PMW-160.I Installation Resource Management
Support Services Performance Work Statement

PMW 160 Installation Management Support of C4ISR Installations

2 May 2007

1.0 INTRODUCTION

The PMW-160.I Installation Resource Manager (IRM) provides direction and execution for all PMW-160 installation efforts, including providing Ship Maintenance (SHIPMAIN), Fleet Modernization Program (FMP) program policy and management of afloat and ashore Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) installation schedules. PMW-160.I is the single point of contact for all PMW-160 C4ISR installation efforts including planning, execution and validation.

2.0 BACKGROUND

Effective 02 August 2004, PEO C4I reorganized internally to provide a more capability-based infrastructure. This reorganization builds on the PEO C4I Roadmap and increases the ability to deliver solutions to new construction platforms. The PMW160 Program Manager is responsible for the acquisition, implementation, and integration efforts in support of the current and future programs that meet the PMW's mission.

PMW-160.I – PMW INSTALLATION RESOURCE MANAGEMENT (IRM)

Installation Resource Management ensures that Systems procured through the Navy Acquisition Process are installed so as the end user (most times, the Warfighter) is aware of the Capability being provided, have the training necessary for optimum usage, and is able to repair and maintain the system under design operational parameters. IRM tracks System Fielding, Funding, and Unit Availability to allow procured systems to be installed with the greatest amount of efficiency at the best cost, by coordinating efforts with the Assistant Program Managers, Installation Activities, Program Office Business Finance Managers, PEO, and Platform PMWs. PMW 160 IRM supports the following PMW 160 systems:

Automated Digital Network System (ADNS) provides routing, switching, baseband, configuration, and monitoring capabilities for interconnecting Naval, Coalition and Joint enclaves worldwide. ADNS utilizes Commercial Off the Shelf/ Government Off the Shelf (COTS/GOTS) equipment and network protocols as specified by the Joint Technical Architecture. ADNS Increment I provides initial limited, Ship to Shore Internet Protocol (IP) connectivity, separation of enclaves, reuse of unused enclave bandwidth, and Ship to tactical Shore IP connectivity. ADNS Increment II provides additional capabilities of Load Balancing, Radio Frequency (RF) restoral, Initial Quality of Service (QoS), Initial Traffic Management, increase data throughput, and has been demonstrated as part of the FORCEnet Integrated Product Demonstration (IPD). ADNS Increment IIA adds converged Voice, Video, and Data enhancements to ADNS INC II. ADNS Increment III will support Transformational Communications, Black Core Routing, and Joint Tactical Radio Systems (JTRS) compatibility with additional capabilities such as IPv6/IPv4 dual stack, and converged IP to Surface, Airborne and Submarines platforms.

The **Combined Enterprise Regional Information Exchange System** (CENTRIXS) provides Navy ships with a reliable, high-speed Local Area Network (LAN) that will provide access to the coalition (Four Eyes, Global Counter Terrorism Task Force (GCTF), CENTRIXS J and K, Multinational Coalition Force Iraq (MCFI) and all other bilateral Wide Area Network (WAN). It provides real-time information exchange between afloat units, Component Commanders, numbered Fleet Commanders and Commanders LANT/PAC Fleet. The CENTRIXS program maximizes the use of both Commercial Off the Shelf (COTS) software and hardware.

Computer Network Defense (CND) delivers tactical network information assurance protection with defense in depth security, proactive vulnerability risk management, and threat monitoring analysis.

Crypto Products provide central planning, procurement, and sustainment of Cryptographic Products throughout their Life Cycle in support of Department of the Navy (DoN) Communication Security (COMSEC) and Transmission Security (TRANSEC) Equipment.

The **Electronic Key Management System (EKMS)** provides for the ordering, generation, distribution, control, and accounting for all cryptographic material (electronic and hardcopy). Navy EKMS consist of Tier 2 sites (approx 700) with Local Management Device and Key Processor (LMD/KP) and Tier 3 elements with the Data Transfer Device (DTD) or AN/CYZ-10. The Tier 2 software and the KP are NSA/L-3 products. The Tier 2 LMD hardware is COTS. The Tier 3 software is a combination of NSA, SYPRIS, and SSC-SD products. The hardware is a SYPRIS product. Implementation is worldwide throughout DoN. Support to all communities includes training, technical support center assistance and CASREP on-site assistance.

