a. The Contractor will provide visibility into program management, cost and schedule performance, systems/software engineering, technical performance, risk management, and issue management.

b. The Contractor will provide visibility into cost and schedule performance measured against the contract baseline through monthly Earned Value Management System reporting and quarterly Contract Funds Status Reporting. **Contract Data Requirements List (CDRL) A001, A002**

c. The Contractor will report ALL Contractor manpower (including subcontractor manpower) required for performance of this contract. The Contractor is required to completely fill in all the information in the format using the following web address: https://cmra.army.mil. As part of its submission, the Contractor will also provide the estimated total cost (if any) incurred to comply with this reporting requirement. Reporting period will be the period of performance (POP) not to exceed 12 months ending 30 September of each Government fiscal year and must be reported by 31 October of each calendar year.

d. The Contractor will host a post-award/contract kick-off meeting at the Contractor's facility no later than (NLT) 30 calendar days after contract award. The Contractor will support quarterly Program Management Reviews (PMRs) with the first PMR to be jointly scheduled between the Contractor and the Government after completion of the Integrated Baseline Review (IBR) event. The purpose of the PMR is to review program status in the following areas: cost, schedule, performance, and risk/issues. **CDRL A003**

e. An IBR will be conducted as soon as the integrated baseline has been fully planned and laid in. The Government requires this to be NLT 120 calendar days after contract award; however, the Contractor will advise of its readiness to enter into an IBR. The Contractor will build a Performance Measurement Baseline (PMB) that assess realism at the lowest level; assess technical, schedule, cost, resource, and management process risks; ensures control account coverage of 80 percent of the CLIN value; and limits the use of level of effort planning. The Contractor will provide work authorization documents; control account plans; schedule planning documents; basis of estimates; and other documentation as early as possible for Government review to assist in the assurance of making the IBR a successful event for the program. After execution of the IBR and the establishment of the PMB, the Contractor will thereafter execute Baseline Reviews (BRs) on a bi-annual basis (every six months) to allow for rolling wave planning. The purpose of the BRs is to review the detailed planning for the next rolling wave period. If substantial changes occur to the PMB over the course of the POP resulting in the need to substantially replan or reprogram the PMB the Government may request subsequent IBRs.

f. To minimize the costs associated with travel and hosting events, the Contractor will consolidate meetings, reviews, Technical Interchange Meetings (TIMs), and conferences as much as practical and feasible. The Contractor will also utilize video

teleconferencing and teleconferencing when possible to minimize travel requirements. The Contractor will coordinate agendas with the Government via electronic means. Deliverables are not required for informal meetings such as working group meetings and TIMs.

g. The Contractor will establish and participate in Integrated Product Teams (IPTs), TIMs, and Engineering, design and test activities such as reviews, meetings, demonstrations, experiments, etc.; this support will be provided on-site, via teleconference, via email, and via web conferencing as directed.

h. The Contractor will review, evaluate, analyze, create, prepare, and submit documentation, data, reports, architectures, and software. The Contractor will be required to travel at times. **CDRL A004**

i. The Contractor will propose and implement a formal joint Contractor/Government Risk Management Process to identify and mitigate/leverage program risks/opportunities on a continual basis. This process will be described in the Contractor's Risk Management Plan (RMP). The RMP will closely integrate risk/opportunity management with key Product Director (PdD) and engineering processes, be consistent with the PdD structure, and support regular reviews of progress. Additionally, the risk management process will provide for direct participation by Subcontractors/Suppliers or provide Government visibility into Subcontractor risk/opportunity management processes, provide for a management tool easily accessible to the Contractor, Government, and Subcontractors, and for those risks that are "realized," provide for a clear link to a well-defined issue management process. Risk reporting will occur via monthly joint IPT meetings and materials created to support the IPT will be available via DI2E and Contractor's Integrated Data Environment (IDE). **CDRL A005**

j. Utilize a Contractor developed/managed IDE to manage the overall execution of the program. The Contractor will submit data in an electronic format and post it on a secure, Contractor-managed IDE to support effective communication and timely exchange of information. This IDE will be secure and password protected to allow for limited and controlled access (Government view only permissions). Only unclassified information will be allowed in this forum. The IDE will be a single, centralized database for the management of all contract generated data. The IDE will be used to access the data listed on the Data Accession List. The system should include facilities for storage of all data developed or utilized for this contract, and provide the Government equal access to data. The IDE will use Microsoft® Office or compatible products. The Contractor will ensure all data is centrally available with unlimited Government access for review. The Government reserves the right to review all data associated with and developed on this contract. **CDRL A006**

k. The Contractor will provide specialists in the areas of interoperability (communications and messaging), system and software architectures, and operational fires and ballistics.

l. The Contractor will provide personnel that serve as Subject Matter Experts (SMEs) in AFATDS 7.0 and Marine Corps related requirements and technical matters. Personnel will directly interface with members of the Marine Corps and address questions, concerns, and requests for information as related to the design, development, deployment, and use of AFATDS 7.0. SMEs will travel approximately thirteen weeks throughout the POP of CLINs 0001 and 0002 to various CONUS locations.

m. The Contractor will provide personnel that serve as SMEs in AFATDS 7.0 and United States Air Force (USAF) machine-to-machine technical interfaces and data exchanges with AFATDS 7.0. Personnel will directly interface with members of the USAF to address questions, concerns, and requests for information related to interoperability between USAF systems and AFATDS 7.0. SMEs will travel approximately thirteen weeks throughout the POP of CLINs 0001 and 0002 to various CONUS locations.

n. The Contractor will provide personnel that service as SMEs in ASCA. Personnel will be required to support coalition interfaces and testing.

o. The Contractor will utilize Government studies and analysis that have been executed to explore ways to improve and simplify the AFATDS system. The Contractor will review the results of these studies and analysis to makes best use of their findings.

p. The Contractor will provide insight into the design by conducting necessary design reviews/milestones. At a minimum, the reviews/milestones will include, but are not be limited to: **Requirements Analysis Review, Preliminary Design Review, Critical Design Review, In Process Review, Test Readiness Review, and Test Completion Review.** The Contractor will address the applicable entry and exit criteria for every review via their IMP.

