08Performance Work Statement (PWS)

For

Soldier Monitoring System (SMS)

U.S. Army Capabilities Program Executive for
Simulation, Training, Testing and Threats (CPE ST3)
12211 Science Drive
Orlando, FL 32826-3276

LTC Kyle G. Hudalla
Product Manager Combat Training
Instrumentation Systems

Date:

DISTRIBUTION STATEMENT C: Distribution authorized to U.S. Government agencies and their Contractors, Administrative or Operational, 18 MAY 2026. Other requests for this document shall be referred to The Capabilities Program Executive Office for Simulation, Training, Testing and Threats (CPE ST3), SFAE-STR-TDC, 12211 Science Drive, Orlando, FL 32826-3276.

Controlled by: CPE ST3
Controlled by: SFAE-STR-TDC
CUI Category: General Procurement and Acquisition
Distribution: C
POC: BRIAN CAFFEE 727.504.5903

Table of Contents

1 Introduction 5
1.1 Mission Objective 5
1.2 Scope 5
1.2.1 System Description 6
1.2.1.1 Monitoring Station (MS) 6
1.2.1.2 Mobile Monitoring Device (MMD) 6
1.2.1.3 Soldier Worn Device (SWD) 6
1.2.1.4 Communication Network and SaaS 6
1.3 Background 6
1.4 Definitions 6
1.5 Applicable Documents 7
1.5.1 Department of Defense Specifications 8
1.5.2 Department of Defense Standards 8
1.5.3 Other Government Documents, Drawings and Publications 9
1.5.4 Industry Documents 10
1.5.5 Availability of Government Documents, Drawings and Publications 11
1.6 Order of Precedence 12
1.7 Acronyms 12
2 General Requirements 14
2.1 Non-Personal Services 14
2.2 Location, Period of Performance, and Hours of Work 14
2.2.1 Place of Performance 14
2.2.2 Period of Performance (PoP) 15
2.2.3 Hours of Work 15
2.2.4 Recognized Holidays 15
2.3 Personnel 15
2.3.1 Contractor Personnel, Disciplines, and Specialties 16
2.3.2 Personnel Conduct 16
2.4 Program Management and Administration 16
2.4.1 Program Meetings and Reviews 16
2.4.1.1 Integrated Product Team (IPT) Meetings 16
2.4.1.2 Program Management Review (PMR) 17
2.4.2 Contract Management 17
2.4.2.1 Integrated Master Schedule (IMS) 17
2.4.2.2 Contract Manpower Reporting Application (CMRA) 18
2.4.2.3 Financial Management 18
2.5 Live Training Transformation (LT2) Product Line Support and Synchronization 18
2.5.1 Synchronization with LT2 Configuration Management Baseline (CMB) 18
2.6 Data Rights 18
2.7 Incident Reporting 19
2.8 Counterfeit Risk Management (CRM) Program 20
2.8.1 Reporting Counterfeit or Suspected Counterfeit parts. 20
2.9 Contractor Training Requirements 20

2.9.1 Antiterrorism Threat (AT) Level 1 Training 20
2.9.2 Access and General protection/Security Policy and Procedures 20
2.9.3 For Contractors requiring Common Access Card (CAC) 21
2.9.4 For Contractors that do not require a CAC, but require Access to DoD Facility or Installation 21
2.9.5 iWATCH Training 21
2.9.6 Army Training Certification Tracking System (ATCTS) Registration 21
2.9.7 Operational Security (OPSEC) Program 21
2.9.8 OPSEC Training Requirement 22
2.9.9 Information Assurance (IA)/Information Technology (IT) Training 22
2.9.10 Information Assurance (IA)/Information Technology (IT) Certification 22
2.9.11 Handling or Access to Classified Information 22
2.9.12 Controlled Unclassified Information (CUI) Training 22
2.9.13 Threat Awareness Reporting Program (TARP) 22
2.10 Organizational Conflict of Interest (OCI) 23
2.11 Government Directed Travel / Temporary Duty 23
2.12 Cybersecurity 23
2.12.1 Security Engineering 23
2.12.2 Cybersecurity (FedRAMP) 24
2.12.2.1 SaaS SMS 24
2.12.2.2 PaaS SMS 24
2.12.2.3 IaaS SMS 24
2.12.3 Cybersecurity Tasks 24
2.12.4 Cybersecurity Compliance 24
2.13 Safety Assessment 25
2.13.1 Hazard Tracking and Risk Resolution 25
2.14 Program Specific Requirements 25
3 Performance Requirements 27
3.1 Specific Tasks 27
3.1.1 Contractor Training Management 27
3.1.2 Contractor Logistics and Supportability Management 28
4 Appendix A – Configuration Management Baseline (CMB) Import File 29
5 Appendix B – Performance Requirements Summary 30

Revision Log

Date	Version Revision	Author	Section(s)	Revision Description
July 26		Brian Caffee	All	Initial Release

1 Introduction

1.1 Mission Objective

Optimize, acquire, field, and sustain Solider Monitoring System (SMS) to minimize risks inherent to individual and isolated training required to improve Warfighter readiness.

Objective of this effort is to ensure continuity and delivery of efficient, effective, and quality **s**ervices of upgraded or new solutions to the nation's warfighters. The goal is to deliver systems on schedule, within cost, and to provide life cycle management to ensure the best value products for the United States Army.

1.2 Scope

This Performance Work Statement (PWS) establishes performance-based requirements to maintain and sustain SMS for Project Manager Training Devices (PM TRADE), Product Manager for Combat Training Instrumentation Systems (PdM CTIS). This includes all efforts necessary to ensure SMS technology and equipment is maintained at or above 95% Ao and provides telephonic and email help desk support to help ensure SMS capability is realized by the user.

This effort enables PdM CTIS to perform life cycle management in support of SMS including Continuous Technology Refresh (CTR), technology insertion, concurrency, upgrades, and disposal. Unless otherwise specified herein, the Contractor shall provide all personnel, equipment, supplies, facilities, transportation, tools, materiel, supervision, New Equipment Training (NET), and Interim Contract Support (ICS) necessary to satisfy the performance-based requirements contained in this PWS.

SMS requirements originated supporting Special Operations Forces (SOF) training that require Soldiers to be separated from Cadre and other trainees for extended durations. SMS provides the ability to observe (virtually) Soldier's locations, receive alerts from Soldiers needing assistance, and compile data for an After-Action Review (AAR). SMS minimizes risk inherent to individual and/or isolated training. Support services required for this effort include maintaining or providing the following:

1. SMS network and Software as a Service (SaaS).
2. Monitoring Stations.
3. Mobile Monitoring Devises.
4. Soldier Worn Devices.
5. Training and training materials.
6. Inventory and installations as required.
7. Repair/replace damaged or inoperable components.
8. Field service and maintenance support.
9. Help desk support.
10. Propagation Studies.
11. Provide maintenance, readiness, and operations reports as required.
12. Support monthly and weekly meetings as required.

