re-tested prior to Government acceptance. A Contractor-developed detailed System Test Plan and test procedures shall be provided and approved by the government prior to the TRR.

(DI-NDTI-80603A) Test Procedure: GAT
Ref: CDRL A00F
(DI-NDTI-80809B) Test/Inspection Report: GAT
Ref: CDRL A00H
(DI-IPSC-81431A) System/Subsystem Specification (SSS)
Ref: CDRL A002

3.4.4 PRODUCTION AND FIELDING READINESS REVIEW

The Contractor shall ensure initial production assets are available to support production for system testing requirements and CONUS/OCONUS fielding timelines. A Fielding Readiness Review will be conducted for the LVC-IA program in conjunction with all fieldings. The main focus of the review is to facilitate provisioning of the system. The Contractor shall provide the required information to the Government prior to each fielding of a major software version of the system.

(DI-SESS-81758A) Logistics Product Data
Ref: CDRL C008
Refer to Annex to Exhibit A (Tailored Logistics Product Data Attribute Selection Sheet & Guidance.)

3.4.4.1 EQUIPMENT RECORD

The Contractor shall provide a record of all equipment fielded by site. The record shall be maintained in the LVC-IA Web portal.

3.4.5 FIRST USE ASSESSMENT (FUA)

FUA is an operational test event to verify that the LVC-IA capability operates in the intended training environment on the home station infrastructure operated by the home station support staff.

The FUA tests the LVC-IA's capabilities as a training tool and supports the Combined Arms Commander – Training with the decision to accredit LVC-IA for use in the Training, Exercises, and Military Operations domain. The FUA consists of a training event where specific measures of performance/effectiveness are monitored.

The Contractor shall review the Combat Developer generated test procedures and test plans prior to the FUA events. The Contractor shall provide technical and Subject Matter Expert assistance, as needed during the FUA.

3.5 SITE ACTIVATION

The Contractor shall conduct survey of Army installations (11 CONUS and 4 OCONUS) with the Government prior to the commencement of LVC-IA system installation and compile the results in a Trainer Facilities Report. The purpose of the site activation activities is to discuss and confirm arrangements for LVC-IA system installation and to provide information on any modifications required at the installation site. During the survey, the Contractor shall:

a. Review the status of the building or location where the system will be installed.
b. Confirm the required positions of equipment, assemblies, cableways, access ways, and any other unique feature, and measure to insure clearance during the installation.
c. Review and confirm the existing and proposed location of power distribution boxes, switches, water and air supply points and air ducting, and other unique building or location features.
d. Determine the availability of required services.
e. Review and confirm arrangements for hours of work, access to work areas, supporting workshops facilities, and on-site personnel participation.
f. Discuss and resolve any outstanding issues pertaining to the installation program.

(DI-FACR-80966) Trainer Facilities Report
Ref: CDRL C001

3.5.1 INSTALLATION PROGRAM

Prior to the arrival of the system at each site, the Contractor shall perform all installation preparatory work; including advising and assisting on-site personnel with any modifications they may be performing.

3.5.2 INSTALLATION SPARES

The Contractor shall propose an integrated spare parts package adequate to support the system for each year and delivered with the installation teams during fielding and set-up. The Contractor shall recommend any special tools or test equipment to be included in the package and provide a price with the consolidated list (to include consumables) to the government for approval.

(DI-ILSS-80134A) Proposed Spare Parts List
Ref: CDRL C002

3.5.3 ON-SITE ACCEPTANCE TEST

The Contractor shall develop On-Site Acceptance Test (OSAT) Procedures to be used during site acceptance testing. The Contractor shall perform a preliminary inspection and test of the equipments to ensure it is functioning properly prior to shipping to the fielding site. Any discrepancies/problems found during the site acceptance test shall be corrected, re-tested and verified by the Government prior to site acceptance.

The Contractor shall provide on-site technical support during the fielding at each site. The Contractor shall delivery the documentation and any other items to operate the system IAW OSAT Procedures but not limited to inspection of hardware and software, Spare Parts List, COTS Manual and associated documentation, Training Materials, and NET.

