

# PERFORMANCE WORK STATEMENT (PWS)

## MILITARY COMMUNITY AND FAMILY POLICY ENCLAVE (MC&FP)

### IT SERVICES AND SUPPORT

JULY 16, 2012

- 1. INTRODUCTION.** The Military Community & Family Policy (MC&FP) programs encompass all resources and the development of new resources, processes, personnel, materials, training, equipment, and technology necessary to provide service members and their families with critical information.

There are emerging needs for this requirement; some have already become established, others are arising, and additional needs are expected to develop in the future. It is understood that this is a dynamic environment encompassing quality of life support systems for military members and their dependents. Due to the continuing war efforts, it can be challenging to predict specific needs.

- 2. SCOPE OF WORK.** The Office of the Under Secretary of Defense (OUSD) for Personnel and Readiness (P&R) Military Community & Family Policy (MC&FP) directorate requires professional Information Technology (IT) services and support for the Military Community & Family Policy Enclave (MCFPE) operational computer systems that hosts the Military OneSource (MOS) and Military Homefront (MHF) websites as well as its supporting applications. IT services will include, the enhancement, development and maintenance of the primarily Oracle Database centered applications and websites. The requirements will encompass network, programming, operations, systems administration, documentation development and maintenance, network architecture design and implementation, database administration and Information Assurance (IA) technological support.
- 3. BACKGROUND.** The MCFPE is comprised of several Information Technology (IT) environments all centered on a multifaceted Oracle database deployment. The hardware and software is currently located at the Space and Naval Warfare Center (SPAWAR) Atlantic, Washington DC Navy Yard datacenter. The enclave is configured as an independent OSD address space with the Defense Research and Engineering Network (DREN) providing the network connection.

The entire Enclave is scheduled to be moved and hosted at a Defense Information Systems Agency (DISA) datacenter. The move is expected to be complete by 1 October 2012. DISA will be providing all hardware and software; the Operating systems maintenance and support, Data backups and Continuity of Operations (COOP) services with a 24 hour Return to Operation (RTO) recovery time.

Utilizing a multiple zone security configuration, the MCFPE supports Production and Pre-Production, DoD Information Assurance Certification and Accreditation Process (DIACAP) certified regions. This provides the MC&FP with a safe and secure platform to deploy tools for the MC&FP staff and a reliable information delivery to the public.

- 4. MAIN OBJECTIVES.** Provide and maintain Information Technology Services Support that encompasses web-centric activity processes, quality assurance, reporting and deliverable documentation with efficiency and cost effective results. Create and maintain assurance of strategic management processes incorporating MC&FP and MCFPE staff coordinated milestones that demonstrate deliverance and integration of mission essential resources (IT and web-centric media, social media and training) that will impact the military community as a whole.

Outline and implement government approved schematic roadmaps that highlight improvements for IT architecture, innovation of resources and improved business processes.

- 4.1.** The MCFPE environment currently includes, but is not limited to applications and websites in 4.1.3.