1.2.1 System Description

Soldier Monitoring System (SMS) is the Army's materiel solution for Soldier monitoring, safety, and AAR for individual and isolated training. SMS reduces risks to Soldiers during individual and isolated training (e.g., land navigation) by providing persistent/real-time geo-tracking and automated alerts (including no-motion, boundary breaches, and Soldier-initiated alerts), which provide critical data for AARs. SMS enhances training realism, mitigates risks, helps ensure Soldier safety, and provides objective data to improve future training through detailed AARs. SMS is mobile, rugged, and has limited impact on Soldier's load and unit logistics. SMS is composed of the following components.

1.2.1.1 Monitoring Station (MS)

The MS component of SMS provides the capability to graphically track each device's location, receive device status/alerts, view all activity (locations, movements, alerts, etc.), and replay event data to support AARs) The MS normally consists of a laptop and a network connection.

1.2.1.2 Mobile Monitoring Device (MMD)

The MMD component of SMS provides capability to graphically track each device's location and receive device status/alerts. The MMD is a portable (dismounted) device used by cadre to monitor and locate Soldiers during a training exercise. MMD normally consists of a tablet and a network connection.

1.2.1.3 Soldier Worn Device (SWD)

The SWD is a small, rugged, waterproof radio that is typically attached to a Soldier's equipment or load-bearing vest. The SWD contains a built-in GPS that transmits the precise location and status data used for real-time monitoring over a Long-Term Evolution (LTE) network. This transmitted data provides the necessary information for an AAR to be created, which may then be used to assess Soldier performance. The device also includes a Soldier-initiated alert (SOS) button for emergencies.

1.2.1.4 Communication Network and SaaS

The communication and user interface (UI) component of SMS provides capability to connect all SMS devices to a secure server, accessible using an intuitive UI. The SMS network normally consists of commercial cellular, augmented with LoRa etc. to ensure adequate coverage, that connects to SMS SaaS riding on Amazon Web Service (AWS).

1.3 Background

Military training contains significant and inherent risk, including terrain, extreme weather, and wildlife; these risks are amplified during individual and/or isolated training, e.g., land navigation. These hazards have caused numerous serious injuries and fatalities over the last several years across the Army. The SMS reduces these risks by providing persistent/real-time geo-tracking and automated alerts, which provide both immediate safety oversight and critical data for analysis. The SMS program was initiated in response to a directive issued by the Vice Chief of Staff, Army (VCSA), following a fatality during a land navigation exercise. This directive emphasized the need to not only mitigate risk but also to improve training effectiveness by analyzing performance. The system's AAR function directly supports this goal by providing objective data

to assess individual and collective performance. The SMS is the Army's materiel solution for Soldier monitoring, safety, and training performance analysis for individual and isolated training.

1.4 Definitions

Contractor – A supplier or vendor awarded a contract to provide specific supplies or service to the Government. The term used in this contract refers to the prime.

Contracting Officer (COR) – A person with authority to enter into, administer, and or terminate contracts, and make related determinations and findings on behalf of the Government. Note: The only individual who can legally bind the Government.

Contracting Officers Representative (COR) – CORs are appointed by the Procuring Contracting Officer (PCO), in accordance with (IAW) Defense Federal Acquisition Regulations (DFARS) 201.602-2. The COR monitors all technical aspects of the contract and assists in contract administration but IS NOT authorized to oblige the Government or make determinations which may culminate into a change to any of the terms and conditions of the contract.

Defective Service – A service output that does not meet the standard of performance associated with the Performance Work Statement.

Deliverable – Anything that can be physically delivered but may include non-manufactured things such as meeting minutes or reports.

Interim Contractor Support (ICS) – Maintenance services and management of site logistical operations until the system fully transitions to a third party LCCS contractor.

Quality Assurance – The Government procedures to verify that services being performed by the Contractor are performed according to acceptable standards.

Quality Assurance Surveillance Plan (QASP) – An organized written document specifying the surveillance methodology to be used for surveillance of contractor performance.

Subcontractor – One that enters into a contract with a prime contractor. The Government does not have privity of contract with the subcontractor.

Workday – The number of hours per day the Contractor provides services in accordance with the contract.

Work Week – Monday through Friday, unless specified otherwise.

1.5 Applicable Documents

The following documents form a part of this PWS to the extent specified herein. In the event of a conflict between documents referenced herein and the contents of this PWS, the contents of the PWS shall be the governing requirement.

1.5.1 Department of Defense Specifications

Document Number	Title	Date
CARDS # 2557	Solider Monitoring System CDD	19 May 2019
DoD 5200.02	Procedures for the DoD Personnel Security Program	29 Oct 2020
DoD Manual 5200.01 – Vol 1	DoD Information Security Program: Overview, Classification, and Declassification	28 Jul 2020
DoD Manual 5200.01 – Vol 2	DoD Information Security Program: Marking of Information	28 Jul 2020
DoD Manual 5200.01 – Vol 3	DoD Information Security Program: Protection of Classified Information	28 Jul 2020
DoDM 8140.03	Cyberspace Workforce Qualification and Management Program	15 Feb 2023
DoDD 5000.01	The Defense Acquisition System	28 Jul 2022
DoDD 5144.02	DoD Chief Information Officer: Change 1	19 Sep 2017
DoDD 8140.01	Cyberspace Workforce Management	05 Oct 2020
DoDD 8500.01	Cybersecurity	07 Oct 2019
DoDI 5200.48	Controlled Unclassified Information (CUI)	06 Mar 2020
DoDI 4140.67	DoD Counterfeit Prevention Policy	26 Apr 2013
DoDI 5000.02	Operation of the Defense Acquisition System	08 Jun 2022
DoDI 8100.04	DoD Unified Capabilities (UC)	09 Dec 2010
DoDI 8500.01	Cybersecurity – Change 1	07 Oct 2019
DoDI 8510.01	Risk Management Framework for DoD Systems	19 Jul 2022
DoDI 8580.1	Information Assurance (IA) In the Defense Acquisition System	09 Jul 2004
DoDI 8582.01	Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information	09 Dec 2019

1.5.2 Department of Defense Standards

Document Number	Title	Date
MIL-PRF-32216B	Evaluation of Commercial Off-the-Shelf (COTS) Manuals and Preparation of Supplemental Data	03 Dec 2021
MIL-STD-130N(1)	Identification Marking of U.S. Military Property	26 Aug 2019
MIL-STD-882E	System Safety	27 Sep 2023
MIL-STD-31000B	Technical Data Packages	21 Aug 2023

Document Number	Title	Date
MIL-STD-461G	Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment	11 Dec 2015
MIL-STD-464D	Electromagnetic Environmental Effects Requirements for Systems	24 Dec 2020
MIL-STD-810H (1)	Environmental Engineering Considerations and Laboratory Tests	18 May 2022
MIL-STD-40051-1D(1)	Preparation of Digital Technical Information for Interactive Electronic Technical Manuals (IETMs) – COEI Work Package Format/Content	22 Nov 2021
MIL-STD-40051-2D(1)	Preparation of Digital Technical Information for Page-Based Technical Manuals (TMs)	22 Nov 2021