The **KG-3X** is a joint interest acquisition effort for which USAF Electronic Systems Command (ESC) Nuclear Deterrence Minimum Essential Emergency Communication Network (MEECN) is the System Program Office (SPO) and Joint Interest Program Office (JIPO). The KG-3X Program will modernize existing KG-3X devices. The program covers the procurement, installation, and sustainment of KG-3X devices through NSA RDT&E and USN OPN/OMN expenditures, for Navy devices.

The **KG-40AR** is a two part (development and production) project to develop and procure a form, fit, function replenishment of the KG-40A (Link 11 encryptor) to meet fleet and coalition requirements until 2015. The KG-40/KG-40A cryptographic devices were developed and fielded in the 1970s and 1980s. These devices provide Communications Security (COMSEC) protection for the Link-11 system used in the Navy's Tactical Data Systems (NTDS), Tactical Data Information Link A (TADIL-A), and Army Patriot Missile data link.

Public Key Infrastructure (PKI) consists of the hardware, software, policies and procedures required to create, manage, store, distribute, and revoke X.509 certificates. Through strong certificate-based authentication, the PKI enhances the security of access to private military networks, web servers and applications. The PKI security services of strong authentication, data integrity, confidentiality, and non-repudiation support the Navy's Defense-in Depth strategy. This strategy includes the capability of sending and receiving secure official email and enabling secure electronic transactions.

Radiant Mercury (RM) provides an automated means to sanitize, downgrade, guard, and transliterate, where appropriate, formatted data at various classification and compartment levels. With the aide of a reliable human reviewer, RM can process nonstandard messages, such as messages with images or unformatted data. The Multi-Security Level (MSL) capability provided by RM is necessary to provide access to relevant information at the appropriate clearance, compartment(s) and/or releasability level across security enclaves while meeting the appropriate confidentiality, availability and integrity requirements. RM is one of several systems specifically designed to provide a MSL capability across all services to DOD information systems, and it is currently integrated in naval, land-based and airborne platforms.

The **Secure Voice** program, a component of the Navy Information Systems Security Program (ISSP), provides secure communication capabilities to the Navy, Marine Corps, Coast Guard and Military Sea Lift Command. The Secure Voice project provides operational and maintenance support to legacy strategic and tactical voice systems, procures and fields new secure voice systems (e.g., STE/FNBDT devices, inter-working functions and gateways) and develops future secure voice capabilities to ensure Navy's secure voice superiority.

Integrated Shipboard Network Systems (ISNS) provides Navy ships with reliable, high-speed SECRET and UNCLASSIFIED Local Area Networks (LANs). It supplies the network infrastructure (switches and drops to the PC), Basic Network Information Distribution Services (BNIDS), and access to the DISN Wide Area Network (WAN) (Secure and Non-secure Internet Protocol Router Network SIPRnet and NIPRnet) which are used by other hosted applications or systems such as NTCSS, GCCS-M, DMS, NSIPS, NMCP, NAVMPS, TBMCS and TTWCS. It enables real-time information exchange and network monitoring within the ship and between afloat units, Component Commanders, and Fleet Commanders and is a key factor in the implementation of the Navy’s portion of Joint Vision 2020. In FY07 and out, the development and integration of the Video Information Exchange System (VIXS) and the Shipboard Video Distribution System (SVDS) become subprograms within the ISNS program. ISNS Increment 2 is the next increment of ISNS capability developed to include wireless network support internal and external to the ship (Expanded Maritime Intercept Operations), disk to disk back up, and increased security.

Consolidated Afloat Networks and Enterprise Services (CANES) is the proposed next generation Afloat Network. CANES Increment 1 will be developed to provide future ISNS, CENTRIXS, SCI Networks, under a single program. SubLAN capabilities are also planned to be incorporated into the program after SubLAN 2 is fielded.

