SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS

OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, AND 30

1. REQUISITION NUMBER: M95450293774

2. CONTRACT NO.	3. AWARD/EFFECTIVE DATE	4. ORDER NUMBER	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
47QTCK18D0001	29-Jun-2022	M6785422F4802		

7. FOR SOLICITATION INFORMATION CALL:	a. NAME	b. TELEPHONE NUMBER *(No Collect Calls)*	8. OFFER DUE DATE/LOCAL TIME

9. ISSUED BY CODE M67854

MARCORSYSCOM, PMM-171
ATTN: CYNTHIA MATTHEWS
2200 LESTER STREET
QUANTICO VA 22556

TEL: 703-432-7849
FAX:

10. THIS ACQUISITION IS [X] UNRESTRICTED OR [ ] SET ASIDE: _____ % FOR:

[ ] SMALL BUSINESS
[ ] WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM
[ ] HUBZONE SMALL BUSINESS
[ ] EDWOSB
NAICS: 541519
[ ] SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS
[ ] 8(A)
SIZE STANDARD: $30,000,000

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED
[ ] SEE SCHEDULE

12. DISCOUNT TERMS
NET 30 DAYS

[ ] 13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)

13b. RATING

14. METHOD OF SOLICITATION
[ ] RFQ [ ] IFB [ ] RFP

15. DELIVER TO CODE M67854

COMMANDER - MARINE CORPS SYSTEMS COMMAND
LAURA ONEILL
2200 LESTER STREET
QUANTICO VA 22134-5050

16. ADMINISTERED BY CODE

SEE ITEM 9

17a. CONTRACTOR/ OFFEROR CODE 6XWA8 FACILITY CODE

SCIENCE APPLICATIONS INTERNATIONAL CORPO
SAIC
MS. KRISTINA O. WILSON
12010 SUNSET HILLS RD
RESTON VA 20190-5856
TELEPHONE NO. (843) 746-6334

[ ] 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER

18a. PAYMENT WILL BE MADE BY CODE HQ0871

DFAS COLUMBUS HQ0871
P.O.BOX 360922
COLUMBUS OH 43213-9022

18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a. UNLESS BLOCK BELOW IS CHECKED [ ] SEE ADDENDUM

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/ SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	SEE SCHEDULE				

25. ACCOUNTING AND APPROPRIATION DATA

See Schedule

26. TOTAL AWARD AMOUNT (For Govt. Use Only)

$2,025,135.05

[ ] 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1. 52.212-4. FAR 52.212-3. 52.212-5 ARE ATTACHED. ADDENDA [ ] ARE [ ] ARE NOT ATTACHED

[X] 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA [X] ARE [ ] ARE NOT ATTACHED

[X] 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN 1 COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED.

[ ] 29. AWARD OF CONTRACT: REF. OFFER DATED . YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS:

30a. SIGNATURE OF OFFEROR/CONTRACTOR

31a. UNITED STATES OF AMERICA (SIGNATURE OF CONTRACTING OFFICER)

30b. NAME AND TITLE OF SIGNER *(TYPE OR PRINT)*	30c. DATE SIGNED	31b. NAME OF CONTRACTING OFFICER *(TYPE OR PRINT)*	31c. DATE SIGNED
Katherine McClees Sr. Contracts Analyst	28 June 2022	Clinton Wells TEL: 703-784-2875 EMAIL: clinton.wells@usmc.mil	28 June 2022

Standard Procurement System (SPS)
Naval Applications and Business Services (NABS)
Marine Corps Systems Command (MCSC)
Program Executive Officer, Manpower, Logistics and Business Solutions (PEO MLB)

Standard Procurement System (SPS)
Performance Work Statement (PWS)

June 2022

Version 7.4

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 Introduction

1.1 Purpose and Scope

Naval Applications and Business Services (NABS), formerly Program Manager, Applications (PM APPS) provides acquisition oversight for a portfolio of United States Marine Corps (USMC) software application systems and has a requirement for Post Deployment Software Support (PDSS) for Standard Procurement System (SPS). SPS falls under the Marine Corps Systems Command (MCSC), Program Executive Office for Manpower, Logistics and Business Solutions (PEO MLB), NABS, Product Manager Procurements, Recruiting, & Training Team.

The scope of this Performance Work Statement (PWS) covers the full range of PDSS for SPS; system maintenance and performance upgrade services, and software upgrades and patch Engineering Change Proposals (ECPs) and optional objectives if exercised. Services include program management, engineering and analysis, deployment, configuration management, quality assurance, risk management, service desk, system and database administration, cybersecurity, testing and evaluation, logistics, training, and audit support.

1.2 Background

As an integral part of the of the Department of Defense (DoD) Business Enterprise Architecture (BEA) Procure 2 Pay (P2P) business process, SPS is a joint program that supports the Contract Writing System for the DoD using a software application called Procurement Desktop Defense (PD2). The Joint Program Management Office (JPMO), part of the Defense Logistics Agency (DLA), is the lead service. The JPMO manages PD2 software development, which is a Commercial off the Shelf (COTS) product, and approves release through SPS Knowledge Base, a website managed through the software developer. Service Release (SR) 17b is the most current release of PD2 (released in 2019) with a SR18 upgrade scheduled to be released Spring 2022. Validation of JPMO released updates and testing with interface partners are conducted before applying updates to the Production system. While JPMO is responsible for the functional requirements, development and testing activities, the SPS PMO at MARCORSYSCOM manages deployment and sustainment of the application for USMC SPS users and provide support to Marine Corps contracting offices.