- 4.1.1. **MC&FP Staff Services:** On-line applications primarily used by MC&FP staff to support programs and task management. (Attachment 1)
- 4.1.2. **Military Community Outreach Staff Applications:** On-line applications primarily used by MC&FP Technical Staff, Subject Matter Experts (SME) and content authors to manage and maintain the data and content of the MC&FP managed intellectual properties. (Attachment 1)
- 4.1.3. **Military Community Outreach Websites and applications:** On-line applications and websites intended for the general public or MC&FP targeted clients and communities.
  - 4.1.3.1. Military OneSource  
<http://www.militaryonesource.mil/>
  - 4.1.3.2. MilitaryHOMEFRONT  
<http://www.militaryhomefront.dod.mil/>
  - 4.1.3.3. Plan My Move  
<http://planmymove.mhf.dod.mil/>
  - 4.1.3.4. Plan My Deployment  
PENDING CURRENTLY IN DEVELOPMENT
  - 4.1.3.5. MilitaryInstallations  
<http://www.militaryinstallations.dod.mil/>
  - 4.1.3.6. HOMEFRONTConnections (login required)  
<https://apps.mhf.dod.mil/homefrontconnections>
  - 4.1.3.7. Military Youth on the Move  
<http://apps.mhf.dod.mil/myom>
  - 4.1.3.8. USA4MilitaryFamilies  
<http://www.usa4militaryfamilies.dod.mil/>
  - 4.1.3.9. Domestic Violence Training System  
<https://codvt.dod.mil>
  - 4.1.3.10. Defense Installation Messaging System (DIMS)  
<https://apps.mhf.dod.mil/dims>
  - 4.1.3.11. Wounded Warrior Resource Center Tracking System (WWRCTS)(CAC or ECA required)  
<https://apps.mhf.dod.mil/wwrcts>
  - 4.1.3.12. MC&FP Information and Resources  
<http://apps.mhf.dod.mil/mcfp/portal>
  - 4.1.3.13. JFSAP Scheduling Form  
<http://jfsap.mhf.dod.mil>
  - 4.1.3.14. Conference Registration Application  
<http://apps.mhf.dod.mil/conf/OWF>
  - 4.1.3.15. MC&FP eMagazine  
<http://apps.mhf.dod.mil/mcfp/emag>
  - 4.1.3.16. Voluntary Education Portal  
<http://apps.mhf.dod.mil/voled>
  - 4.1.3.17. EFMP Education Directory  
<http://apps.mhf.dod.mil/efmp/directory>
  - 4.1.3.18. MOS Discussion Boards  
<https://forums.militaryonesource.mil/>
  - 4.1.3.19. Blog Brigade  
<http://blog-brigade.militaryonesource.mil/>
  - 4.1.3.20. MSEP Jobs  
<https://msepjobs.militaryonesource.mil/>
  - 4.1.3.21. eSponsorship Training  
<http://apps.mhf.dod.mil/esat>
  - 4.1.3.22. Online Learning  
<http://apps.mhf.dod.mil/olearn>

4.1.3.23. Warfighter Registration  
<http://apps.mhf.dod.mil/conf/OWF>

## 5. APPLICABLE DOCUMENTS – ATTACHMENTS

- 5.1. Attachment 1 MCFP Enclave Applications: Details the name, function primary users, technologies and number of screen forms/pages.
- 5.2. Attachment 2 Technical References: Specific references that include DoD directives and instructions, OMB memo and circulars, public law, U.S. code, Defense Information Systems Agency STIG guidance, and OSD guidance.
- 5.3. Attachment 3 MC&FP Enclave User Statistics: Includes user statistics for 21 web-based applications/sites.
- 5.4. Attachment 4 Hardware Baseline for SPAWAR Navy Yard Data Center: Lists Hardware, make, model and installed software/operating system for each asset.
- 5.5. Attachment 5 MC&FP owned domain names: List includes all domain names that are not dot-mil.
- 5.6. Attachment 6 Hardware Baseline for DISA Data Center: Lists hosts, storage capacity and software for each asset.
- 5.7. Attachment 7 Terms and Conditions
- 5.8. Attachment 8 Quality Assurance Surveillance Plan (QASP)
- 5.9. Attachment 9 DoD Forms & Conditions
- 5.10. Attachment 10 Administrative Considerations
- 5.11. Attachment 11 Project CLIN Structure
- 5.12. Attachment 12 MC&FP Case Management System Overview with Link to DEMO Site

## 6. REQUIREMENTS

### 6.1. Security and user access

The Contractor shall certify that all of their personnel requiring access to the MC&FP Database and its applications are properly trained and fully informed of their responsibilities when engaging sensitive MC&FP data. Personnel assigned to or utilized by the contractor in the performance of this contract shall be United States citizens. Personnel who require access to the MC&FP database and its applications must be determined trustworthy as a result of a favorable completion of a National Agency Check (NAC). (Attachment #10)