(DI-NDTI-80603A) Test Procedure: OSAT
Ref: CDRL A00F
(DI-NDTI-80809B) Test/Inspection Report: OSAT
Ref: CDRL A00H

3.6 SYSTEM TECHNICAL SUPPORT

The Contractor shall provide staff and technical support that include training, logistics functions, hardware and software engineering functions, software licensing, support services, spare parts, travel overtime, maintenance, supply, replacement of non-fair wear and tear parts, Contractor activity and facility relocations, adding and deleting training devices, transportation of equipment, development, productions, installation of software upgrades, re-host and modifications kits as authorized by individual contract work directives. The Contractor shall

document the description of each task, the man-hours spent, cost of materials and services and the results of each service(s).

(DI-MGMT-80227) Contractor's Progress Status and Management Report
Ref: CDRL B001

3.6.1 POST DEPLOYMENT SOFTWARE SUPPORT

The Contractor shall define and provide a PDSS capability and facility to support sustainment of LVC-IA system software and its associated subsystems and components, based on the Government Furnished Property (GFP). This includes Help Desk support, system and software engineering support, and Maintainer/Operator upgrade training and technical refresh. The PDSS facility shall be able to achieve accreditation at the SECRET level for operation and storage within one year of contract award.

3.6.1.1 HELP DESK SUPPORT

The Contractor shall provide users access to a help desk to solve user problems. The Contractor shall maintain a Help Desk 24/7 support capability. The help desk shall be operationally manned during the scheduled operation hours of the team. The Government will provide 14 days notice for Help Desk support required for ad-hoc exercise support in which case the Contractor shall provide after working hours and weekend support. The Contractor shall maintain records of reported incidents, derive metrics from the data, and compile a monthly report stored on the LVC-IA portal. The metrics shall include as a minimum:

- Author: Person who initiates the ticket.
- Status: In Progress, Open, Close.
- Priority: Urgent, High, Medium, Low.
- Assignee: Person who is responsible for the ticket.
- Category: Category of the issue described in the ticket, i.e. Gateways, Cross Domain Solution (CDS), etc.
- Target Version: Software Version #.
- Reporting Site: Site where the problem is reported, i.e. Ft. Campbell.
- Response Time: See table below.
- Duration: How long a ticket has been open.
- Actual Time Spent: Time actually spent (Phone support only).

The Contractor shall recommend to Government a priority to each help desk ticket when it is opened based on the severity of the problem. The Contractor PDSS lead will monitor and follow up on the progress of all help desk tickets and keep Government key personnel informed on progress. All urgent and high codes must be communicated directly to the appropriate area for

immediate resolution. The Contractor shall meet the response times for the priority levels as defined below:

Priority	Definition	Response Time
Urgent	LVC-IA Site is experiencing an outage and cannot access primary application. Problem has no work-around solution available.	Site shall be contacted < 1 hour
High	Site cannot access a non-critical business. Problem has short-term work-around solution available.	Site shall be contacted < 24 hours
Medium	Site cannot access a non-critical application, or a user has an inquiry: question on how things work, service, request, etc. Problem has long-term work-around solution available.	Site shall be contacted < 24 hours
Low	Request for replacing a hardware device or installing software application for user. Includes replacement media, Portal user creations, portal project requests etc.	Site shall be contacted < 48 hours

3.6.1.2 PROBLEM TROUBLE REPORT (PTR) PROCESS

1. The Contractor shall create a PTR process. The Contractor shall implement a Portal Issue Tracker tool to track PTRs. Relevant files, such as log files or images, shall be attached to the ticket. As a minimum, the Contractor shall track the following fields:
    a. **Subject** – Short summary description of the observed issue.
    b. **Description** – Detailed description of the issue. This field should describe the symptoms of the issue in as much detail.
    c. **Status** – The current status of the issue. This field is defaulted to "Open" and, typically, should not be changed at Issue creation. In the rare case of an issue that needs immediate attention, this field may be set to "Assigned" with the **Assigned to** field being set to an appropriate person.
    d. **Priority** – The priority of the ticket (Critical, High, Medium, Low). This field is used to indicate the order at which tickets are worked. Highest priority tickets will be worked first.