Common PC Operating System Environment (COMPOSE) is a streamlined software package based on a modular architecture that provides Basic Network Information Distribution Services (BNIDS) used by other program of record systems such as CENTRIXS, ISNS, SubLAN, and SCI networks. Essentially, COMPOSE establishes an operating system environment that provides basic network domain services (e.g., account management, domain name service, e-mail, web-based services), core office automation applications (e.g., word processing, spreadsheet, presentation), and security services (e.g., anti-virus).

Enterprise Services/Composeable FORCEnet (CFn) provides the common core enterprise services and service oriented architecture (SOA) to allow organizations ubiquitous access to reliable, decision-quality information through a net-based services infrastructure and applications to bridge real-time and near-real-time communities of interest (COI). The SOA will empower the edge user to pull information from any available source, with minimal latency, to support the mission. Its capabilities will allow DoN as well as GIG users to task, post, process, use, store, manage and protect information resources on demand for warfighters, policy makers and support personnel.

Personal Computer (PC) System is comprised of Commercial Off the Shelf (COTS) PCs (desktop and laptop computers) and client software for afloat UNCLASSIFIED and SECRET enclaves. PCs constitute the infrastructure to support robust C4ISR and Network-Centric Warfare capabilities such as command and control functions, intelligence gathering, email and chat communications, online training, image analysis, and maintenance and personnel functions for Sailors/Marines in the afloat environment. PCs are provided for amphibious ships, surface combatants, and aircraft carriers.

Sensitive Compartmented Information (SCI) Networks provides secure WAN IP access to ship and Shore National web sites and SIGINT and Intelligence databases, allowing for seamless interaction between shore, surface, submarine and airborne SI LAN's. Specifically, SCI Networks ensures the availability of networks in defiance of hostile Information Warfare (IW). Technical, physical, and procedural security is used to control access, protect Department of Navy (DoN) information technology resources, and ensure continuous operation of the system within an accredited security posture. SCI Networks fully complies with stated network security policies and is interoperable with deployed network security capabilities. In addition, SCI Networks provides Network Enterprise Services critical to the operational availability of time sensitive indications and warning data, GCCS-M, DCGS-N SI analytic capabilities, and implementation of advanced tactical cryptologic sensor functionality. SCI Networks is the SI FORCEnet enabler that allows tactical participation in the intelligence and sensor grids.

Submarine Local Area Network (SubLAN) provides Navy submarines, with reliable, high-speed SECRET and UNCLASSIFIED Local Area Networks (LANs). When the SubLAN network is combined with other subsystems, it will deliver an end-to-end network-centric warfare capability. The SubLAN program is comprised of two increments - SubLAN 1 and SubLAN 2. SubLAN 1 provides network infrastructure including an Unclassified Wireless Local Area Network (UWLAN), servers, and the Common PC Operating System Environment (COMPOSE), which provides the server and operating system environment for other applications such as Non Tactical Data Processing System (NTDPS) and Navy/Marine Corps Portal (NMCP) to run on. SubLAN 2 provides a full complement of SIPRNET drops, SCI drops, additional switch/backbone capacity, and improved reliability upgrades to SubLAN 1.

Shore Naval Messaging projects include the DMS, Legacy Messaging systems, Naval Regionalized Enterprise Messaging System (NREMS), Tactical Messaging Gateway (TMG), and DMS IA products.

A) **DMS** is an OSD-mandated replacement for the legacy Automated Digital Network (AUTODIN) message delivery architecture; it implements a single organizational messaging system throughout DoD, with seamless strategic (ashore) and tactical (afloat) Joint interoperability.
B) **Legacy Messaging systems** – which encompasses NOVA, CUDIXS, DMDS, FSM, FMX/DUSC, PCMT, GateGuard, and MMS – require life cycle support management during the extended transition of tactical users from legacy messaging to DMS.
C) **NREMS** is an initiative to replace the existing client-server DMS architecture with DMS-compliant, net-centric enterprise messaging, in order to simplify software upgrades and hardware end-of-life replacements, facilitate consolidation of DMS Service Provider sites, and provide a clear migration path to Net-Centric Enterprise Services (NCES) messaging.
D) **TMG** is the messaging gateway between shore-based organizations and the Fleet. TMG incorporates DMS core and COTS products to deliver DMS messages and attachments to the Fleet.
E) **DMS** includes several IA products including the Certification Authority Workstation (CAW) and the Defense Information Infrastructure (DII) Guard. The CAW provides capability to program FORTEZZA Cards (PCMCIA Cards) for use with DMS to provide encryption and digital signatures for organizational messaging. The DII Guard provides the capability for message traffic to traverse enclaves of different classification levels, enforce local security rules, provide non-repudiation, and provide data integrity