Deliverable(s):

CDRL A001	*Integrated Program Management Report (DI-MGMT-81861)*
CDRL A002	*Contract Funds Status Report (DI-MGMT-81468)*
CDRL A003	*Report, Record of Meeting Minutes (DI-ADMIN-81505)*
CDRL A004	*Trip Reports (DI-MISC-80508B)*
CDRL A005	*Contractor's Risk Management Plan (DI-MGMT-81808)*
CDRL A006	*Data Accession List (DI-MGMT-81453A NOT 1)*

6.6 Task 6 Software Design and Engineering

a. The Contractor will design/modernize a software baseline in accordance with the AFATDS 7.0 SRS and provide design documentation. **CDRL A007, A008, A009, A010**

b. The Contractor will employ "leading edge" and truly innovative engineering principles in order to ensure the application of best practices, defined processes, standards, and incorporate a development structure that embodies innovation, flexibility, and agility.

c. The Contractor will recognize and recommend opportunities for design improvements, optimization, and streamlining throughout the course of development. The Contractor will identify these opportunities to the Government along with associated recommendations that could be pursued throughout the course of development.

d. The Contractor will collaborate with various Contractors for the AFATDS 7.0 design effort (e.g. previous AFATDS 6.8.1.1 developer, interfacing components developers (software and hardware, etc.).

e. The Contractor will accept Government-Furnished AFATDS baselines for inclusion into the AFATDS 7.0 baseline undergoing development.

Deliverable(s):

CDRL A007	*Software Development Plan (DI-IPSC-81427A NOT 1)*
CDRL A008	*System/Subsystem Specification (DI-IPSC-81431A NOT 1)*
CDRL A009	*Software Design Description (DI-IPSC-81435A NOT 1)*
CDRL A010	*System/Subsystem Design Document (DI-IPSC-81432A NOT 1)*

6.7 Task 7 Requirements Decomposition and Management of Development

a. The Contractor will prepare, update, and manage documents to include but not limited to: Software Requirement Specification, Software Version Description, Interface Requirement Specification, and Interface Control Documents. **CDRL A011**, **A012, A013, A014**

b. The Contractor will develop requirements at the system, interface, and software levels. All system, interface, and software requirements will be documented using the DOORS. The database will be continually maintained and updated to account for test cases, code unites, and traceability of functional requirements to the requirements definition documentation. The Contractor will maintain the technical database for the baselines: 1) entering contractor system test; 2) entering test for record; 3) entering Army Interoperability Certification testing; and 4) constituting final delivery to the Government. Contractor will monitor and manage all change notices after requirements definition documentation is baselined.

c. Contractor will establish a metrics program for the collection and reporting of software metrics which will provide insight into the developmental progress and trends. These metrics at a minimum will: 1) track developmental progress; 2) provide status; 3) trends of software defects/faults; and 4) will give an indication of the extent to which testing success is achieved. The Contractor will readily have

available the source lines of code count, by language type for each baseline product. **CDRL A015**

Deliverable(s):

CDRL A011	*Software Requirements Specification (DI-IPSC-81433A NOT 1)*
CDRL A012	*Software Version Description (DI-IPSC-81442A NOT 1)*
CDRL A013	*Interface Requirements Specification (DI-IPSC-81434A NOT 1)*
CDRL A014	*Interface Control Document (DI-SESS-81248B)*
CDRL A015	*Software Metrics Report (DI-MGMT-80368/T)*

6.8 Task 8 Configuration Management

a. The Contractor shall employ a comprehensive CM program in alignment with EIA-649-1 through the life-cycle of the contract. At a minimum the following items will be under CM control: 1) Those portion of the Software Development Environment (SDE) critical to software development and maintenance; 2) Non-developmental software products acquired by the Contractor for use in the operational software or the SDE; 3) All AFATDS software components and baseline documentation; and 4) All GFI software to use and reuse with AFATDS 7.0. **CDRL A016**

b. The Contractor will provide insight into the CM program by inviting the Government to all CM meetings and allowing full participation in the Contractor's Configuration Control Board (CCB) as a voting member. CCB meetings with be held no less than monthly and will include all Subcontractors.

c. The Contractor will establish and maintain a configuration change control process. The Contractor will prepare and maintain configuration baseline description records to provide for configuration identification, change control, status accounting, compatibility, traceability and integrity of configuration items. If required, the Contractor will submit engineering change proposals, request for waivers/deviations for all Class 1 changes. **CDRL A017, A018**

Deliverable(s):

CDRL A016	*Configuration Management Plan (DI-SESS-81875)*
CDRL A017	*Engineering Change Proposal (DI-SESS-81880)*
CDRL A018	*Request for Waiver/Deviation (DI-SESS-81732)*

6.9 Task 9 Quality Assurance

a. The Contractor will implement and maintain a Quality Assurance Program. Contractor's established internal quality assurance control and inspection procedures shall be made available for Government review. **CDRL A019**

b. The Contract will implement and maintain a Government Furnished Equipment (GFE) program and manage all GFE provided for the Government. **CDRL A020**

Deliverable(s):
CDRL A019 Quality Assurance Program Plan (DI-QCIC-81794 NOT 1)
CDRL A020 Government Furnished Equipment Status Report (DI-MGMT-80269)

6.10 Task 10 Technical Publications

a. The Contractor will develop an Interactive Software User Manual and Interactive Software Administration Manuals for U.S. Army Material Command Logistics Support Activity Authentication and Army Publication Directorate distribution in Interactive Electronic Technical Manual format in accordance with MIL-STD-40051-1B and ETM (PDF) format in accordance with MIL-STD-40051-2B. The Contractor will develop all IETMs with additional interactivity and animation to include automated troubleshooting, interactive scalable vector graphics, and 3D objects. The Contractor will develop the IETMs for Digital Versatile Disc (DVD), webserver, and later use (by the Government) as a system embedded file. The Contractor will also develop IETMs to be compatible with the latest version of the AGM. **CDRL A021, CDRL A022**

b. Contractor will assist with updating technical manuals to reflect the new capability of AFATDS system components. **CDRL A022**

c. The Contractor will conduct validation events and participate in verification events of Technical Bulletin procedures and descriptions contained in the publications at the Contractor facilities. The Contractor's validation records will be available for the Government inspection at any time. The Government reserves the right to witness the Contractor validation. **CDRL A022**

d. The Contractor will participate in the verification and logistics demonstration events to be held at Continental U.S. locations as identified by the Government.

e. The Contractor will participate in Government verifications for all technical publication in order to record all 'red-lines' at the location designated by the Government. Red-Line changes will be incorporated within these documents during the conduct of the verification event. The Contractor will provide specified quantity of all draft products for these Government verifications.

f. The Contractor will participate in and support PM MC logistics demonstrations in order to record all "red-lines" at the location designated by the Government. The Contractor will provide specified quantity of all draft products.

g. The Government will verify all manuals procedures and equipment descriptions at the Contractor's or Government's facility. The Contractor will deliver draft publications for review by the Government.