1.5.3 Other Government Documents, Drawings and Publications

Document Number	Title	Date
AR 25-1	Army Information Technology	15 Jul 2019
AR 25-2	Army Cybersecurity	04 Apr 2019
AR 190-13	The Army Physical Security Program	27 Jun 2019
AR 380-5	Army Information Security Program	25 Mar 2022
AR 381-12	Threat Awareness and Reporting Program	01 Jun 2016
AR 525-13	Antiterrorism	03 Dec 2019
AR 530-1	Operations Security	26 Sep 2014
AR 702-20	Counterfeit Risk Management Product Assurance	09 Jan 2023
ARMY DIR 2014-05	Policy and Implementation Procedures for Common Access Card Credentialing and Installation Access for Uncleared Contractors	07 Mar 2014
CNSSI No. 1253	Committee on National Security Systems Instructions - Security Categorization and Control Selection for National Security Systems	27 Mar 2014
DFARS Subpart 204.73	Safeguarding Covered Defense Information and Cyber Incident Reporting	30 Oct 2023
DFARS 252.204-7012	Safeguarding Covered Defense Information and Cyber Incident Reporting.	30 Oct 2023
DFARS 252.204.7020	NIST SP 800-171 DoD Assessment Requirements	30 Oct 2023
DFARS 252.225.7043	Antiterrorism/Force Protection for Defense Contractors Outside the United States	30 Oct 2023
DFARS 252.239.7001	Information Assurance Contractor Training and Certification	25 Apr 2024

Document Number	Title	Date
FAR 31.205-46	Travel costs	04 Dec 2023
FAR 52.204-2	Security Requirements	04 Dec 2023
FISP 140-2	Federal Information Processing Standards Publication – Security Requirements for Cryptographic Modules	03 Dec 2002
FISP 140-3	Federal Information Processing Standards Publication – Security Requirements for Cryptographic Modules	22 Mar 2019
FIPS 199	Federal Information Processing Standards Publication – Standard for Security Categorization of Federal Information and Information Systems	May 2003
FIPS 200	Federal Information Processing Standards Publication – Minimum Security Requirements for Federal Information and Information Systems	Mar 2006
Public Law 113-283 113th Congress	Federal Information System Management Act (FISMA) of 2014	18 Dec2014
LT2-TRADE-PLN-000384	Live Training Transformation (LT2) Operations Guide – Version CC	24 Apr 2024
SAE-GEIA-STD-0007C	Logistics Product Data	16 Apr 2014

1.5.4 Industry Documents

Document Number	Title	Date
ANSI/IEC 60529:2004	Degrees of Protection Provided by Enclosures (Ip Code)	23 Sep 2020
ANSI Z535.4-2011 (R21017)	American National Standard for Product Safety Signs and Labels	20 Oct 2017
NFPA 70	National Electric Code (NEC) Handbook	2023 Edition
ANSI/TIA-606-D	Administration Standard for Telecommunications Infrastructure	05 Oct 2021
ATA SPEC 300:2020.1	Air Transport Association (ATA) Specification for Packaging of Airline Supplies	01 Jan 2020
NIST SP 800-34	Contingency Planning Guide for Federal Information Systems	11 Nov 2010
NIST SP 800-37 Rev 2	Guide for Appling the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach	Dec 2018
NIST SP 800-47	National Institute of Standards and Technology (NIST) Special Publication (SP), Managing the Security of Information Exchanges	Jul 2021

Document Number	Title	Date
NIST SP 800-53	National Institute of Standards and Technology (NIST) Special Publications (SP) 800-53 Security and Privacy Controls for Federal Information Systems and Organizations	Sep 2020
NIST SP 800-53A	Assessing the Security Controls and Privacy Controls in Federal Information Systems and Organizations	Jan 2022
NIST SP 800-53 Rev. 5	Security and Privacy Controls for Information Systems and Organizations	10 Dec 2020
NIST SP 800-60 Vol 1	Guide for Mapping Types of Information and Information Systems to Security Categories	Aug 2008
NIST SP 800-60 Vol 2	Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices	31 Jan 2024
NIST SP 800-61	National Institute of Standards and Technology (NIST) Special Publication (SP) Computer Security Incident Handling Guide	06 Aug 2012
NIST SP 800-70	National Checklist Program for IT Products Guidelines for Checklist Users and Developers	Feb 2018
NIST SP 800-128	Guide for Security-Focused Configuration Management of Information Systems	Aug 2011
NIST SP 800-137	Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations	Sep 2020
NIST SP 800-160 Rev1	Systems Security Engineering	09 Dec 2021
NIST SP 800-171	Contract Self-Assessment against Basic National Institute of Standard Technology	Nov 2023
DISA eMASS User Guide -Version 1.1	US Army NETCOM Enterprise Mission Assurance Support Service (eMASS) Access and Administration Operational Tactics, Techniques and Procedures	18 Dec 2019
DISA eMASS User Guide -Version 1.1	US Army NETCOM Enterprise Mission Assurance Support Service (eMASS) Assets Module Operational Tactics, Techniques and Procedures (TTP)	18 Dec 2019

1.5.5 Availability of Government Documents, Drawings and Publications

1. Army Regulations (ARs), Field Manuals (FMs) and Technical Manuals (TMs) are available at: https://armypubs.army.mil/
2. Department of Defense (DoD) publications are available at: https://www.esd.whs.mil/DD/DoD-Issuances

3. Department of Defense (DoD) standards are available at: https://quicksearch.dla.mil/
4. Department of Defense (DoD) directives are available at: http://www.esd.whs.mil/Directives/issuances/dodd/
5. Military Standards are available at: https://quicksearch.dla.mil/
6. Live Training Transformation (LT2) Operations Guide Version CC, 24 April 2024, Document No. LT2-TRADE-PLN-000384. Available at: https://www.lt2portal.mil/DesktopModules/Cpe.FileServe/api/ServeFile/LT2_L1/LT2OperationsGuide/Default.htm
7. Industry Standards: American National Standards Institute (ANSI) Webstore: http://webstore.ansi.org/
8. Chief Information Officer – DoD Cyber Workforce DoD Cyber Workforce (defense.gov)

1.6 Order of Precedence

In the event of a conflict between the text of this PWS and the references cited herein, the text of the PWS shall take precedence. The Contractor shall notify the Government of any conflict so they may address the discrepancy. Nothing in this PWS, however, supersedes applicable laws and regulations.