The **Navy Marine Corps Enterprise Services (NMES)** provides enterprise services to application developers that will promote sharing of authoritative data and warfighting and warfighting support (business) processes. Additionally, NMES will promote and support the reduction of server and software redundancies that exist in the DoN enterprise. The NMES is a secure framework relying on Global Directory service, PKI certificates and Common Access Cards to provide a Single Sign-on (SSO) for authorizing and gaining access to the underlying web services, regardless of the user or service locations. The NMES's SOA is based on mature industry standards designed to unify the DoN's disparate networks, applications and people. It will enhance Navy mission effectiveness by providing timely and secure access to customized views of multiple data sources that support warfighting and warfighting support (business) processes/missions, by establishing a single authoritative source of applications and data, and through the re-combination of authoritative data "on-the-fly". It enables the Functional Area Managers (FAMs) to execute portfolio management by providing a vehicle for consolidation and integration of their applications and databases while facilitating the transition to enterprise wide functional warfighting and warfighting support (business) processes.

Tactical Messaging, formerly known as Naval Modular Automated Communication System II (NAVMACS II)/Single Message Solution (SMS), automates and increases the speed and efficiency of handling organizational message traffic aboard ships. Tactical Messaging products are being procured to host tactical (afloat) DMS Proxy and replace the older NAVMACS systems, which lack the speed and capacity to handle current message traffic loads during periods of accelerated combat operations. Tactical DMS satisfies Multi-command Requirements of Operational Capability (MROC) requirements to transition to IP based organizational messaging. Tactical Messaging uses Commercial Off-the-Shelf (COTS) hardware and software, Government Off-the-Shelf (GOTS) furnished software, developmental software, and DMS software to provide a technologically improved shipboard message processing system capable of exchanging messages electronically between afloat units and organizations, and individuals in the Department of Defense (DoD) and other federal agencies. The system features PKI signed and encrypted email transfers to/from an afloat unit with the Tactical Messaging Gateway (TMG) enclaves located at the two Naval Computer and Telecommunications Area Master Stations (NCTAMS). The TMG acts as a proxy for the afloat units and submits messages into the DMS backbone. HW and SW procurement and installation requirements will transition to the ISNS program. Tactical Messaging continues to provide NAVY requirements management and product certification. Tactical Messaging retains the Submarine Messaging implementation requirement. There is also a NAVMACS II system providing the legacy interface to Legacy at the NCTAMS as well as other afloat units.

The **Key Management Infrastructure (KMI)** program is a communication security (COMSEC) key distribution and hardware management system consisting of interoperable Joint Service and Civil Agency key management systems. NSA established the EKMS program to meet multiple objectives, which includes supplying electronic key in a secure and operationally responsive manner and providing COMSEC managers with an automated system capable of ordering, generation, distribution, storage, security, accounting, and access control. Equipment includes Local Management Devices (LMDs), Local COMSEC Management Systems (LCMS), Data Transfer Devices (DTDs), Key Processor (KP) devices, and Public Key Infrastructure (PKI) security products.

The **Secure Data** program includes equipment to secure record and data communications. Equipment includes CND and Cryptographic COMSEC equipment. The CND program secures Navy network information systems and includes the following equipment: DII Guard, which allows two way flow between Secret high Local Area Networks (LANs) and Unclassified LANs, Firewall components, which provides protection for networks from unauthorized users, Virtual Private Networks (VPNs), which provides encrypted “Point-to-Point” virtual communication networks, Intrusion Detection System (IDS), Administrator Tool Kits, Network Security tools and Network Intrusion filters. COMSEC equipment includes various KG families of crypto products to include FASTLANEs (KG-75), TACLANEs (KG-175), as well as KIV-7s, KIV-19s.