Deliverable(s):

CDRL A021 Software User Manual, Software Administration Manual (DI-IPSC-81443A NOT 1)
CDRL A022 Interactive Electronic Technical Manuals, Technical Bulletins (DI-MISC-80711A)

6.11 Task 11 Training

a. The Contractor will support the Government's training program. The Contractor will coordinate with the Government's training providers (including other contractors) to identify training impacts engendered by the new capabilities.

b. The Contractor will perform individual task analysis on Contractor produced software for AFATDS and associated equipment, and determine which of the individual critical tasks that will impose training requirements for AFATDS operators and leaders (both Non-Commission Officer and Officer) in support of the following: Military Occupational Specialty (MOS) 13D, 13P, 13F, and 13R40; Warrant Officer MOS 131A and officer Area of Concentration 13A. Results of the task analysis will be recorded and the analysis will be the delta that will require task modification.

c. The Contractor will develop and maintain battle focused, task oriented, scenario driven Shareable Content Object Reference Model (SCORM) Conformant Operator Interactive Multimedia Instructions (IMI) Levels 2 to 3 in accordance with Department of Defense Instruction (DoDI) 1322.26, AR 350-1, and TRADOC Pamphlet 350-70-12. These products will support NET, instructor and key personnel training; institutional training; sustainment; and self-development training for all skill levels to be hosted on the Army Learning Management System and system embedded using a common development framework.

d. The Contractor will develop IMI and package learning content in multiple formats to include: Advanced Distributed Learning; SCORM Versions 1.2 and 2004 3rd and 4th editions; Flash (.SWF); HTML 5; and as a native Android app (.apk). **CDRL A023, A024**

e. The Contractor will support reuse of IMI material from a shared Government identified repository in order to maintain a consistent framework for developed courseware and support import of 3D objects, HTML 5, and Unity 3D from the PM MC, COE, CPCE, and MCE portfolio. At contract award, the Government will provide the appropriate source files for any reuse IMI materials. The Government will also provide access to the appropriate share repositories. The contractor is not required to procure any licenses for accessing to the shared repositories.

f. The Contractor will develop learning products that can be published to the Army Learning Management System standalone compact disc/DVD, webserver, or system embedded.

g. The Contractor will develop and maintain Tactics, Techniques, and Procedures Handbooks for the AFATDS Portfolio.

h. The Contractor will develop and maintain Quick Reference Card Sets based on the multiple variations of setup and configuration.

i. The Contractor will develop and maintain blended training strategies that incorporates the use of the IMI and IETMs in the classroom.

j. The Contractor will develop IMI to be compatible with the latest version of the AGM standard browser (Internet Explorer 8 and above). The government projects that by the time AFATDS 7.0 development is started the Internet Explorer version will be capable of supporting HTML5 features.

k. The Contractor will design, develop, and conduct an Instructor and Key Personnel (I&KP) training for the Government NET team (Government's Training Contractor); TRADOC service school instructors/training developers; and testers/data collectors/evaluators. Each training course will be in accordance with TRADOC Regulation 350-70. Any deviations will be approved by the Government.

l. The Contractor will provide I&KP to support the training developers, combat developers, testers and independent evaluators in support of test events, to be conducted NLT four months prior to scheduled Test Player Training Start or as defined in the Outline Test Plan.

m. Prior to Government acceptance, all NET training products and IMI courseware will be validated in accordance with guidelines specified in TRADOC Regulation 350-70-10. The Contractor will conduct validations (with oversight) in a Government designated facility with a target population (or a population that possess the critical characteristics of the target population) furnished by the Government. The Contractor will document the Government's critique, reconcile identified issues, provide feedback, and incorporate mutually agreed comments into the training application.

n. The Contractor will participate in the verification and logistics demonstration events to be held at Continental U.S. locations as identified by the Government.

o. The Contractor will participate in Government verifications for all training products in order to record all 'red-lines' at the location designated by the Government. Red-line changes will be incorporated within these documents during the conduct of the verification event. The Contractor will provide the specified quantity of all draft products for these Government verifications.

p. The Contractor will support, at a minimum, three separate training conferences. The training conferences will be at a schedule to be determined by the Government.

Deliverable(s):
CDRL A023 Instructional Media Package (DI-PSSS-81526C)
CDRL A024 Program of Instructions, Lesson Plans, Doctrine and Tactics Training, NET, Tactics, Techniques, Procedures Handbooks, Quick Reference Card Set (DI-PSSS-81522C)

6.12 Task 12 Information Assurance

6.12.1 Subtask 1 RMF Process

The Contractor will support the Government's cybersecurity implementation of the RMF process for AFATDS 7.0. The Contractor will support all aspects of the RMF including the following:

- System Security Plan
- Categorize System
- Select Security Controls
- Implement Security Controls
- Assess Security Controls
- Authorize System
- Monitor Security Controls

The Contractor will develop a System Security Plan (SSP) that provides an overview of the security requirements for the system and describes the security controls in place or planned for meeting those requirements. The security plan should include implementation status, responsible entities, resources, and estimated completion dates. Security plans may also include, but are not limited to, a compiled list of system characteristics or qualities required for system registration, key security-related documents such as a risk assessment, privacy impact assessment, system interconnection agreements, contingency plan, security configurations, configuration management plan, and incident response plan.

6.12.2 Subtask 2 Categorize System

The Contractor will support Step 1 of the RMF, categorize the system. The system has the following RMF Categorization levels: Confidentiality: Medium; Integrity: High; Availability: High. The results of the system categorization will be documented in the SSP. The system categorization is a coordinated effort between the Contractor and the Government's cybersecurity team. The system will be described (including system boundary) and documented in the SSP. The Government has the responsibility of registering the system in the enterprise Mission Assurance Support Service (eMASS). After the Government registers

the system in eMASS the Contractor will be responsible for inputting data into the eMASS system, as outlined in the following sections.

6.12.3 Subtask 3 Select Security Controls

The Contractor will support Step 2 of the RMF to select appropriate security controls based on the system categorization. The Contractor will assist the Government in the selection of appropriate controls by identification of the security control baseline for the system, and documenting these in the SSP. Baseline controls and control overlays will be tailored for the system. Overlays may add or subtract security controls, or provide additional guidance regarding security controls, resulting in a set of security controls applicable to the system that is a combination of the baseline and overlay. The combination of baselines and overlays address the unique security protection needs associated with the system. If necessary, control sets will be tailored (modified) in response to increased risk from changes in threats or vulnerabilities, or variations in risk tolerance. Tailoring decisions must be coordinated with the Government, and aligned with operational considerations and the system environment. Security controls will be added or removed only as a function of specified, risk-based determinations. Tailoring decisions, including the specific rationale (e.g., mapping to risk tolerance) for those decisions, will be documented in the security plan for the system. A monitoring strategy must be developed and documented as a system-level strategy for the continuous monitoring of the effectiveness of security controls employed within or inherited by the system, and monitoring of any proposed or actual changes to the system and its environment of operation. The strategy must include the plan for annual assessments of a subset of implemented security controls, and the level of independence required of the assessor (e.g., Information System Security Manager (ISSM) or Security Control Assessor (SCA)). The breadth, depth, and rigor of these annual assessments will be reflective of the security categorization of the system and threats to the system. Delivery of the security control selection will consist of input into the eMASS system on SIPRNET.