1.7 Acronyms

Acronym	Meaning
AAR	After Action Review
ACA	Associate Contractor Agreements
APM	Assistant Program Manager
ASSIST	Acquisition Streamlining and Standardization Information System
ATO	Authority to Operate
CAC	Common Access Card
CBT	Computer-Based Training
CDRL	Contractual Data Requirements List
CHESS	Computer Hardware, Enterprise Software Solutions
CIS	Core Instrumentation System
CLIN	Contract Line-Item Number
CM	Configuration Management
CMRA	Contractor Manpower Reporting Application
COR	Contracting Officers Representative
COTS	Commercial-Off-the-Shelf
CTR	Continuous Technology Refreshment
CUI	Controlled Unclassified Information
CWBS	Contract Work Breakdown Structure
DFARS	Defense Federal Acquisition Regulation Supplement

DID	Data Item Description
DISA	Defense Information Systems Agency
DMSMS	Diminishing Manufacturing Sources and Material Shortages
DoD	Department of Defense
DODD	Department of Defense Directive
DODI	Department of Defense Instruction
DODM	Department of Defense Manual
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FAR	Federal Acquisition Regulation
FRACAS	Failure Reporting and Corrective Action System
FTE	Full Time Equivalents
FY	Fiscal Year
GAT	Government Acceptance Test
GFE	Government Furnished Equipment
GFI	Government Furnished Information
HQDA	Headquarters Department of the Army
IA	Information Assurance
IAVA	Information Assurance Vulnerability Alert
IAW	In Accordance With
IDIQ	Indefinite Delivery Indefinite Quality
IOC	Initial Operational Capability
IPMR	Integrated Program Management Report
IT	Information Technology
IUID	Item Unique Identification
LAN	Local Area Network
LCCS	Life Cycle Contractor Support
LRU	Line Replaceable Units
LT2	Live Training Transformation
LVC-IA	Live, Virtual and Constructive-Integrated Architecture
Man-P	Manufacturer’s Part Number
MIL-STD	Military Standard
NACI	National Agency Check with Inquiries
NDI	Non-Development Item
NET	New Equipment Training
NETCOM	Network Enterprise Technology Command
NSC	Network Security Component

OEM	Original Equipment Manufacturer
OIS	Objective Instrumentation System
OM	Operator's Manuals
OPSEC	Operations Security
PAC	Post Award Conference
PMR	Program Management Review
POA&M	Plan of Action and Milestones
PBO	Property Book Officer
PCO	Program Contracting Officer
QASP	Quality Assurance Surveillance Plan
RFP	Request for Proposal
RMF	Risk Management Framework
SMM	System Maintenance Manuals
SOC	Security Operations Center
SOW	Statement of Work
STIG	Security Technical Implementation Guide
SVR	System Verification Review
SW	Software
T&E	Test and Evaluation
TADSS	Training Aids, Devices, Simulations and Simulators
TDP	Technical Data Package
TDPI	Technical Data Package Index
TM	Technical Manuals
TRL	Technology Readiness Level
WBS	Work Breakdown Structure

2 General Requirements

2.1 Non-Personal Services

The Government shall not supervise Contractor employees nor control the method by which the Contractor performs the required tasks. Under no circumstances will the Government assign tasks to, or prepare work schedules for, individual Contractor employees. It shall be the responsibility of the Contractor to manage its employees and to guard against any actions that are of the nature of personal services or give the perception of personal services. If the Contractor believes that any actions constitute, or are perceived to constitute personal services, it shall be the Contractor's responsibility to notify the PCO immediately.

2.2 Location, Period of Performance, and Hours of Work

2.2.1 Place of Performance

Contractor shall perform requirements of this PWS at the following locations:

1. Fort Benning, GA
2. West Point, NY
3. Fort Rucker, AL
4. Fort Sill, OK
5. Yuma Proving Ground, AZ
6. Fort Campbell, KY
7. Fort Bragg/ Camp Mackall, NC

2.2.2 Period of Performance (PoP)

Period of Performance (PoP) for this effort is 12 months.

2.2.3 Hours of Work

Contractor shall maintain an adequate workforce for the uninterrupted performance of all tasks defined within this PWS. The Contractor is responsible for conducting business, between the hours of 0900 and 1700 Monday thru Friday except Federal holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government directed facility closings.

A "normal work week" in this situation is defined as one not exceeding the norm for the area, as determined by labor law and which compensation for exceeding 40 weekly hours is not paid at a premium rate. Any work requirements in addition to the normal work week shall be authorized in advance, in writing, by the cognizant Government PCO.

2.2.4 Recognized Holidays

Contractor is normally not required to perform services on recognized U. S. federally recognized holidays occurring during normal workweek hours unless otherwise directed by the APM or Contracting Officer Representative (COR). Concessions are made for religious holidays, at the discretion of the Government, when it does not interfere with operations. When a U.S. holiday occurs on a Saturday or a Sunday, the holiday is observed on the preceding Friday or following Monday, respectively.

1. New Year’s Day
2. M. L. King Memorial Day
3. Presidents Day
4. Memorial Day
5. Juneteenth
6. Independence Day
7. Labor Day
8. Columbus Day
9. Veteran’s Day
10. Thanksgiving Day
11. Christmas Day

2.3 Personnel

Contractor shall maintain the effectiveness of their employees by providing initial and refresher training as required to meet the PWS requirements. Contractor shall provide appropriate

administrative support for employees to perform their function(s) in the tasked environment, to include emergency situations.

2.3.1 Contractor Personnel, Disciplines, and Specialties

Contractor shall provide necessary resources and infrastructure to manage, perform, and administer the contract. Contractor shall ensure that all personnel meet the minimum qualifications/skills outlined in the PWS with respect to education, training and experience. Contractor shall provide the labor categories, labor rates, and man hours utilized in the performance of these requirements and shall ensure that the resources are the minimum necessary to accomplish the task.

2.3.2 Personnel Conduct

Contractor shall ensure that employees always conduct themselves in an ethical and professional manner while performing under this effort. Contractor shall take every action possible to ensure that its employees do not engage in activities that may embarrass or cause harm to the Government, and/or the Government of the applicable partner nation(s) within which its personnel may be operating. If a Contractor or subcontractor employee is removed from the job site or dismissed from the premises, the Contractor shall provide sufficient personnel to satisfy the requirement as required by the PWS. Unless otherwise specified, the Contractor shall replace removed/dismissed personnel within ten (10) calendar days as to not negatively impact performance. The Government shall not be liable for costs to relocate employees removed for misconduct or performance failures.

Personnel being replaced shall immediately be removed from the performance environment, placed in an administrative status, and returned to the U.S. as expeditiously as possible unless they have been placed on some type of legal International Hold status.

2.4 Program Management and Administration

Contractor shall delineate program management and administrative efforts to ensure the effective and efficient execution of all SMS related tasks. Contractor shall establish clear organizational lines of authority and responsibility at the execution levels, as required, to ensure effective management of the resources assigned to the requirement(s). Furthermore, the Contractor shall immediately notify the Government Assistant Program Manager (APM) and/or Technical Government Representative of any issues or concerns that arise via email (john.d.lindsey16.civ@army.mil) arise.