Priority	Description
Critical	Assignee shall work immediately, taking priority over all other assigned tickets. Assignee will suspend work on other tickets.
High	Assignee will work as-soon-as-possible, taking precedence over other lower priority assigned tickets.

Medium	Assignee shall work all higher priority assigned tickets first. Medium priority tickets shall not be worked before all higher priority tickets are being worked or are complete.
Low	Assignee shall work all higher priority assigned tickets first. Low priority tickets will be worked as time permits.

e. **Category** – Indicates the category of the issue described in the ticket. For example, if the issue is a problem with one of the gateways, the "Gateways" category should be selected. If it is an issue with Radiant Mercury, the "CDS" category should be selected.

f. **Workaround** – Proves a description of how to work around the identified issue. This can be a procedural workaround or a software workaround. The workaround must be reasonable and allow continued use of the system without significant hindrance. If no workaround is available, fill in this field with "None".

g. **Severity** – Numeric value from 1-5 indicating how the issue affects the system.

Severity	**Applies if a problem could:**	
1	a. Prevent the accomplishment of an operational or mission essential capability.	b. Jeopardize safety, security, or other requirement designated "critical".
2	a. Adversely affect the accomplishment of an operational or mission essential capability and no work-around solution is known.	b. Adversely affect technical, cost, or schedule risks to the project or to life cycle support of the system, and no work-around solution is known.
3	a. Adversely affect the accomplishment of an operational or mission essential capability but a work-around solution is known.	b. Adversely affect technical, cost, or schedule risks to the project or to life cycle support of the system, but a work-around solution is known.
4	a. Result in user/operator inconvenience or annoyance but does not affect a	b. Result in inconvenience or annoyance for development or support personnel, but does not

	required operational or mission essential capability.	prevent the accomplishment of those responsibilities.
5	Any other issue that should be captured about the system.	

3.6.1.3 PRODUCTION & DEPLOYMENT PROCESS

LVC-IA production system testing will be conducted prior to fielding. System testing will be monitored by the LVC-IA government representatives and approved for shipping.

Software updates that include PTR fixes will be directed by the Configuration Control Board (CCB). This effort shall fall under the responsibility of the program's PDSS effort. The CCB shall direct the Contractor to support the verification of changes before fielding. Once PTR fixes and testing are completed, these fixes shall be assigned with an ".xx" nomenclature to signify an interim version release. Subsequently, the PDSS section shall deploy the software to the respective installations and the Contractor shall install and confirm those updates are operating correctly. Installation personnel observations of anomalies or issues shall provide detailed information in the authorized discrepancy form to the PDSS section.

3.6.1.4 MAINTAINER/OPERATOR UPGRADE & TECHNICAL REFRESH TRAINING

The Contractor shall provide annual Upgrade Training & Technical Refresh courses for both Maintainers and Operators. Each course will stagger 6 months apart. The training shall be held at the Contractor's PDSS facility.

3.7 INTELLECTUAL PROPERTY AND DATA RIGHTS

The Contractor shall provide the Government with unlimited data rights to any intellectual property, source code and data produced in the course of design, configuration, deployment, training, testing, utilization, and support delivered under this contract. All delivered data shall be marked accordingly.