6.12.4 Subtask 4 Implement Security Controls

The Contractor will support Step 3 of RMF, implementation of security controls. The system (including applications) will be configured in accordance with applicable Security Technical Implementation Guides (STIGs) which are coordinated with the Government ISSM and SCA. STIGs are product-specific and document applicable DoD policies and security requirements, as well as best practices and configuration guidelines. STIGs are associated with security controls through Control Correlation Identifier (CCIs), which are decompositions of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 security controls (as amplified by Committee on National Security Systems 1253) into single, actionable, measurable items. Security Requirements Guide (SRG) is developed by Defense Information Systems Agency (DISA) to

provide general security compliance guidelines and serve as source guidance documents for STIGs. When a STIG is not available for a product, an SRG may be used. STIGs, SRGs and CCIs are available on the Information Assurance (IA) Support Environment Website (https://iase.disa.mil). STIG and SRG compliance results for products will be documented as security control assessment results within the security assessment report and reviewed by the PM MC responsible ISSM. The Contractor will coordinate the selection of applicable STIG, SRG, and CCI with the Government's ISSM. The Contractor will support the implementation of security controls for the system. The Contractor will participate in CCB and other meetings to coordinate for implementation of security controls. Security control requirements will be documented as a trouble report for tracking of implementation. These will be prioritized by the CCB. The DISA SRG/STIG Collection Tool will be used to document applicable documents. In addition, each control will be documented with the applicable trouble report identifier in eMASS.

6.12.5 Subtask 5 Assess Security Controls

The Contractor will support Step 4 of RMF, security control assessment. The Contractor will develop a plan to assess the security controls, known as the Security Assessment Plan. An assessment methodology can be found in NIST Special Publication 800-53A. The Contractor will assess the security controls in accordance with the security assessment plan and DoD assessment procedures. Assessment procedures are used to verify that a security control has been properly implemented. SRG and STIG compliance results will be documented and used as part of the overall security control assessment. This assessment process will be conducted any time there are updates or changes made that would impact the assessments. Assessments will be recorded. If no vulnerabilities are found through the process of executing the assessment procedures, the security control is recorded as compliant. If vulnerabilities are found, the control is recorded as Not Compliant (NC) in the Plan of Action and Milestones (POA&M), with sufficient explanation. Vulnerability severity values are assigned to all NC controls by the SCA as part of the security control analysis to indicate the severity associated with the identified vulnerability. As part of the overall assessment prior to authority to operation, the Government will assign an assessment team. This team will be responsible for assessing overall compliance, determination of risk level, assessing and characterizing the aggregate level of risk to the system, and preparing the security assessment report. The Contractor will support the ISSM and assessment team in performing this assessment.

6.12.6 Subtask 6 Authorize System

The Contractor will support Step 5 of RMF, authorize system. The Contractor will assist in the authorization process through review of the POA&M with the ISSM. The POA&M identifies tasks that need to be accomplished to remediate or mitigate vulnerabilities, specifies resources required to accomplish the elements

of the plan, and includes milestones for completing tasks and their scheduled completion dates. The Contractors' assistance in developing the POA&M is vital to ensuring its maintenance throughout the system life cycle. Once posted to the POA&M, vulnerabilities will be updated after correction or mitigation actions are completed, but not removed. The associated trouble report will be documented and referenced in the POA&M. The Government will assemble the security authorization package for submission to the Authorization Official (AO) for review and final acceptance. The risk determinations will be submitted to the AO prior to approvals.

6.12.7 Subtask 7 Monitor Security Controls

The Contractor will support Step 6 of the RMF, continuous monitoring of security controls. This is accomplished by continuously monitoring the system for security-relevant events and configuration changes that negatively affect security posture. The Contractor will use the continuous monitoring strategy that was developed for the system and documented in the SSP. Periodic assessment of the quality of security controls implementation against performance indicators, such as: security incidents; Government exercises; and operational evaluations will be conducted by the Government, with the assistance of the Contractor. In addition, the Contractor will conduct internal assessments when system changes are being considered, to determine the risk of the changes. The Contractor must report any significant change in the security posture of the system, and recommended mitigations, immediately to the Government's ISSM. The Contractor or Government may recommend to the SCA or AO a reassessment of any or all security controls at any time. As part of the continuous monitoring process, the Contractor will ensure all servers, switches, routers firewalls, and any other equipment used on the network and managed by the Contractor are Information Assurance Vulnerability Assessment (IAVA) compliant. All network and security devices will be kept current, configurations will be installed to allow the most secure network possible while allowing for proper operation, and access to (and through) the network devices shall be strictly controlled. Server operating systems will be kept up to date and IAVA compliant. Contractor will assist the Government in performing periodic scans and inspections to ensure compliance. The Government will be provided with the necessary system accounts to view all system and device configurations for all sites handling AFATDS data to ensure compliance with configuration management, DoD, Army best security practices, and the National Security Agency router secure configuration guidelines. In addition, access will be provided to the security information management system to view any analysis results to coordinate response to security incidents. The Contractor will configure the Government's Assured Compliance Assessment Solution (ACAS) for each individual system.

6.12.8 Subtask 8 Security Engineering

a. The Contractor will comply with software development security requirements per DoDI 8500.01 "Cybersecurity" and to include: principle of last-privilege; AGM compliance; public key infrastructure and password compliance; STIG compliance; warning labels/classification banners; detailed identification of all Ports, Protocols, and Services required for operations (internal and external); maximum compliance DoD ports, protocols, and services management /category assurance list, mobile-code restrictions, allocation of all security requirements into the SRS. The Contractor will deliver a SSP documenting all security aspects of the program and a Cybersecurity Artifact Package. **CDRL A025, CDRL A026**

b. The Contractor will ensure maximum AFATDS compliance with HBSS without performance degradation.

c. The Contractor will have the ability to protect International Traffic in Arms Regulations (ITAR) restricted software, documentation, and related data products.

d. The Contractor will have the ability to generate and store classified materials and comply with Operational Security (OPSEC) regulations. The Contractor will develop an OPSEC plan to be reviewed and approved by the responsible Government OPSEC officer, per AR 530-1, Operations Security. This standard operating procedure/plan will specify the Government's critical information, why it needs to be protected, where it is located, who is responsible for it, and how to protect it. In addition, the Contractor shall identify an individual who will be an OPSEC Coordinator. The Contractor will ensure that this individual becomes OPSEC Level II certified per AR 530-1. Per AR 530-1, Operations Security, new contractor employees will complete Level I OPSEC training within thirty (30) calendar days of reporting for duty. All contractor employees will complete annual OPSEC awareness training. **CDRL A027**

e. The Contractor will deliver a Critical Functional Analysis and Program Protection Implementation Plan and support all required Government efforts to develop the Program Protection Plan. **CDRL A028, CDRL A029**

f. The Contractor will perform software assurance evaluation of AFATDS code and shall incorporate fixes through the development cycle to ensure that the final delivered version is free of defects.