(CDRL #) DI-MGMT-81928 Contractor's Progress and Status Report

2.4.1 Program Meetings and Reviews

2.4.1.1 Integrated Product Team (IPT) Meetings

Contractor shall host and participate in weekly Integrated Product Team (IPT) meetings and address the full spectrum of the program status including system engineering, schedule, financial, integrated logistics support, and testing. The Government and Contractor may schedule or cancel a scheduled IPT meeting as deemed necessary. Telephone conferences and video teleconferencing may be utilized for IPT meetings. The Contractor shall provide an email

summary to the Government of the meeting minutes, action items, and track resolutions for each item until closure within 24-hours.

2.4.1.2 Program Management Review (PMR)

Contractor shall conduct biannual Program Management Reviews (PMR) in accordance with (IAW) a jointly agreed upon schedule and location. The PMR shall provide a program overview regarding the issues, status and planned activities of the program.

Contractor shall coordinate and obtain Government concurrence of PMR topics at least two weeks prior to the PMR. Additionally, the Contractor shall provide a read ahead to Government at least one week prior. The slides shall contain an action item log to capture programmatic actions and assign a point of contact (POC) that shall report to the Government APM or Contracting Officer Representative (COR).

(CDRL #) DI-ADMN-81505 Report, Record of Meeting/Minutes – PAC

2.4.2 Contract Management

Contractor shall establish processes and assign appropriate resources to effectively administer PWS requirements. The Contractor shall create, and review functions required to fulfill the requirements of the PWS at the Prime and subcontractor levels. The Contractor shall manage the timeliness, completeness, and quality of problem identification. The Government shall not supervise nor control the contract service personnel providers performing the services herein. Personnel shall be accountable solely to the Contractor who, in turn is responsible to the Government.

Contractor shall provide expedient responses to Government requests for contractual actions consistent with customer and/or PWS priorities as they occur. The Contractor shall assign a point of contact between the Government and Contractor personnel assigned to support PWS efforts. The Contractor shall maintain proper and accurate time keeping records of personnel assigned to support individual PWS requirements. The Contractor shall maintain consistent communication with and provide timely response to the cognizant COR/Alternate COR (ACOR) inquiries.

Contractor shall maintain the capability to implement an Associate Contractor Agreement (ACA) with any subcontractors for exchanging software data, accessing, and using third party software and equipment, receiving technical support, working interface issues, transitioning to Life Cycle Contractor Support (LCCS) and/or agreeing on equipment use and time. All ACAs shall be communicated to the Government before establishment.

2.4.2.1 Integrated Master Schedule (IMS)

Contractor shall develop, manage, update, and maintain an Integrated Master Schedule (IMS) to include tasks required to execute all work requirements defined herein. All contract schedule information delivered or presented at program meetings and or reviews shall originate from the IMS and shall include program milestones, accomplishments, predecessor and successor events and their dependencies, meetings, conferences, reviews, and deliveries as of contract inception. The Contractor shall conduct a critical path analysis to estimate each task duration, and to determine the amount of schedule flexibility prior to technical and project reviews, as requested by the Government.

(CDRL #) DI-MGMT-81861C Integrated Program Management Data and Analysis Report (IPMDAR) – Integrated Master Schedule

2.4.2.2 Contract Manpower Reporting Application (CMRA)

Contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services under this contract via a secure data collection site. The Contractor is required to completely fill in all required data fields using the following web address: http://www.ecmra.mil/. Reporting inputs shall be for labor executed during the period of performance during each Government Fiscal Year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year. Contractors can find User Guides, Frequently Asked Questions and may direct questions to the help desk at http://www.ecmra.mil/.

2.4.2.3 Financial Management

The Contractor shall plan, budget, schedule, and control all financial resources allocated to meet the requirements of this PWS within the funding limitations set forth under the individual Contract Line-Item Number (CLIN)/Purchase Order (PO)/Military Interdepartmental Purchase Request (MIPR).

(CDRL #) DI-MGMT-81468A Contract Funds Status Report (CFSR)

2.5 Live Training Transformation (LT2) Product Line Support and Synchronization

Contractor shall participate in Live Training Transformation (LT2) technical and management level working groups as defined in this PWS. The Contractor shall support all collaboration efforts that align with the LT2 strategy to include at a minimum,

1. Participation in the Core Asset Working Group (CAWG) meetings.
2. Completion and submission of Core Asset Change Proposals (CACP) for new and revised components, to inform the community of the work being performed.

2.5.1 Synchronization with LT2 Configuration Management Baseline (CMB)

The Contractor shall synchronize their efforts with the LT2 Lifecycle Configuration Management Baseline (CMB) for all CTIS systems. The Contractor shall,

1. Update the CMB Import File Template (See Appendix A) content before effort completion.
2. Transfer the Technical Data Package (TDP) to the Lifecycle Contractor via the LT2 Product Data Management Infrastructure.

(CDRL #) DI-MISC-80711A Scientific and Technical Reports – Configuration Management Baseline (CMB)

2.6 Data Rights

Contractor shall disclose data items that are provided to support SMS as part of their proposal.

2.7 Incident Reporting

The Contractor shall promptly report pertinent facts regarding incidents involving Government property damage, personnel misconduct, or injury to personnel and to cooperate in any resulting safety and/or security investigations. The Contractor shall adhere to the following Incident Levels (IL), based on severity, when determining specific incident reporting protocols. These reporting requirements should not be perceived to take precedence over an individual's personal assessment with regards to his or her own health and well-being. The Contractor shall prepare an Accident/Incident Report IAW the CDRL.

MINOR INCIDENTS: The Contractor shall report pertinent facts regarding the incidents involving minor equipment/property damage, and/or personnel misconduct, and/or injury within forty-eight (48) hours of the initial discovery. The Contractor shall notify the appropriate Government Point(s) of Contact (POCs) (i.e. TO COR) via telephonic or electronic (email) means. For this IL, minor property damage is defined as damage that does not pose any risk of non-performance of the requirement(s) for which it was intended and poses no risk of bodily injury to any person(s) operating in and around it. For this IL, minor injury is defined as superficial; including but not limited to minor cuts, bruises or muscle strains.

MODERATE INCIDENTS: The Contractor shall report pertinent facts regarding incidents involving moderate equipment/personnel misconduct/property damage or injury within twenty-four (24) hours of the initial discovery. The Contractor shall notify the appropriate Government Point(s) of Contact (POCs) (i.e. cognizant PCO, local authorities and COR, where applicable, telephonically). A voice mail message left telephonically is not acceptable to meet this requirement. Within 40 hours of the initial verbal report, the Contractor shall submit an Accident/Incident Report IAW the CDRL to the PCO and the TO COR. For this IL, moderate equipment/property damage is defined as damage that causes a diminished training capability and poses some risk of non-performance of the requirement(s) for which it was intended and/or poses some risk of bodily injury to any person(s) operating in and around it. For this IL, moderate injury is defined as injuries that temporarily incapacitate an individual (to include but not limited to, twisted ankles and concussion) but which does not pose any significant hindrance to the Individuals' performance of the requirement(s).