### 6.2. Operational Support

- 6.2.1. Non Duty Day operations will be on-call for recovery support within 5 hours.
- 6.2.2. Provide system administration during normal duty days for all government provided servers and equipment. (Attachment 4)
  - 6.2.2.1 Daily application checks using Oracle Enterprise Manager:
    - 6.2.2.1.1 Connectivity checks
    - 6.2.2.1.2 Services checks
    - 6.2.2.1.3 Event log reviews
    - 6.2.2.1.4 Space utilization
    - 6.2.2.1.5 Checking daily backups for successful completion
    - 6.2.2.1.6 Anti-virus support and recording results in system logs.
    - 6.2.2.1.7 As required, provide and track alerts of downed services, restarting services, updating/upgrading server software, updating server scripts, troubleshooting and coordinating for repair of connectivity problems and troubleshooting and correcting failed backups. The results of the daily application checks will be recorded in the Government Tasking, Assignments and Reporting (TAR) system.
- 6.2.3. Provide Quarterly Baseline validation report of all equipment and software by the 10th of the month.
- 6.2.4. Maintain problem/resolution logging in the Tasking, Assignments and Reporting (TAR)
- 6.2.5. Identify any firewall or network related problems and report them to the MC&FP Operations Manager or Program management using the Government Tasking, Assignments, and Reporting (TAR) application within 1 business day.

- 6.2.6. Maintain Usage database (total number of users and most frequently accessed screens) on all MC&FP websites to provide government analysts ad hoc research usage information
- 6.2.7. Collaborate with and assist SPAWAR Atlantic technical staff with moving the MCFPE to the DISA data center. NOTE: This may not be necessary should this task be complete before award of this contract.

### 6.3. **Information Assurance (IA) Support**

Ensure that compliance with all new or standing DoD and OPM Information Assurance requirements for MCFPE are maintained in accordance with the Department of Defense Directive DoDD 8570.01 (Attachment 2 - 1.1.2.) (requirements; such as the DISA Information Assurance Vulnerability Management (IAVM) notices, new DISA Security Technical Implementation Guidelines (STIG) checks, the DISA Port and Protocol guidance, or DISA Directives, Communications Tasking Orders (CTOs), Operational Orders (OPORDs).

- 6.3.1 Contractor shall manage the required DoD system security certification and accreditation posture necessary to sustain the MCFPE current Authority To Operate (ATO) at MAC Level III Sensitive.
- 6.3.2 Provide engineering support for the development and implementation of application security architectures to meet new and evolving DoD security requirements.
- 6.3.3 Coordinate with the other IT staff and contractors to ensure all Information Assurance related issues are addressed within mandated schedules.
- 6.3.4 Provide Information Assurance Oversight and Regulatory Compliance support.
- 6.3.5 Maintain the system security and DIACAP documentation to keep pace with the evolving MCFPE architecture.
- 6.3.6 Maintain an accurate and current baseline document recording configuration changes within 10 business days. (Attachment 4)
- 6.3.7 Coordinate and execute Security Test and Evaluation Plans (ST&E Plan) to ensure availability and integrity of the MCFPE during all upgrades and functional enhancements.
- 6.3.8 Review the government provided monthly data created by the DISA Retina Network Security Scanner to determine the current Information Assurance posture, assessing system vulnerabilities; determining adequacy of security controls, and mitigating residual risk.
  - 6.3.8.1 Validate all MCFPE assets are Retina scanned or the current DISA required scanning tool as at least one a month.
  - 6.3.8.2 All MCFPE Windows based Assets will be Gold Disk scanned at the Platinum level at least one a month.
  - 6.3.8.3 All new or changing STIGS will be reviewed monthly for impacts on the MCFPE and implement mitigations for compliance.
  - 6.3.8.4 All MCFPE relevant STIGS will be reviewed at least once a calendar year. Providing the government a risk assessment report.
- 6.3.9 Utilize the DISA Vulnerability Management System (VMS) to maintain current and all emerging threats and risks are identified, acknowledged, implement or mitigated within the DISA mandated timelines.