Deliverable(s):

CDRL A025	*System Security Plan (DI-MISC-80711A)*
CDRL A026	*Cybersecurity Artifact Package (DI-MISC-80508B)*
CDRL A027	*Operations Security Plan (DI-MGMT-80934C)*
CDRL A028	*Critical Functional Analysis (DI-MISC-80508B)*
CDRL A029	*Program Protection Implementation Plan (DI-ADMN-81036)*

6.12.9 Subtask 9 Information Assurance Vulnerability Management (IAVM) and Security Update Support

a. The Contractor will develop an IAVM Plan that meets RMF controls for the system. The IAVM plan, will include monthly evaluation of Information Assurance Vulnerability Messages to include: Information Assurance Vulnerability Alerts (IAVAs), Information Assurance Vulnerability Bulletins (IAVBs), and situational awareness reports that can be located in the Army IAVM non-secure internet protocol router portal: https://west.esps.disa.mil/NETCOM/sites/G3/G36. In addition to IAVM and in accordance with good engineering practice the plan will also review the Contractor's security patches available for system software for inclusion in the next scheduled system software update, since these items may post well in advance of a DoD IAVM issuance. **CDRL A030**

b. The Contractor will update the IAVM Plan to reflect the current Government contracted support for monthly perimeter and quarterly core component updates. Perimeter defenses, such as the firewall, Virtual Private Network (VPN), policy based router and switches will be updated for IAVM compliance monthly. All patches will be tested to verify they do not interfere with the operation of the system, and procedures for deploying will be developed in coordination with the Government and rehearsed at the Contractor site.

c. The Contractor will develop a plan for RMF controls that provides for evaluation of any new system software/components. This evaluation will include:

- Filter for applicability from the following: quarterly STIG updates; IAVAs and IAVBs; Vulnerability Scans; Trouble Reports (TRs), Change Requests (CRs), engineering change proposals; commercial-off-the-shelf IA/IA-enabled device security patches.
- Perform initial IA assessment and document, if applicable.
- Provide justification for non-applicable vulnerabilities and STIG updates.
- Generate CRs from IA analysis, if applicable.
- Generate DoD information assurance certification and accreditation process /RMF CR/TR from IA analysis, if applicable.
- Provide monthly status of IAVA/IAVBs to IA Security Officer (IASO).
- Provide quarterly report of STIGs to IASO.
- Support the CCB.

Deliverable(s):
CDRL A030 *IAVM Plan (DI-MISC-80508B)*

6.12.10 Subtask 10 Cybersecurity Monitoring and Assessment

a. As the DoD transitions from host based security compliance assessments to the utilization of enterprise tools, organizational processes and workflows will be required to adapt a new methodology in support of continuous monitoring efforts. Industry standards such as the Security Content Automation Protocols (SCAP) and ACAS are evolving in support of the mission to rapidly deploy content to any security compliance tool in a normalized format. The compliance tool is now becoming a weapon on the information security battlefield. The Contractor will develop a process for implementation of cybersecurity tools developed by DoD for monitoring compliance and assessing systems for vulnerability introduced in the development, implementation or maintenance phases of a system. This suite of tools will be deployed as the Continuous Monitoring Suite (CMS). The Contractor will deliver the CMS for use across PM MC Systems. **CDRL A031**

b. ACAS is an integrated software solution that is scalable to an unlimited number of locations. The solution's tiering ability will give DoD enhanced enterprise security while being easy to install and manage. It can be easily deployed via download to all DoD agencies – without the need to procure and install appliance devices. The ACAS product suite easily provides the required automated network vulnerability scanning, configuration assessment, application vulnerability scanning, device configuration assessment, and network discovery it needs. Further, the product suite generates the required reports and data, with a centralized console, and is SCAP compliant. The Contractor will include the ACAS software in the CMS.

c. SCAP provides information awareness based on standardized results from those tools to accreditors; systems administrators; information system security managers; and senior civilian and military commanders for determining risk to their environment. The SCAP Validation Program is designed to test the ability of products to use the features and functionality available through SCAP and its component standards. SCAP checklists standardize and enable automation of the linkage between computer security configurations and the NIST SP 800-53 controls framework. The current version of SCAP is meant to perform initial measurement and continuous monitoring of security settings and corresponding SP 800-53 controls. In this way, SCAP contributes to the implementation, assessment, and monitoring steps of the DoD RMF.

Deliverable(s):
CDRL A031 Continuous Monitoring Suite (DI-MISC-80508B)

6.13 Task 13 Safety

The Contractor will conduct and implement a system safety management and engineering program using MIL-STD-882E. The Contractor will provide a system safety program plan for Government review and approval. The SSPP will include the tasks the Contractor will perform to fulfill the level of rigor activities and system and software safety analysis per MIL-STD-882E and the Joint Software System Safety Engineering handbook. The Contractor will provide a safety assessment report for Government review and approval. The safety assessment report will include the outputs from the tasks specified in the SSPP. The Contractor will analyze the AFATDS operational and requirements, considering the new AFATDS client architecture and AFATDS operating in CPCE and MCE. The Contractor will provide a preliminary hazard list, related to the design, operations, and functional capabilities of the proposed design, operating in CPCE and MCE, and recommend a strategy for mitigating, controlling, or minimizing the potential hazards. The Contractor will analyze and provide the safety impact of code reuse. **CDRL A032, CDRL A033**

Deliverable(s):
CDRL A032 System Safety Program Plan (DI-SAFT-81626)
CDRL A033 Safety Assessment Report (DI-SAFT-80102C

6.14 Task 14 Test and Evaluation

a The Contractor will establish, implement, and maintain a Test and Evaluation Program to verify compliance. This program will allow the maximum insight for the Government of all test activities and for detailed descriptions and tracking of all testing errors. The Contractor will develop and deliver test plans, test descriptions, and test reports. **CDRL A034, A035, A036**

b The Contractor will design and execute regression testing to verify that prior existing capability still function as required. The Contractor will conduct an analysis of the new requirements, anticipated interfaces, and other interoperability aspects to determine test modifications and scope of regression test threads to be executed during a specific release of the software and develop the regression test threads to ensure that no collateral breakage has occurred during the development and that no new errors have been introduced into software components that previously executed correctly. The Contractor will execute the regression test during the testing of each build of an AFATDS version.

c Integration of the latest NABK with AFATDS 7.0 will be performed. The Contractor will establish a suite of test cases specific to exercising the NABK within AFATDS 7.0 and conduct NABK specific testing in sufficient depth to accommodate safety considerations. NABK test cases used on the prior AFATDS versions will be provided as GFI to the Contractor.

d The Contractor will modify the NABK test tool that auto-runs the NABK test cases provided as GFI. The NABK test cases will be provided in XML format, which necessitates a change to the front end of the NABK test tool.