4. ACRONYM LIST

ACRONYM	DESCRIPTION
A&A	Assess and Authorize
AO	Authorizing Official
AR	Army Regulation
AT	Antiterrorism
AVCATT	Aviation Combined Arms Tactical Trainer
BOIP	Basis Of Issue Plan
CCB	Configuration Control Board
CCTT	Close Combat Tactical Trainer
CDD	Capability Development Document
CDR	Critical Design Review
CDRL	Contract Data Requirements List
CDS	Cross Domain Solution
CESI	Cole Engineering Services, Inc
CFSR	Contract Funds Status Report
CHESS	Computer Hardware Enterprise Software and Solutions
CIA	Confidentiality, Integrity and Availability
CIO	Chief Information Officer
CIPR	Contract Invoicing and Payment Report
CL	Confidentiality Level
CMP	Configuration Management Plan
CMVP	Cryptographic Module Validation Program
CNSSI	Committee on National Security Systems Instruction
CONUS	Continental United States
COR	Contracting Officer's Representative
COTS	Commercial Off The Shelf
CPD	Capability Production Document
CSPAR	Common Standards, Products, Architectures and/or Repositories
CSPEI	Computer Software Product End Item
CTO	Communications Tasking Order
CWBS	Contract Work Breakdown Structure
DOD	Department Of Defense
DODI	Department Of Defense Instruction
DODM	Department Of Defense Manual
DODAF	Department Of Defense Architecture Framework

DSTS	Dismounted Soldier Training System
EVMS	Earned Value Management System
FCA	Functional Configuration Audit
FoS	Family Of Systems
FVT	Functional Verification Test
FUA	First Use Assessment
GAT	Government Acceptance Test
GFE	Government Furnished Equipment
GOTS	Government Off The Shelf
HBSS	Host-Based Security System
HITS	Home Station Instrumentation Training System
IA	Information Assurance
IAW	In Accordance With
IAVA	Information Assurance Vulnerability Alert
IAVM	Information Assurance Vulnerability Management
IBR	Integrated Baseline Review
ICD	Interface Control Document
ICS	Interim Contract Support
IDE	Integrated Digital Environment
IE	Integration Event
IMP	Integrated Master Plan
IMS	Integrated Master Schedule
IPMR	Integrated Program Management Report
IPT	Integrated Product Team
IRS	Interface Requirement Specification
IS	Information System
IT	Information Technology
ITE	Integrated Training Environment
IUID	Item Unique Identification
JDIF	Joint Development Integration Facility
JLCCTC-ERF	Joint Land Component Constructive Training Capability-Entity Resolution Federation
LCC	Life Cycle Cost
LVC	Live Virtual Constructive
LVC-IA	Live Virtual Constructive – Integrating Architecture
MAC	Mission Assurance Category
NDI	Non-development Item
NET	New Equipment Training

NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSI	National Security Information
NSS	National Security Systems
NSTISSP	National Security Telecommunications and Information Systems Security Policy
O&M	Operations and Maintenance
OCONUS	Outside Continental United States
OSMP	Open System Management Plan
OSAT	On-Site Acceptance Test
P3I	Pre-Planned Product Improvement
PDD	Product Definition Data
PDSS	Post Deployment Software Support
PEO STRI	Program Executive Office Simulation Training Instrumentation
PM ITE	Program Manager Integrated Training Environment
PdM WTI	Product Manager Warrior Training Integration
PMB	Performance Measurement Baseline
PMR	Program Management Review
PTR	Problem Trouble Report
RAM	Reliability, Availability and Maintainability
RMF	Risk Management Framework
SAR	Safety Assessment Report
SDP	Software Development Plan
SEMP	System Engineering Management Plan
SIPRNET	Secret Internet Protocol Router Network
SMP	System Measurement Performance
SOW	Statement of Work
SPS	Software Product Specification
SRR	Systems Requirements Review
SRS	Software Requirements Specification
STIG	Security Technical Implementation Guides
STOC	Simulation and Training Omnibus Contract
SVD	Software Version Description
TADSS	Training Aids Devices Simulators Simulations
TDP	Technical Data Package
T&E	Test and Evaluation

TEMP	Test and Evaluation Master Plan
TIM	Technical Interchange Meeting
TPM	Technical Performance Measure
TRR	Test Readiness Review
UID	Unique Identification
VBS3	Virtual BattleSpace 3
WTI	Warrior Training Integration