### 6.4. **Configuration Management**

Ensure MCPFEs risk of failure is minimized with effective Configuration control protocols specified by the Department of Defense Directive DoDD 8500.01E (Attachment 2 - 1.1.1) and the Department of Defense Instruction 8500.2 (Attachment 2 - 1.2.1)

- 6.4.1 Contractor shall ensure all technical deliveries will conform to the requirements set forth in the OSD MC&FP MCFPE Configuration Management Plan (CMP). (Attachment 2 - 1.8.2 and Attachment 2A)
- 6.4.2 Contractor shall actively participate in all requirements of the MCFPE configuration Control Board as outlined in the MCFPE Change Control Board (CCB) Charter. (Attachment 2 - 1.8.1, and Attachment 2A)

## 6.5. Application Development and Sustainment

To support the MCFPE by creating new, expanding or enhancing existing MC&FP applications, tools and Websites.

6.5.1 Contractor shall provide Information Technology (IT) application support to the MCFPE by creating new and enhancing existing MC&FP Websites and applications as identified in 4.1.3 of the PWS.

6.5.2 Services are:

6.5.2.1 Requirements analysis.

6.5.2.2 Programming.

6.5.2.3 Testing.

6.5.2.4 Project Management

6.5.2.5 Quality control and monitoring of MCFPE development activities.

6.5.2.6 Web-site and application development, enhancements and modifications.

6.5.3 Provide programming and technical support:

6.5.3.1 Hyper Text Markup Language (HTML)

6.5.3.2 Cascading Style Sheets (CSS)

6.5.3.3 Extensible Markup Language (XML)

6.5.3.4 Oracle Application Express (APEX)

6.5.3.5 Structured Query Language (SQL)

6.5.3.6 Oracle Procedural Language/Structured Query Language (PL/SQL)

6.5.3.7 Microsoft Transact-SQL

6.5.3.8 JAVA

6.5.3.9 JAVA Script

6.5.3.10 Hypertext Pre-Processor (PHP)

6.5.3.11 MySQL Database Administration

6.5.3.12 Drupal

6.5.3.13 Extensible Hypertext Markup Language (XHTML)

6.5.3.14 Internet Information Services (IIS) Web Server

6.5.3.15 Apache Tomcat Web Server

6.5.3.16 Apache Web Server

6.5.3.17 Microsoft Exchange

6.5.3.18 Microsoft Active Directory

6.5.3.19 Windows PowerShell scripting

6.5.3.20 Red Hat Enterprise Linux

6.5.3.21 Windows Server

6.5.3.22 Linux Bash shell scripting

6.5.3.23 Active Server Pages .NET (ASP.NET)

6.5.3.24 Java Server Pages (JSP)

6.5.3.25 WordPress

6.5.3.26 phpBB

6.5.3.27 Oracle Database

6.5.3.28 Oracle WebCache

6.5.3.29 Oracle HTTP Server

6.5.3.30 Technologies that the contractor determines required for future use are to be supported.

6.5.4 Maintain Section 508 compliance for all applications and websites.

6.5.5 Design, develop and support large, complex applications or integrated suites of applications for the MCFPE.

6.5.6 Gather or receive user requirements and functional designs, including system and information flow diagrams and perform technical design Tasks including program/module specifications, operations requirements, and security and information requirements.

6.5.7 Coordinate application and utility programs including coding, testing, implementation and maintenance.

- 6.5.8 Support and maintain the Akamai NetStorage and Akamai Web Application Accelerator services used by MCFPE as part of this PWS. <http://www.akamai.com>
- 6.5.9 All government support requests loaded in the Tasking, Assignments, and Reporting (TAR) will be acknowledged by the contractor within 3 business days. Acknowledgement will include the projected completion date or a date the projected completion date will be provided.
- 6.5.10 Contractor will be required to maintain and manage the MC&FP owned commercial Domain Names. (Attachment 5 - Public Domain Names)
  - 6.5.10.1 This will include the responsibility of maintaining and configuring the MC&FP Network Solutions Management Account. <http://www.networksolutions.com>

## 6.6. Documentation

Ensure all documentation and reference materials for the MCFPE are accurate and up to date.