e The Contractor will conduct a Test for Record (TFR), which is defined as the controlled execution of Government approved system-level test cases, regression threads, and a stability test. The Contractor will ensure that the TFR also includes testing of security and safety requirements. The TFR is subject to Government observation, the focus of which is to determine the level of compliance with the AFATDS specifications.

f The Contractor will support exercises, experiments, demonstrations, and test events, which occur at locations other than the Contractor's facility. These events will include but not be limited to integration testing with interfacing systems; interoperability tests with coalition partners; joint certification testing; mission command engineering test events; operational test events; safety test events; security test events; central technical support facility; integration events and army interoperability; backward compatibility test events; and ASCA test events. Contractor personnel who are experts in the operations of the AFATDS will be available to support on-site. Also, personnel who are experts in on-site modifications and system administration to facilitate experimental operational concepts and pre-deployment/mission essential exercises will also be available to support on-site.

g The Contractor will support testing of AFATDS 7.0 by the Fire Support Test Directorate at Fort Sill, Oklahoma. In support of this testing, the Contractor will provide source code and associated build products. The Contractor will provide all requisite activities to resolve errors found during Government conducted tests, subsequent to the test completion review. These activities include but are not limited to, attending test related meetings, evaluating errors/anomalies, correcting software and test cases, conducting testing and regression testing, and preparing and submitting documentation and delivery of corrected baseline versions. The Contractor will also select, modify (if necessary), and execute a set of regression test cases required to verify that AFATDS remains in compliance with applicable specifications, that error fixes are valid, and that related functionality is not negatively impacted. The Government will reserve the right to approve the Test Case selection and to observe the conduct of tests. This effort will be completed upon Software Acceptance of the final software baseline.

Deliverable(s):
CDRL A034 Software Test Plan (DI-IPSC-81438A NOT 1)
CDRL A035 Software Test Description (DI-IPSC-81439A NOT 1)
CDRL A036 Software Test Report (DI-IPSC-81440A NOT 1)

6.15 Task 15 Software Deliveries and Acceptance

The Contractor will deliver the AFATDS 7.0 software in interim and final builds. These deliveries will be fully executable versions of the software to be installed in the target runtime environment. Engineering releases will be delivered to the Government

beginning one hundred twenty (120) days after contract award with subsequent engineering deliveries being provided every sixty (60) days thereafter. Final software delivery will occur in accordance with the POP of the CLIN and the established program IMP. Formal baseline acceptance will be in alignment with the validation and verification section of the AFATDS SRS. **CDRL A037**

Deliverable(s):
CDRL A037 Computer Software Product (DI-IPSC-81488)

6.16 Task 16 Engineering Support Services

As directed by individual Technical Direction Letters (TDLs), the Contractor will provide engineering support services. This support shall be targeted in the areas of but no limited to: systems/software engineering; new requirements decomposition; requirements trade analysis and risk assessments; training; and Government developmental/operational testing support.

Deliverable(s):
To be specified in individual TDLs

Engineering Support Surge: The Government may require surge support during the base or any option period, and surge modifications for Engineering Support Services. Surge support over the life of the contract will not exceed $20M. Throughout the lifecycle of the contract, TDLs may be issued for tasks involving Systems/Software Engineering Support Services; New Requirements Decomposition and Analysis; Requirements Trade Analysis and Risk Assessments; Conducting Training; and Government Developmental/Operational Testing Support. The cost of each TDL will be negotiated and agreed upon based on the labor hours and from the agreed upon rates in the contract. The fixed fee is payable for 8%.

7. Performance Standards.

The performance standards associated with this contract are primarily defined in the AFATDS Incentives Plan. TDLs executed for Engineering Support Services will include performance standards and quality assurance surveillance procedures unique to the scope of each TDL.

8. Incentives.

See Incentives Plan RFP HC1028-16-R-0005, attachment J-3.

9. Place of Performance.

The Contractor will perform all activities at the Contractor's facilities with the exception of when travel is required to support the requirements of the SOO. Contractor will travel to various (Continental United States only) locations in support of AFATDS development efforts.

10. Period of Performance.

This effort has a 5 year POP (26-month base CLIN; one optional 26-month CLIN; two 12-month base POP plus four 1-year option CLINs).

11. Delivery Schedule.

The delivery schedule for the associated CLINs under this contract are as listed in identified Section B. The delivery requirements associated with all CDRLs is captured in the Contractor's IMP.

SOO Task#	Deliverable Title	Format	Number	Calendar Days After Contract Start
6.5	Integrated Program Management Report	Ref: CDRL A001		
6.5	Contract Funds Status Report	Ref: CDRL A002		
6.5	Report, Record of Meeting Minutes	Ref: CDRL A003		
6.5	Trip Reports	Ref: CDRL A004		
6.5	Risk Mgmt Plan	Ref: CDRL A005		
6.5	Data Accession List	Ref: CDRL A006		
6.6	Software Development Plan	Ref: CDRL A007		
6.6	System/Subsystem Specification	Ref: CDRL A008		
6.6	Software Design Description	Ref: CDRL A009		
6.6	System/Subsystem Design Document	Ref: CDRL A010		
6.7	Software Requirements Specification	Ref: CDRL A011		
6.7	Software Version Description	Ref: CDRL A012		
6.7	Interface Requirements Specification	Ref: CDRL A013		
6.7	Interface Control	Ref: CDRL A014		

	Document	
6.7	Software Metrics Report	Ref: CDRL A015
6.8	Configuration Management Plan	Ref: CDRL A016
6.8	Engineering Change Proposal	Ref: CDRL A017
6.8	Request for Waiver/Deviation	Ref: CDRL A018
6.9	Quality Assurance Program Plan	Ref: CDRL A019
6.9	Government Furnished Equipment Status Report	Ref: CDRL A020
6.10	Software User Manual, Software Administration Manual	Ref: CDRL A021
6.10	Interactive Electronic Technical Manuals, Technical Bulletins	Ref: CDRL A022
6.11	Instructional Media Package	Ref: CDRL A023
6.11	Program of Instructions, Lesson Plans, Doctrine and Tactics Training, NET, Tactics, Techniques, Procedures Handbooks, Quick Reference Card Sets	Ref: CDRL A024
6.12.8	System Security Plan	Ref: CDRL A025
6.12.8	Cybersecurity Artifact Package	Ref: CDRL A026
6.12.8	Operations Security Plan	Ref: CDRL A027
6.12.8	Critical Functional	Ref: CDRL A028

	Analysis	
6.12.8	Program Protection Implementation Plan	Ref: CDRL A029
6.12.9	Information Assurance Vulnerability Management Plan	Ref: CDRL A030
6.12.10	Continuous Monitoring Suite	Ref: CDRL A031
6.13	System Safety Program Plan	Ref: CDRL A032
6.13	Safety Assessment Report	Ref: CDRL A033
6.14	Software Test Plan	Ref: CDRL A034
6.14	Software Test Description	Ref: CDRL A035
6.14	Software Test Report	Ref: CDRL A036
6.15	Computer Software Product	Ref: CDRL A037
6.16	Specified in individual TDLs	To be specified in individual TDLs
* Standard Distribution: 1 copy of the transmittal letter without the deliverable to the Contracting Officer shall be uploaded to https://www.ditco.disa.mil/dcop/Public/ASP/dcop.asp (for further information see Section F. 3 of the contract and Chapter 5, Section 2.b. of the Task Order Guidelines. 1 copy of the transmittal letter with the deliverable to the Primary COR.		