The **Secure Voice** program includes equipment to enable secure voice communications. Equipment includes various configurations of Secure Terminal Equipment (STE), Secure Voice for the 21st Century Internetworking Function (SV-21 IWF) equipment and Secure Voice 21st Century Crypto (SV-21 Crypto) equipment. The STE is a ship and shore desktop terminal for classified voice, data, facsimile, and video conferencing to replace the existing legacy STU-III units in a phased approach. STE has various configurations that include: Office, Data, Tactical, Narrowband, Condor (wireless), C2 (TACTERM), OMNI and Omega. The SV-21 IWF and SV-21 Crypto equipment includes various configurations that provide the capability for a direct dial, rack mountable, multi-channel gateway that transfers clear or encrypted digital voice/data to multiplexer radio frequency equipment for SATCOM transmission. Associated ancillary items for Secure Voice products include: handsets, power supplies, PUP sleeves, and upgrade kits.

3.0 SCOPE

This Task Order acquires installation project support for PMW-160.I Installation Resource Management Support, in the areas of installation planning, initiation of install preparations, and the daily tracking of install executions. This effort shall also provide technical, and installation project management for the integration of all PMW-160 C4ISR Shipboard systems. The Contractor shall assist PMW-160.I to prepare accurate and standardized C4ISR installation requirements, documentation, process development, database entry and provide installation tracking assistance. This assistance shall cover NNFE C5IMP, Fleet Modernization Program (FMP), SHIPMAIN, Fleet Response Plan (FRP) and Installation Systems Configuration Management for each PMW-160 system.

4.0 APPLICABLE DIRECTIVES/DOCUMENTS

The Contractor shall adhere to the following documentation in accordance with paragraph 5.0, Performance Requirements:

Document	No./Version	Title	Date
Handbook	MIL-HDBK-61A(SE)	Configuration Management Guidance	7-Feb-01
Manual	NAVSEA SL720-AA-MAN-010/020 Rev 2	Fleet Modernization Program (FMP) Management and Operations Manual	10-Jun-02
Manual	NAVSEA TS 9090-310D	Alterations to Ships Accompanied by Alteration Installation Teams (AIT)	4-Feb-04
NAVSEAINST	4130.12B	Configuration Management (CM) Policy and Guidance	
OPNAVINST	1500.76	Navy Training System Requirements, Acquisitions and Management	21-Jul-98
OPNAVINST	11102.1	Equipment Facility Requirements (EFR) Plan	21-Oct-96
PEOC4I& SPACEINST	4081.1	SPAWAR PBL Implementation Plan	Draft
SECNAVINST	5000.2 Series	Implementation of Mandatory Procedures for Major and Non-Major defense Acquisition Programs and Major and Non-Major Information Technology Acquisition Programs	6-Dec-96
SPAWARINST	1500.2	Consolidated SPAWAR/PEO Training Process	14-Mar-03
SPAWARINST	4720.1	Shore Installation Process Handbook	12-Jun-03
	4720.3b	NC5IMP	
SPAWARINST	4160.3A	SPAWAR and PEO C4I and Space Policy, Procedures, and Responsibilities for Technical Manual Management Operations and Life Cycle Support	19-Jul-04
SPAWARINST	4130.5	Handbook for Field Changes and Engineering Changes	5-Jan-04
SPAWARINST	5721.1	SPAWAR Section 508 Implementation Policy	18 Jan 02
Standard	MIL-STD-973 (13)	Configuration Management	
		SHIPMAIN ONEBOOK	
CONOPS		PEO C4I SPACE CONOPS	

5.0 PERFORMANCE REQUIREMENTS

The Contractor shall perform the following tasks in accomplishing the requirements of this Task Order (TO). The Contractor shall provide the necessary timely assistance to meet program emergent requirements as requested by the PMW-160 Program Manager, PEO, PMW-160.I or other properly designated authority.