- 6.6.1 Maintain all DIACAP documentation to keep it current with the MCFPE applications and system configuration.
- 6.6.2 Maintain and author all Standard Operating Procedures (SOP) necessary to document the daily operations Tasks and reoccurring work.

## 6.7 Network Enclave Management

Contractor to provide governance to and oversight of the MCFPE as follows:

- 6.7.1 Performance Management - Measure and make available to the government monthly, enclave and application performance information to ensure performance is maintained at an acceptable level.
- 6.7.2 Account Management – Maintain the user and host account security credentials required to access and maintain the MCFPE.
- 6.7.3 Fault Management - Detect, log, notify users of, and (to the fullest extent possible) automatically fix network problems to keep the network running effectively.
- 6.7.4 Security Management - Control access to network resources according to MCFPE Security Design Plan to mitigate network risk of sabotage (intentionally or unintentionally) and sensitive information cannot be accessed by those without appropriate authorization.
- 6.7.5 Taxonomy Management - Create and manage the taxonomy definitions used in the MCFPE to capture metadata supporting the user interfaces presentation requirements (Attachment #1).

## 6.8 System Architecture Support

Contractor will provide architectural design and standards development insuring the MCFPE is following the most effective technology paths to meet the MC&FP Mission. Contractor will define conceptual and physical architectures, develop proof of concepts, and determine the application components required in the support of the MCFPE initiatives.

- 6.8.1 Contractor will provide qualified resources to:
  - 6.8.1.1 Provide Architectural, Design and Development consultative services to other MC&FP staff.
  - 6.8.1.2 Estimate level of effort and costs for new and emerging development efforts.
  - 6.8.1.3 The contractor will provide technical integration guidance to the MC&FP staff when other government and contract staff supporting MCFPE development efforts as the work relates to the enclave, and implementation of recommended development and/or migration plans.
  - 6.8.1.4 Analyze potentially new IT resource efforts or website functionalities.
  - 6.8.1.5 Oversee Operation and Maintenance of the MCFPE platform.
  - 6.8.1.6 Provide system integration of new features, functions, content, applications, and components.
  - 6.8.1.7 Assist in developing and deploying newly identified applications.
  - 6.8.1.8 Respond to system failure or technical difficulties.
  - 6.8.1.9 Utilize commercial products developed by Oracle Corporation and other approved DoD COTS Vendors to implement web-based IT solutions (applications and websites).
  - 6.8.1.10 The contractor will develop and execute detailed systems testing and implementation plans, test specifications and test cases for all system and application changes.

- 6.8.1.11 Ensure development standards are defined and implemented and that development staff is educated on use of standards.

## 6.9 Oracle and MySQL Database Administration support

Maintain and oversee the activities of all databases used in the MCFPE. Oracle is the primary database used on MCFPE comprising 95% of the workload, the remaining 5% is MySQL.

- 6.9.1 Maintain the database configurations for the optimal performance.
- 6.9.2 Perform database back-up and restoration procedures as per DoD requirements, standards and MCFPE operations documentation.
- 6.9.3 Establish user security requirements and monitor access.
- 6.9.4 Monitor performance, managing parameters to provide fast query responses.
- 6.9.5 Map out the conceptual design for a planned database implementations.
- 6.9.6 Translate logical designs into a specific data models to support new and changing applications.
- 6.9.7 Refine the database physical designs to meet system storage requirements and support evolving functional needs.
- 6.9.8 Write database documentation, including data standards, procedures and definitions for the data dictionary (metadata) to support and maintain the MCFPE DIACAP accreditation.
- 6.9.9 Maintain, manage and test quarterly the database back-up and recovery plans ensuring that the storage, archiving and recovery procedures are functioning correctly.
- 6.9.10 Review the database capacity posture quarterly to ensure the MCFPE can support any new or expanding applications.

## 6.10 Helpdesk Support

Provide Tier 1 Helpdesk services for MC&FP Websites, applications during normal business hours. A second Tier 1 helpdesk will also be provided to support the MC&FP Case Management System; this must be manned 24 hours a day, 365 days a year. Provide technical resources and staff to operate Tier 1 Helpdesk services for MC&FP Websites, applications and projects during standard government business hours.