12. Security Requirements.

All security requirements are specified in the Contract Security Classification Specification, DD Form 254 (Attachment J-2). The highest level of security for this effort is SECRET. This section shall be considered a supplement to block 13 of the Government provided DD 254. The following security requirements shall apply to this effort.

12.1 Facility Security Clearance

The Contractor shall also have access to Communication Security (COMSEC), For Official Use Only, and security classification guide information. in performing the contract the Contractor will also have access to classified information at the Contractor's facility; will be able to receive and generate classified material; fabricate, modify, and store classified hardware; require a COMSEC account, have OPSEC requirements, and be authorized to use the defense courier services.

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

12.2 Security Clearance and IT Level

All personnel performing on this contract must be U.S. citizens. Those personnel requiring access to Secret information require at a minimum an interim Secret security clearance. Per AR 381-12 Threat Awareness and Reporting Program (TARP), contractor employees with security clearances must complete annual TARP training: http://cdsetrain.dtic.mil/thwarting/. Certifications will be submitted to the COR on an annual basis.

12.3 Investigation Requirements

All personnel requiring access to Secret information, under this contract must undergo a favorably adjudicated National Agency Check, Local Agency Check and Credit Check (NACLC) as a minimum investigation. The NACLC will be maintained current within 10-years and requests for Secret Periodic Reviews (SPRs) will be initiated ninety (90) days prior to the 10-year anniversary date of the previous NACLC or SPR.

12.4 Security Contacts

The applicable Security contacts for this Contract are:

Name:	
Organization:	U.S. Army, PM MC
DODAAC:	W80YBY
Address:	PM MC W6DR PEO C3T BLDG 6007 COMBAT DRIVE ABERDEEN PROVING GROUND, MD 21005-1846
Phone Number:	TBD
Fax Number:	TBD
E-Mail Address:	TBD

13. GFE/GFI.

All GFE for this contract is captured in the AFATDS 7.0 GFE attachment to the contract. See RFP attachment J-5.

14. Other Pertinent Information or Special Considerations.

a. Identification of Possible Follow-on Work. Not applicable.

b. Identification of Potential Conflicts of Interest. Not applicable.

c. Identification of Non-Disclosure Requirements. Contractor personnel working under this contract with access to Controlled Unclassified Information (CUI) or Secret information shall be required to sign Non-Disclosure Agreements (NDAs). All NDAs shall be maintained by the Contractor and submitted to the COR prior to accessing any CUI or Secret data.

INSTRUCTIONS FOR ACCESS TO THE AFATDS SOFTWARE BASELINE, TECHNICAL DOCUMENTATION

Note: Contractors who qualified and received access to the AFATDS software baseline and technical documentation during market research DO NOT need to reapply or resubmit forms. Contractors that were approved for access to the AFATDS source code and technical documentation under the Access Compliance Certification are granted extended access past the 180 days. Contractors are allowed keep all AFATDS source code, technical documentation, and derivative products for no later than 10 CALENDAR DAYS AFTER CONTRACT AWARD. Access requirements and those approved for access to this information remains unchanged and shall be followed as described in the Access Compliance Certification. No later than 10 calendar days after contract award, contractors shall comply with destruction requirements as documented in their Access Compliance Certification."

To qualify for access to afatds software baseline and technical documentation, the following criteria must be met:

- Maintain compliance with Code of Federal Regulations Title 22, Subchapter M, ITAR and provide evidence of current registration in accordance with Part 122 Section 122.1.

- Have a software development environment that is approved for the generation, maintenance and control of ITAR items.

- Have an existing facility security clearance of at least U.S. SECRET from the Defense Security Service. Provide a copy of the facility clearance letter with Joint Personnel Adjudication System Security Management Office Code for verification.

- Candidates must be participants in the Defense Industrial Base (DIB) Cyber Security / Information Assurance (CS/IA) program. The DoD DIB CS/IA program enhances and supplements participants' capabilities to safeguard DoD information that resides on, or transits, DIB unclassified information systems. See https://dibnet.dod.mil/ for additional information.

Instructions for Access:

Contractors must contact Dustie Thompson, Contract Specialist via email dustie.m.thompson.civ@mail.mil; (618) 229-9127 AND Karen Kinzel, Contracting Officer, karen.m.kinzel2.civ@mail.mil (618) 229-9243 for access to the AFATDS software baseline and technical documentation.

Contractors will then be required to complete an Access Certification of Compliance, complete a NDA, and provide a complete mailing address.

Upon receipt and clearance by the Contracting Officer, AFATDS baseline and technical documentation will be mailed a package via FEDEX for access to pertinent information.

FOR ACCESS TO SRS:

*Note: AFATDS SRS will be distributed via secure website transfer.

Contractors must have submitted a NDA and may request by contacting Dustie Thompson, Contract Specialist via email dustie.m.thompson.civ@mail.mil; (618) 229-9127 AND Karen Kinzel, Contracting Officer, karen.m.kinzel2.civ@mail.mil (618) 229-9243.

d. Packaging, Packing and Shipping Instructions. Not Applicable

e. Inspection and Acceptance Criteria. As stated in Section E of the contract.

f. Property Accountability. Not Applicable

g. DoD Enterprise Service Management Framework (DESMF) Compliance. All IT service requirements contained within this SOO shall be conducted in accordance with the DESMF which can be accessed at https://community.apan.org/esmf_consortium_working_groups/m/desmf_ed_ii/default.aspx.

h. Supply Chain Risk Management. Not Applicable

15. Section 508 Accessibility Standards. Not applicable, AFATDS is exempt from Section 508 compliance as it is a National Security System.

Contract Number:	To Be Determined (TBD)
Task Order Number:	N/A
Tracking Number:	HC1028-16-R-0005
Follow-on to Previous Contract and Task Order Number:	Not Applicable

1. Contracting Officer's Representative (COR).

a. Primary COR.

Name:	TBD
Organization:	
Department of Defense Activity Address Code (DODAAC):	
Address:	
Phone Number:	
Fax Number:	
E-Mail Address:	

b. Alternate COR.