5.1 PMW 160 Program Installation Support (OPN)

5.1.1 In support of PMW-160.I the contractor (known as PMW-160 IRM Support) shall review technical documentation, PMW-160 installation plans/intentions, and provide progress status reports on significant technical or programmatic issues or concerns related to installation of all PMW-160 C4ISR products as related to platform availabilities. The contractor shall create and submit monthly progress status reports within fifteen days of the following month to PMW-160.I.

5.1.2 The Contractor shall prepare installation status and evaluation reports, assessment of program/project resource requirements and installation documentation, based on thorough review of all installation documentation and databases. The reports shall be prepared as directed and submitted within seven days of assessment completion.

5.1.3 The Contractor shall prepare assigned briefs, white papers, presentations and training to illustrate installation processes and initiatives under study or development. The reports shall be prepared as directed and submitted within seven days of assessment completion.

5.1.4 The Contractor shall prepare installation assessment reports and related financial analysis assisting PMW-160.I in developing and maintaining the financial health of PMW-160 installation efforts. Specific assessment reports and executive summary reports on afloat, shore and Design Support Allocation (DSA) work plans are required which will be based on thorough review of all installation documentation and databases. Action items will be subsequently generated to document issues and discrepancies. The Contractor shall prepare and submit reports within seven days of assessment completion.

5.1.5 With respect to installation planning, platform installation plans/intentions coupled with specific PMW-160 platform or product knowledge, the Contractor shall review technical documentation, provide procedural interface between the Platform PMWs, PMW-160, the PEO, SPAWAR 04M and other System Commands (SYSCOMs) as necessary, providing progress status reports on significant technical or programmatic issues or concerns related to installation resource planning, execution and integration.

5.2 PMW-160 Overarching Installation Support (OPN)

The Contractor shall assist PMW-160.I to provide platform, product and PMW-160 program support required to install PMW-160 products on board ships and/or shore facilities.

5.2.1 Installation Files

5.2.1.1 The Contractor shall provide PMW-160 liaison support to all installation activities, collecting all equipment installation documentation, plans and intentions for PMW-160, while ensuring the required information is forwarded to the appropriate party for review and approval. The Contractor shall conduct liaison activities as directed or necessary to ensure adequate program support and timely response by PMW-160.I.

5.2.1.2 The Contractor shall maintain inputs into the designated installation database or individual tracking system of PMW-160 or the PEO entering all documentation, plans and installation intentions into the installation file repository, designated installation database, or individual tracking system, to facilitate review and approval or rejection for designated approval cycles. The Contractor shall update the databases, tracking systems and files within 48 hours of information receipt.

5.2.1.3 The Contractor shall generate and forward notification within and outside PMW-160 when documentation is not received within the appropriate schedule for the designated system installations. The Contractor shall maintain a PMW-160.I notification file, and generate notices five days and two days prior to the required due date as necessary to ensure a timely response. The Contractor shall provide a monthly report detailing all response due dates and the date the response was received.

5.2.2 Installation Work Plan Support

5.2.2.1 The Contractor shall support installation work plans and changes provided by PMW-160 or the PEO, including gathering scope of work documentation. The Contractor shall update the PMW-160.I installation files within 24 hours of receiving new installation information from the PMW and/or PEO.

5.2.2.2 The Contractor shall assist PMW-160 personnel in tracking installation estimated costs, development and approval of Ship Change Documents (SCD), Ship Configuration Change Proposal (SCCP), Justification/Cost Forms (JCFs), Ship Alteration Records (SARs), Installation Requirements Drawings (IRD), SHIP Installation Drawings (SID), Equipment Delivery Date(s) (EDD) and other necessary installation documentation. The Contractor shall maintain PMW-160.I ship installation cost and approval spreadsheets and databases current at all times. The Contractor shall update the spreadsheets and databases within 24 hours of information receipt.

5.2.2.3 The Contractor shall assist PMW-160 personnel in tracking installation-estimated costs, development and approval of Shore related products such as Standard Plans, Test Plans, Installation System Operational and Verification Test (SOVT) Report, Basic Electronic System Engineering Plan (BESEP), Fleet Readiness Control Board (FRCB) inputs, Risk Mitigation Plan, Installation Design Plans (IDPs) and the Site Survey Report as necessary. The Contractor shall maintain PMW-160.I shore installation cost and approval spreadsheets and databases current at all times. The Contractor shall updates the spreadsheets and databases within 24 hours of information receipt.