MAJOR INCIDENTS: The Contractor shall report pertinent facts regarding incidents involving major equipment/property damage, and or major personnel misconduct, and/or major injury or fatality immediately upon initial discovery in person or telephonically, to the appropriate Government Point(s) of Contact (POCs) (i.e. cognizant PCO, Program Director, local authorities). A voice mail message left telephonically is not acceptable to meet this requirement. The Contractor shall also IMMEDIATELY secure the site to ensure the preservation of evidence and cooperate in any resulting safety and/or security investigations. Within twenty (24) hours of the initial verbal report, the Contractor shall submit an Accident/Incident Report IAW the CDRL to the PCO and TO COR. For this IL, major equipment/property damage is defined as damage that ceases, severely diminishes the training capability and/or poses a serious risk of bodily injury to any person(s) operating in and around it. For this IL, major injury is defined as any injury/illness that completely incapacitates an individual, to include but not limited to bone breaks, loss of limb(s).

After an incident, the Contractor shall take appropriate steps to correct the situation and inform the Government of the corrective action taken.

(CDRL #) DI-SAFT-81563 Accident/Incident Report

2.8 Counterfeit Risk Management (CRM) Program

Contractor shall implement a Counterfeit Risk Management (CRM) Program, IAW AR 702-20, Counterfeit Risk Management Product Assurance, to address counterfeit parts and materiel management of the supply chain. The Contractor shall ensure the CRM program meets all counterfeit prevention measures listed in DoDI 4140.67. The Contractor shall use new and authentic materiel, commodities, items, assemblies, subassemblies, and components. The Contractor shall purchase materiel directly from original equipment/component manufacturers, manufacturer authorized/franchised distributors, or authorized aftermarket manufacturers. The Contractor shall, at the time of each individual Supplier quotation to a Seller, shall obtain from Seller: (i) the company name and location of the source of supply, and (ii) a representation that Seller is authorized to sell the materiel. The Contractor shall have access to the Government-Industry Data Exchange Program (GIDEP) for both counterfeit prevention and counterfeit notification.

2.8.1 Reporting Counterfeit or Suspected Counterfeit parts.

Contractor shall report all counterfeit or suspected counterfeit parts to the PCO within 5 days and GIDEP NLT 60 days of making that determination. In reporting this to the PCO, the Contractor shall also address the impact of this determination on current contract requirements.

2.9 Contractor Training Requirements

2.9.1 Antiterrorism Threat (AT) Level 1 Training

AT Level I Training is required for Contractor employees performing work within an Army-controlled installation, facility, or area. All Contractor employees, including subcontractor employees, requiring access to Army installations, facilities, or controlled access areas shall complete AT Level I awareness training within 30 calendar days after contract start date or effective date of incorporation of this requirement into the contract, whichever applies. The Contractor shall maintain and 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 10 days after completion of training. AT Level I awareness training is available at https://jko.jten.mil.

2.9.2 Access and General protection/Security Policy and Procedures

Contractor and all associated subcontractor 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 (FPCON) at any individual facility or installation change, the Government may require changes in contractor security matters or processes.

2.9.3 For Contractors requiring Common Access Card (CAC)

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 IAW Army Directive 2014-05, Policy and Implementation Procedures for Common Access Card Credentialing and Installation Access for Uncleared Contractors. The Contractor employee shall 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 six (6) months or more. At the discretion of the sponsoring activity, an initial CAC may be issued based on a favorable review of the Federal Bureau of Investigation (FBI) fingerprint check and a successfully scheduled NACI at the Office of Personnel Management.

2.9.4 For Contractors that do not require a CAC, but require Access to DoD Facility or Installation

Contractors and all associated sub-contractors employees shall comply with adjudication standards and procedures using the National Crime Information Center Interstate Identification Index (NCIC-III) and Terrorist Screening Database (Army Directive 2014-05/AR 190-13), applicable installation, facility and area commander installation/facility access and local security policies and procedures (provided by Government representative); or, at OCONUS locations, in accordance with status of forces agreements and other theater regulations.

2.9.5 iWATCH Training

Contractor and all associated subcontractors shall brief all employees on the local iWATCH Army program (training standards provided by the requiring activity ATO). 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 30 calendar days of new employees commencing performance with the results reported to the COR upon request from the Government.

2.9.6 Army Training Certification Tracking System (ATCTS) Registration

All Contractor employees with access to a Government Information Systems (IS) must be registered in the ATCTS at commencement of services and must successfully complete the DoD Information Assurance Awareness Training prior to access to the IS and then annually thereafter.

2.9.7 Operational Security (OPSEC) Program

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 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. The Contractor shall implement OPSEC measures as ordered by the Government. In addition, the Contractor shall have an identified certified Level II OPSEC coordinator per AR 530-1.

Program OPSEC plans shall be coordinated with and approved by the identified Government representative, as specified in the Contractor Data Requirements List (CDRL). Program

protection measures shall be applied and approved by this individual at all locations where CI is developed, produced, analyzed, maintained, transported, stored, tested, or used in training.

2.9.8 OPSEC Training Requirement

Per AR 530-1, Operations Security, the Contractor employees shall complete Level I OPSEC Awareness training. New employees must be trained within 30 calendar days of their reporting for duty and annually thereafter and the results reported to the COR upon request by the Government.

2.9.9 Information Assurance (IA)/Information Technology (IT) Training

All contractor employees and associated subcontractor employees shall complete the DoD IA awareness training before issuance of network access and annually thereafter. All contractor employees working in IA/IT functions shall comply with DoD and Army training requirements in DoDD 8140.01, DoD 8570.01-M and AR 25-2 within six (6) months of appointment to IA/IT functions.

2.9.10 Information Assurance (IA)/Information Technology (IT) Certification

Per DoD 8570.01-M, Defense Federal Acquisition Regulation Supplement (DFARS) 252.239.700, Information Assurance Contractor Training and Certification, and AR 25-2, the contractor employees supporting IA/IT functions shall be appropriately certified upon contract award. The baseline certification as stipulated in DoD 8570.01-M shall be completed upon delivery order award.

2.9.11 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 (CFR Title 32 Part 117) and (2) any revisions to DOD 5220.22-M, notice of which has been furnished to the Contractor.

2.9.12 Controlled Unclassified Information (CUI) Training

Include DFARS clause 252.204-7012, which requires the contractor to comply with NIST 800-171. Also include DFARS provision 252.204-2019 into solicitations. Acquisition officials should follow procedures outlined in DFARS 204.73 and verify vendors have an adequate NIST SP 800-171 summary assessment score within the Supplier Performance Risk System (within PIEE). If the score doesn't show a medium- or high-level assessment with a score of 110 or better (as described in the "NIST SP 800-171 DoD Assessment Methodology"), include clause 252.204-7020 and obtain the vendor's "system security plan" and "plan of action" for NIST SP 800-171 verification and assurance by Army security officials.

2.9.13 Threat Awareness Reporting Program (TARP)

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 (CI) agent or other trainer as specified in AR381-12, paragraphs 2-4b.