- 6.10.1 Provide live phone support from 0800-1700 EST Monday through Friday with voicemail support after hours and on weekends and holidays.
- 6.10.2 Support and manage all help requests originating from an 800-phone number provided to the contractor. The government shall retain ownership of the phone number used.
- 6.10.3 Ensure all help requests will be acknowledged within 5 business hours.
- 6.10.4 Manage the Application Messaging System (AMS). Provide Tier 1 services to manage and route all user queries from the AMS application.
- 6.10.5 Ensure all requests are forwarded to the appropriate subject matter expert and ensure all requests are properly closed when the action is complete. Contractor will provide resources and staff to operate a 24 hours a day, 365 days a year, manned Tier 1 Helpdesk service to support the Military OneSource (MOS) Case management System (CMS).

Provide Technical and user access assistance to the users and managers of the Military OneSource (MOS) Case Management System (CMS). This CMS application will be used by Military OneSource (MOS) Managers and contracted agents to manage and maintain information from all MC&FP projects and programs that require participant information tracking. Currently under development the CMS is planned to be deployed by August 2012. The Military OneSource (MOS) Employee Assistance Program (EAP) and Spouse Education and Career Opportunities (SECO) call centers are scheduled to utilize the CMS starting FY 2013.

Contractor will provide a "Toll Free" phone so users will have access through a unique, phone number, email and AMS messages service. See Attachment #12, CMS Application Information and Link to Demo site.

## 6.11 Project Status Report and Accounting

- 6.11.1 The Report will be delivered at the Close of Business (COB) every Wednesday.

- 6.11.2 Accomplishments this week: Describe in bullet format any and all notable Tasks completed since the last report.
- 6.11.3 Planned activities next week: Describe, in bullet format, the projected activities for the upcoming week.
- 6.11.4 Future planned activities: Describe, in bullet format, notable projects or Tasks projected for the near future (2 to 10 weeks)
- 6.11.5 Issues to be resolved: Describe, in bullet format, any topics, issues, resources or Tasks that are preventing progress on deliveries.
- 6.11.6 All Tasks and work performed will be documented in the MCFPE Tasking, Assignments and Reporting (TAR) application. Entries will be made daily with meaningful narrative descriptions of the work performed and the hours expended.
- 6.11.7 Contractor will be required to participate in weekly Status telephonic meetings for technical issues and projects.
- 6.11.8 Contractor will be required to attend a weekly Management meeting for administrative and situational awareness issues and projects. This will be a telephone meeting.
- 6.11.9 Contractor to attend quarterly management meetings. These meetings are either face to face, Video Tele Conference or telephonic and the contractor will be advised of the schedule accordingly.
- 6.11.10 This will be an in person, face to face meeting at a government location in the Washington DC area.
- 6.11.11 Contractor will use the government's Technical Assistance Reporting (TAR) system to obtain government assignments, report progress and obtain government approval on completed assignments. Contractor will enter time devoted to assignments in the TAR application.

## 7. DELIVERABLES

7.1 **Standing Reports.** The following reports will be provided to the government.

7.1	Deliverable	Frequency	Acceptable Medium/Format	Submit to
	Bi-Monthly Progress Report via MHF TAR System	15 <sup>th</sup> and last day of each month	Electronically in MS Word Excel PowerPoint	COR and Director MC&FP
	Monthly Roll-up Reports via MHF TAR System (Includes changes and implementations)	Monthly	Electronically in MS Word Excel PowerPoint	Director MC&FP
	Applications and Database Operations and Effectiveness Report	At the close of each quarter	Electronically in MS Word Excel PowerPoint	COR and MC&FP Functional Representative
	Quarterly Manpower and ODC Report	Quarterly – NLT 10th calendar day following the end of each of the 4 fiscal year quarters or delivery date as designated by the COR	Electronically in MS Word Excel PowerPoint	COR and MC&FP Technical Representative
	Security user access report To include testing status of each contractor, date each user completed each course, and their citizenship.	Monthly	Electronically in Excel	Government Information Assurance Manager (IAM)