5.2.2.4 The Contractor shall assist the PMW, the PEO and SPAWAR 04M as assigned in these efforts and ensure the installation file repository, designated installation database, or individual tracking system is current and complete. The Contractor shall maintain a log of all installation changes, approvals, and documentation received and entered, for each installation file. The Contractor shall make this information available to PMW-160.I personnel when requested.

5.2.2.5 The Contractor shall notify appropriate personnel from PMW-160 when installation documentation is incomplete, missing or late on the same day the oversight is noted.

5.2.3 Installation Milestones

The Contractor shall assist PMW-160 in coordinating Shipcheck/Site Survey and equipment installation dates. The Contractor shall maintain the installation file repository, designated installation database, or individual tracking system and program/project milestone schedule, making modifications on the same day changes are received, to ensure the file is kept up-to date.

5.2.4 Installation Completion Documentation

The Contractor shall track all installation completion documentation such as System Operational and Verification Test (SOVT) Report, Integrated Logistics Support (ILS), initial training and Installation (Alteration) Completion Reports in accordance with current policies and associated processes. The Contractor shall include installation completion documentation within the installation file, designated installation database, or individual tracking system updating the file within the same day new information is received.

5.2.5 Reporting

The Contractor shall support and track any install related information required to answer Planning Yard, Installation Management Office (IMO), Consolidated Installation Contractor and Alteration Installation Team (AIT) questions concerning system installation relating to PMW-160. The Contractor shall research, analyze, locate and include any information in the installation file repository, designated installation database, or individual tracking system as necessary for PMW-160 or the PEO to answer the above questions.

5.2.6 Representation

The Contractor shall provide PMW-160 or the PEO technical representation at Installation Planning Working Groups, Production, PMW-160.I, PMW-160 or other installation planning/coordination/status meetings as assigned. The Contractor shall provide all documentation required to support PMW-160.I’s position at these meetings and conferences. The Contractor shall submit all material to be used at these meetings and conferences for approval no later than fives days prior to the scheduled meeting, and submit required documentation modifications for approval no later than one day prior to the scheduled meeting.

6.0 DELIVERABLES/PRODUCTS/SCHEDULES

The Contractor shall provide the following deliverables within the timeframe specified via NMCI compliant software products:

REQUIREMENT	DUE DATE
Monthly Status Report	Due the 10th of the following month
Weekly SUBHEAD Status Reports	Due Monday of the following week
Trip Report	Due within 5 days of return from Travel
Briefing Materials	As required
Technical Papers	As required
Installation Assessment Reports	As required

7.0 SECURITY

The nature of this task may require access to Secret information and spaces. The contractor may be required to attend meetings at Secret levels.

8.0 NAVY MARINE CORPS INTRANET (NMCI)

The nature of this task does not require Contractors to procure NMCI seats for personnel at the Contractor's facility. The Government will provide six (6) on-site NMCI seats under this task order for FY08, with an estimated increase in future options.

9.0 BEST PRACTICES

Work performed by the Contractor shall provide support to PMW-160 command-level “Best Practices” principles incorporated in the SPAWAR Program Manager’s Toolkit Acquisition Support Office Guides (1) Acquisition Program Structure Guide; (2) Contract Management Process Guide; (3) Program Manager’s Handbook; (4) Scheduling Guide; (5) Systems Engineering Guide; (6) Technology Alignment Guide and support the command wide implementation process.

10.0 TASK ORDER MANAGER

Michael D. Davis; (619) 524-7231; michael.d.davis@navy.mil

11.0 TRAVEL

It is estimated that the below trips may be required for the completion of the deliverables for this task order. All contractor travel will be approved in advance by the Task Order Manager (TOM).

Travel:

Travel	**# Trips**	**# People**	**# Days**
San Diego, CA to Arlington, VA	2	2	5
San Diego, CA to Charleston SC	2	4	5
San Diego, CA to Norfolk, VA	2	2	5