2.10 Organizational Conflict of Interest (OCI)

Contractor and subcontractor personnel performing work under this PWS may receive, have access to or participate in the development of proprietary or source selection information (e.g., cost or pricing information, budget information or analyses, specifications, or work statements, etc.) or perform evaluation services which may create a current or subsequent OCI as defined in FAR 9.9-5, Organizational and Consultant Conflicts of Interest. The Contractor shall notify the PCO immediately whenever it becomes aware that such access or participation may result in any actual or potential OCI and shall promptly submit a plan to the PCO to avoid or mitigate any such OCI. The Contractor's OCI mitigation plan will be determined to be acceptable solely at the discretion of the PCO. In the event the PCO unilaterally determines that any such OCI cannot be satisfactorily avoided or mitigated, the PCO may affect other remedies as he or she deems necessary, including prohibiting the Contractor from participation in subsequent contracted requirements which may be affected by the OCI.

2.11 Government Directed Travel / Temporary Duty

This PWS shall require Contractor personnel to travel to, from and within the Continental US (CONUS) and/or Outside the Continental US (OCONUS) locations as specified herein.) The Contractor may be authorized travel expenses at rates no higher than the substantive provisions of the Joint Travel Regulation (JTR), IAW FAR Part 31.205-46, and the limitation of funds specified in this contract. All travel requires Government approval and authorization by the APM or COR prior to schedule travel. The Contractor shall be responsible for coordinating all travel arrangements to, from, and in-and-about all CONUS and/or OCONUS Points of Destination. Airfare costs shall be the lowest priced airfare available to the contractor during normal business hours. Airfare costs more than the above standard airfare are unallowable except as authorized under FAR 31.205-46(b).

Additionally, non-program management office travel shall be conducted and invoiced IAW FAR 31.205-46 Travel Costs and the JTR. All program management travel not specifically directed by the Government shall be funded by the contractor as part of their program management pricing via indirect rates or within the contractor's competitive pricing. Routine program management travel shall not be funded by any travel CLIN.

2.12 Cybersecurity

2.12.1 Security Engineering

Contractor shall incorporate secure engineering principles IAW NIST SP 800-160 Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. The basis for this is to establish a multidisciplinary security and specialty approach to engineering, resulting in sustainably trustworthy secure systems throughout the system life cycle. Contractor shall address security issues from a stakeholder protection needs, concerns, and requirements perspective and to use established engineering processes to validate that such needs, concerns, and requirements are addressed with appropriate fidelity and rigor. Contractor shall test, verify, and document that the security architecture of the system complies with the security requirements as identified in the ATO and System Security Plan (SSP). Contractor shall use DoD approved assessment tools to implement control solutions on the system prior to deployment to assess the Security Controls and provide relevant artifacts upon completion.

2.12.2 Cybersecurity (FedRAMP)

Contractor shall leverage PM TRADE/PdM CTIS Cybersecurity processes and procedures to the maximum extent possible to validate a common approach across all SMS instantiations. The Contractor shall provide a detailed plan to achieve a Cybersecurity FedRAMP Moderate ATO.

SMS includes Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS)/Platform-as-a-Service (PaaS) support. This effort includes required services to ensure SMS capability is maintained.

2.12.2.1 SaaS SMS

1. Web Application for user management, organization management, training event management, training event after action report, real time tracking of SWDs, SWD communication for SOS acknowledgement/deactivation, user manual.
2. SWD Management System for configuring and maintaining SWDs. Provides management of firmware updates, real time configuration of SWDs, and interface from the Web Application to SWD Communications System.
3. SWD Communications System for handling secured communications from the SWD to the cloud. Implements configurations done by the SWD Management System and applies them to SWDs. Forwards positioning and SOS information to Web Application.

2.12.2.2 PaaS SMS

1. Network Load Balancer
2. Application Load Balancer
3. Web Application Firewall
4. Network Firewall
5. Container Registry
6. Container Engine
7. Database Servers
8. Secure Storage
9. DNSSEC

2.12.2.3 IaaS SMS

1. Server infrastructure required to run SMS
2. Secure Backups

2.12.3 Cybersecurity Tasks

Contractor shall incorporate secure engineering principles IAW NIST SP 800-160 Systems Security Engineering. The basis for this is to establish a multidisciplinary security and specialty approach to engineering, resulting in sustainably trustworthy secure systems throughout the system life cycle.

2.12.4 Cybersecurity Compliance

Contractor shall test, verify, and document that the security architecture of the system is IAW the security requirements as identified in the system specification and/or as defined in the existing RMF package according to system categorization, overlays, and control selection. Contractor

shall use DoD approved assessment tools to implement control solutions on the system prior to the Governments performance to assess the Security Controls.

2.13 Safety Assessment

Contractor shall conduct safety analysis and identify classification hazards as an integral part of the system design effort. Contractor shall develop a hazard risk index including hazard severity and hazard probability levels for all hazards. Contractor shall document information about each hazard. 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 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.

2.13.1 Hazard Tracking and Risk Resolution

Contractor shall implement and maintain a safety process to analyze, identify, evaluate, eliminate, control, and track each hazard until final resolution is reached throughout the term of this SOW. The Contractor shall notify the APM or Government representative of any safety features and controls incorporated into the design to eliminate hazards or reduce their associated risks to levels acceptable to the Government. The Contractor shall include an evaluation of the system during performance as well as the safety impacts due to inadvertent functioning or functional failure. Subsystems that the system shall interface with shall be evaluated to ensure hazards and risks are avoided. The Contractor shall obtain Government approval of the final hazard resolution.

(CDRL #) DI-SAFT-80101C System Safety Hazard Analysis Report (SSHAR)

2.14 Program Specific Requirements

The Contractor shall perform to the standards identified in this PWS and associated contract documents as follows,

1. Contractor shall meet or exceed all specified requirements contained in the SMS CDD dated 19 March 2019.
2. Contractor's solution shall provide adequate coverage, ensuring there are no "dead zones" in the training areas. In addition, the contractor shall,
   a. Conduct wave propagation analysis as necessary to ensure coverage objectives are met.
   b. Provide repeaters as necessary to ensure coverage objectives are met.
3. Contractor shall comply with all applicable security and cyber policies and regulations.

4. Contractor shall ensure Soldier monitoring is continuous, depicting locations on a user-friendly map interface enabling cadre and leadership to easily track each Soldier's location.
    a. System will provide automated alerts to the MS and MMD when it detects "no-motion" from an SWD.
    b. SWD will be tamper proof and prevent users from powering down the device.
    c. System will be capable of providing geo-fences with automated alerts when Soldier crosses boundaries or enters restricted areas.
5. Contractor shall ensure SMS provides After Action Reviews (AAR)s.
    a. AARs will depict Soldier routes "bread crumb trails" including Soldier speeds, climb/decent, and distance.
    b. AARs will be capable of displaying multiple routes at the same time.
6. Contractor shall provide services required to maintain SMS technology and ensure performance objectives are achieved, and SMS capability maintained. Services include providing:
    a. Training and training materials.
    b. Inventory and installations as required.
    c. Repair/replace damaged or inoperable components.
    d. Field service and maintenance support.
    e. Help desk support.
    f. Wave propagation studies for all SMS 2 radio bands (as required).
    g. Support monthly and weekly meetings as required.
7. Contractor shall provide monthly reports on the achievement of SMS Reliability Availability and Maintainability (RAM) requirements of Ao 95%.
    a. Contractor shall provide repair/replacement of inoperative devices within five (5) working days of identification.
    b. Contractor shall conduct two (2) field service/remedial training site visits per year, per site.
    c. Contractor shall provide monthly maintenance status reports.
    d. Breakout of damaged/inoperable devices and components.
    e. Breakout of faults and actions taken.
    f. Breakout of maintenance logistics with the following dates: customer shipped, item received, items repaired/replaced, item shipped, item received by customer.
    g. Itemized totals for all maintenance actions.
    h. Analysis of maintenance problem areas (recurring issues).
8. SMS Help Desk
    a. Contractor shall provide email and telephonic technical support to SMS site operators.