7.1.1 **Quarterly Manpower and Travel/ODC Report** – The contractor shall populate a Manpower and ODC Report. Typical report shall include, number of contracted staff (sub-contractors), staff titles, number of hours worked correlated with the appropriate section of the PWS. Cost data shall include other direct costs (ODCs) invoiced by each contracted staff, Example: John Doe – JTR Approved

Travel to San Diego (air fare, per diem, total etc.) for the month it occurred. Cost data shall also include all other contractor ODCs (not invoiced based on individuals) for the month it occurred. The government may direct minor adjustments to the reporting information and media as required to maintain the accuracy and usefulness of the information provided. The Quarterly Manpower and ODC Report shall be submitted no later than the tenth (10<sup>th</sup>) calendar day of the following quarter for each of the quarters during the awarded performance period.

The contractor shall construct the report using the following format and fields:

<b>Contract Number</b>				<b>Contract Amount</b>	\$
<b>Program Manager</b>				<b>Contract Funds Expended</b>	\$
<b>Contractor Sub-Contractor Last Name</b>	<b>PWS Section</b>	<b>Hours</b>	<b>Special Projects</b>	<b>Labor Category</b>	<b>On Site/Off Site</b>

<b>Other Direct Costs (ODCs)</b>	<b>Total</b>
Travel	\$ -
Materials	\$ -
Training	\$ -
Total (Qtr)	\$ -
Total Expended to Date	\$ -

Document ODC, cost and description below:

<b>ODCs</b>	<b>Cost</b>	<b>ODC Description</b>

## 7.2 Weekly Project Status Report and Accounting

- 7.2.1 The Report will be delivered at the Close of Business (COB) every Wednesday.  
 Accomplishments this week: Describe in bullet format any and all notable Tasks completed since the last report.  
 Planned activities next week: Describe, in bullet format, the projected activities for the upcoming week.  
 Future planned activities: Describe, in bullet format, notable projects or Tasks projected for the near future (2 to 10 weeks)

Issues to be resolved: Describe, in bullet format, any topics, issues, resources or Tasks that are preventing progress on deliveries.

- 7.2.2 All Tasks and work performed will be documented in the MCFPE Tasking, Assignments and Reporting (TAR) application. Entries will be made daily with meaningful narrative descriptions of the work performed and the hours expended.
- 7.2.3 Contractor will be required to participate in weekly Status telephonic meetings for technical issues and projects.
- 7.2.4 Contractor will be required to attend a weekly Management meeting for administrative and situational awareness issues and projects. This will be a telephone meeting.
- 7.2.5 Contractor to attend quarterly management meetings. These meetings are either face to face, Video Tele Conference or telephonic and the contractor will be advised of the schedule accordingly.
- 7.2.6 This will be an in person, face to face meeting at a government location in the Washington DC area.
- 7.2.7 Contractor will use the government's Technical Assistance Reporting (TAR) system to obtain government assignments, report progress and obtain government approval on completed assignments. Contractor will enter time devoted to assignments in the TAR application.

### 7.3 **Program Management**

Contractor shall provide a Program Management Plan to coordinate all objectives of this PWS as to, quality, compliance as stated in the QASP and all referenced DoD instructions and policies.

### 7.4 **Quality Control Plan**

A final Quality Control Plan (QCP) is due with the Technical Quote (Volume 1).

## **THIS PWS INCLUDES THE FOLLOWING ATTACHMENTS:**

1. List of MCFP Enclave Applications
2. Technical References
3. MCFPE User Statistics
4. Navy Yard Hardware Baseline
5. Public Domain Names
6. DISA Hardware Baseline
7. Terms & Conditions
8. Quality Assurance Surveillance Plan (QASP)
9. Forms and Conditions Appendix (DoD)
10. Administrative Considerations
11. CLIN Structure
12. Case Management System(CMS) Overview
13. Technical Questions and Answers – Informational Purposes only