Name:	TBD
Organization:	
DODAAC:	
Address:	
Phone Number:	
Fax Number:	
E-Mail Address:	

2. Contract Title. Advanced Field Artillery Tactical Data System (AFATDS) 7.0

3. Background. The AFATDS is a multi-service, automated Command, Coordination, Communication, and Computing system that provides automated fire support and coordination to all echelons, from Firing Unit through Theater Level, at Army, Marine Corps, Naval Firing Platforms, Navy Command and Amphibious Assault Ships, Air Force Operations Centers and Joint Command and Control Centers. AFATDS enables the Force Commander's guidance to be automatically applied in the Fires Warfighting Function to plan, execute, and deliver effects at all levels of command within the current and future force. AFATDS can automatically tailor the selection of fire support assets (field artillery, mortars, close air support, naval gunfire, attack helicopters and offensive electronic warfare assets) based on Commander's Guidance, thereby enabling maximum effective use of all available fire support assets across the full spectrum of conflict.

It is the Government's objective to modernize the underlying AFATDS architecture, redesign the AFATDS front-end to a fully web and role based interface, integrate available common services made available through the Army's Common Operating Environment (COE) and incorporate advanced embedded training technologies to aid in operator initiated system instruction and refresher training. This next generation version of AFATDS is referred to as AFATDS 7.0.

4. Objectives: To procure an innovative and state-of-the-art solution that provides a modernized backend AFATDS architecture; incorporates the common services provided by COE Version 3 (v3); implements role duty based functionality; and provides embedded computer based training.

5. Scope. Scope of the effort includes system architecture design and analysis, system software interface support, design/system engineering and system integration. This effort also includes software design and development,

programmatic, engineering, testing, training, and integration for the implementation of the AFATDS capability in support of fires operational requirements within the Army and USMC operational architecture from fires platoon to echelon above Corps, Joint and Coalition command staffs, ASCA, and other international agreements.

6. Performance Requirements. *(Provide a narrative of the specific performance requirements or tasks that make up the PWS. Number the tasks sequentially, e.g., Task 1 - Title of Task and description, Task 2 - Title of Task and description, etc. Describe in clear terms, using active language, what work will be performed. A PWS must be "outcome-based," i.e., they must include the development and delivery of actual products (e.g., assessment report, migration strategy, implementation plan, etc.) Structure the PWS around the purpose of the work to be performed, i.e., what is to be performed, rather than how to perform it. The services acquired must not fall into the category of "personal services." Personal services are those contracted efforts that, by express terms, or as administered, make contractor personnel appear, in effect, as Government employees. See FAR Part 37.102 for a detailed discussion of personal services.*

For each requirement, there should be a corresponding standard(s), a statement of the maximum allowable degree of deviation from the standard, the method of surveillance to determine whether the standard is met, and a positive and/or negative incentive based on adherence to the standard.

6.1 Task 1 - Enterprise Management Controls. *(Example)*

6.1.1 Subtask 1 - Integration Management Control Planning. Provide the technical and functional activities at the required for integration of all tasks specified within this PWS. Include productivity and management methods such as quality assurance, progress/status reporting and program reviews. Provide the centralized administrative, clerical, documentation and related functions.

6.1.2 Subtask 2 - Task Order Management. Prepare a Task Order Management Plan describing the technical approach, organizational resources and management controls to be employed to meet the cost, performance and schedule requirements throughout TO execution. Provide a monthly status report monitoring the quality assurance, progress/status reporting and program reviews applied to the TO.

Deliverables: Task Order Management Plan *(Example)*
Monthly Status Report

6.2 Task 2. *(Description)*

6.2.1 Subtask 1. *(Description)*
6.2.2 Subtask 2. *(Description)*

Deliverables: *Test Plan* (List the deliverables associated with each task.)
Software Release Report

7. Performance Standards. *(Performance standards establish the performance levels required by the Government. These standards are driven by the application systems being converted or developed. Ensure that each standard is necessary, carefully chosen and not unduly burdensome. Identify only those outputs that are essential and should express the outputs in clear, concise, commonly used, easily understood, measurable terms. Do not repeat material in the PWS that is already included in other parts of the contract. Structure the PWS around the purpose of the work to be performed, i.e., what is to be performed, rather than how to perform it.*

Performance Standard	Acceptable Quality Level (AQL)	Method of Surveillance
Subtask 6.1.1 – Upgrade integrated COTS products IAW established	Performance occurs with no required re-performance or re-work at least 80% of the time. Problems	Routine inspection of deliverable products and services.

maintenance agreements.	that occur are minor and are resolved in a satisfactory manner.	
Subtask 6.5.1 - Briefing material will be delivered on time and IAW Government POC guidance	Materials contain required information and are delivered on time at least 90% of the time. Revisions that occur are minor and are resolved in a satisfactory manner.	Routine inspection of the materials.

8. Incentives. See Incentive Plan

9. Place of Performance. *(Specify whether the work will be performed at the contractor's site or at a Government site. For local or long distance travel, say:* Travel in and around the primary place of performance may be required throughout the period of performance. Additional travel within CONUS *or OCONUS (if applicable)* may be required to support the requirements of this PWS.

The following paragraph is required when the contractor performs work on-site at a government facility.

Alternate Place of Performance - Contingency Only. As determined by the Contracting Officer's Representative (COR), contractor employees may be required to work at an alternate place of performance (e.g., home, the contractor's facility, or another approved activity within the local travel area) in cases of unforeseen conditions or contingencies (e.g., pandemic conditions, exercises, government closure due to inclement weather, etc.). Non-emergency/non-essential contractors should not report to a closed government facility. Contractor shall prepare all deliverables and other contract documentation utilizing contractor resources. To the extent possible, the contractor shall use best efforts to provide the same level of support as stated in the PWS. In the event the services are impacted, reduced, compromised, etc., the Contracting Officer or the contractor may request an equitable adjustment pursuant to the Changes clause of the contract.

10. Period of Performance. 5 years: 26-month base Contract Line Item Number (CLIN); one optional 26-month CLIN; two 12-month base periods of performance (PoPs), plus four 1-year option CLINs. As directed by the COR, the contractor shall continue performance in emergency or mission essential conditions. Additionally, the contractor may be required to account for the whereabouts of their personnel should this information be requested by the COR.

11. Delivery Schedule. *(Describe precisely the items to be delivered, both during the period of performance (i.e., relating to the specific tasks described in paragraph 6. above) and at completion of the contract. Describe the schedule either in terms of calendar days from the date of contract Award or in calendar days when other projects or program elements are dependent on the delivery, e.g. "10 calendar days after draft plan approved." The required table format is as follows:)*

PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.1.1	Plan	A003/DI-MGMT-80347 *(Example)*	Date or calendar days after award or event		Standard Distribution*	Draft - 15 Final – 30
6.1.2	Report	A008/DI-MGMT-80368 *(Example)*			Two Copies to COR; Letter Only to KO	Monthly, on 5th workday
6.1.3	Software	Contractor-Determined Format *(allowable if desired)*			Standard Distribution*	180
6.x	*(Continue*	*as needed to document*	*deliverables)*			