3 Performance Requirements

Government will evaluate the Contractor's performance under this PWS in accordance with (IAW) Task Statements, Standards (STDs), Acceptable Quality Levels (AQLs), Method of Surveillance, and Performance Incentive as described in the Performance Requirements Summary matrix set forth in Appendix B. Additionally, the Quality Assurance Surveillance Plan (QASP) shall be used to assess contractor performance by identify what is going to be inspected, the inspection process, and who will do the inspection. Performance Standards are representative of a Satisfactory rating within the Government QASP. The Acceptable Quality Levels (AQLs) for selected Performance Standards are not all-inclusive and are subject to modification as required or directed by the Government. The QASP defines how the performance standards will be applied, the frequency of surveillance, and the acceptable quality levels (performance thresholds).

Contractor will be notified in writing of the Government's determination of its performance level for each performance objective, including all instances where the contractor failed to meet the acceptable quality level. Government will conduct informal interim counseling sessions with the contractor's Program/Task Order (TO) Manager to identify any active TO performance that is not meeting the acceptable quality levels. These sessions will be conducted at least quarterly to provide the Contractor a fair opportunity to improve its performance level.

3.1 Specific Tasks

This PWS incorporates the following High-Level Objectives (HLOs): 1) Contractor Resources Management 2) Contractor Project Management; 3) Contractor Training Management; 4) Contractor Engineering Management and 5) Efficient and Effective Control of Labor Resources. It is the Contractor's responsibility to employ the necessary resources to ensure accomplishment of all performance objectives stated herein.

3.1.1 Contractor Training Management

Contractor shall provide and manage all required training and training assistance for New Equipment Training (NET), Operator, and Maintenance Training.

1. Contractor shall plan, prepare, conduct, and document NET, Operator and Maintenance Training using established systems operation guidelines, safety processes and plans.
    a. AQL: NET training provided with only minor (less than 15%) corrective actions and only minor Government intervention required.
    b. AQL: Operator training provided with only minor (less than 15%) corrective actions and only minor Government intervention required.
    c. AQL: Maintenance training provided with only minor (less than 15%) corrective actions and only minor Government intervention required.
2. Contractor shall propose, and the Government shall approve the days for training. The Contractor shall conduct the training courses on location at the Government site where the system is to be installed or at another mutually agreed location and collect a roster of trained personnel.
    a. AQL: Training calendar IAW IMS.
    b. AQL: Roster of trained personnel collected and analyzed for each type of training

provided.

3. Contractor shall provide qualified instructors and Subject Matter Experts (SMEs) for training management.
    a. AQL: Instructor qualification and certification documentation provided by the proponent upon request.
4. Contractor shall analyze and prepare all training materiel to accommodate training environments and class sizes.
    a. AQL: Technically supportable using the current and/or mandated software/system, i.e. Microsoft Office products, etc. and delivery materials appropriate for the training environment and class size.
    b. AQL: Technically supportable materials (hardware, software, TADSS, tools, etc.) provided with sufficient support to permit execution of PWS requirements.
    c. AQL: Instruction content is suitable for intended student population, knowledge, skill level and training objectives in all modes of operation.

(CDRL #) DI-ILSS-80872 Training Materials

3.1.2 Contractor Logistics and Supportability Management

1. Contractor shall provide Return Merchandise Authorization (RMA) for shipping of faulty or damaged SMS components to a repair center.
    a. Contractor shall have a shipping account with a logistics vendor to expeditiously (less than 5 business days) process repair items. Contractor shall provide shipping labels to SMS sites once authorized by the Government.
    b. Contractor shall maintain and provide logistics tracking of all equipment returned from the repair center by serial number, to include description of work completed on each device and required replacement parts.
    c. Contractor shall report logistics tracking quarterly to ACOR of all equipment repaired by serial number, to include description of work completed on each device and all required replacement parts.
    d. Contractor shall maintain and provide upon request a detailed inventory list of all SMS components, to include location and status.

4 Appendix A – Configuration Management Baseline (CMB) Import File

The CMB CDRL is a template for importing data into the LT2 Product Data Management (PDM) Infrastructure.

CMB CDRL Template.xlsx

5 Appendix B – Performance Requirements Summary

PERFORMANCE OBJECTIVE	PERFORMANCE STANDARD	ACCEPTABLE QUALITY LEVEL (AQL)	METHOD OF SURVEILLANCE	PERFORMANCE INCENTIVE
High Quality Technical Performance	**TO requirements met with little rework/re-performance required and with few minor and no significant problems encountered** *Performance meets all technical and functional requirements, and is highly responsive to changes in technical direction and/or the technical support environment* *Assessments, evaluations, analyses, recommendations, and related input are thorough, reliable, highly relevant to TO requirements, and consist of substantial depth and breadth of subject matter* *Deliverable reports contain all required data and meet all applicable CDRL requirements*.	**Contractor delivery of products and/or services meets all TO requirements. Performance occurs with no required** **re-performance/ rework at least 80% of time.** **Problems that are encountered are minor and resolved in a satisfactory manner.**	**Routine Inspection of Deliverable Products/Services**	**Assignment of performance rating for QUALITY criteria:** *EXCEPTIONAL:* *Performance and deliverables meet all and exceed many TO requirements. Performance delivered with no required re-performance/rework at least 95% of time; problems that are encountered are minor and resolved in a highly effective manner.* *VERY GOOD:* *Performance and deliverables meet all and exceed some TO requirements. Performance delivered with no required re-performance/rework at least 90% of time; problems that are encountered are minor and resolved in an effective manner.* *SATISFACTORY:* *Performance and deliverables meet all TO requirements. Performance delivered with no re-performance/rework at least 80% of time; problems that are*

				encountered are minor and resolved in a satisfactory manner. *<u>MARGINAL:</u>* *Some TO requirements not met and/or performance delivered with re-performance/rework required more than 20% of time. Problems encountered were resolved in a less than satisfactory manner.* *<u>UNSATISFACTORY:</u>* *Many TO requirements not met. Numerous re-performances/rework required. Substantial problems were encountered, and inadequate corrective actions employed.*