SPS is commonly referred to as SPS, SPS/PD2, PD2, and PD-squared. The term SPS will be used throughout this document.

SPS automates and standardizes the procurement process starting with receipt of the Purchase Request (PR) from the Defense Agencies Initiative (DAI) system through contract closeout. DAI was developed as an Enterprise Resource Planning (ERP) system to consolidate the automation of financial and administrative functions that are needed by multiple DoD agencies. DAI is a financial management initiative that transforms business and financial management processes and systems to provide accurate, reliable, and timely business information to support effective business decision making for agencies within the DoD. DAI supports the solution which provides best practices in financial management applied consistently across organizations within the DoD – compliant with the Department's BEA - including the Standard Financial Information Structure.

Previously, SPS did fall under the Paperless Acquisition (PA) Systems to include PR Builder and the Universal Interface (UI). In November 2021, PR Builder migrated to DAI.

The USMC uses SPS to support all contracting and interfaces with two (2) external systems: the UI and Navy ERP. Each Marine Corps Regional Contracting Office contains PD2 client workstations that connect to the SPS database server supporting their contracting office. Approved contracting actions are transmitted from SPS Adapters to the UI for transmission to the Global Exchange (GEX) and DAI. The UI, managed by the PR Builder Systems Integrator (SI), sends the SPS contract award eXtensible Markup Language (XML) files supporting the posting of accounting transactions to DAI via GEX. Procurement Data Standard (PDS) XML validations are also passed between SPS the UI and the GEX. Contract award post-script and index file pair transactions are transmitted to the GEX and are then sent to Electronic Document Access (EDA) as well as Wide Area Workflow which is part of the Procurement Integrated Enterprise Environment (PIEE). Contracting actions are reported from PD2 to the Federal Procurement Data System – Next Generation and vendor data is synchronized between PD2 and System for Award Management. Marine Logistics Group (MLG) contingency contracting elements utilize laptops with PD2 software called SPS-C, which is a stand-alone capability allowing Expeditionary Contracting Platoons use SPS-C while in a disconnected, austere environment.

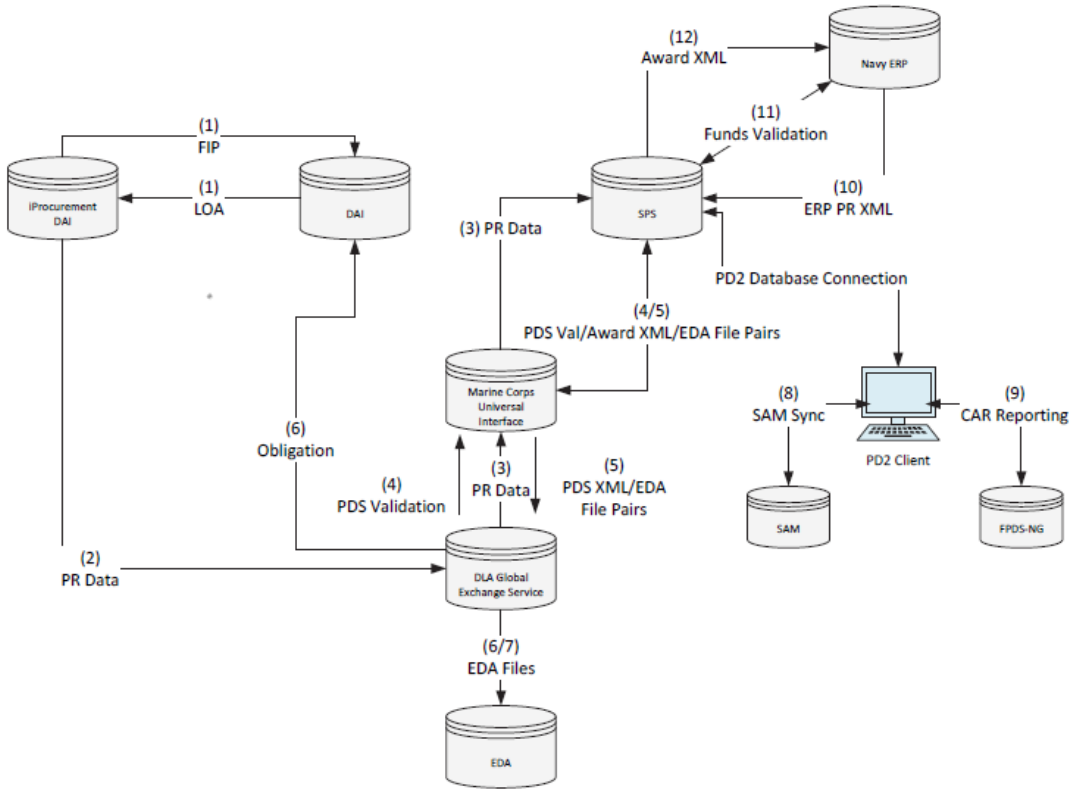
Currently, SPS is undergoing an ECP wherein a direct bilateral interface to the GEX is to be established. This requirement is in support of the DAI enterprise migration efforts per the Assistant Deputy Commandant, Installation & Logistics, Logistics Division dated 3 March 2021. Once this bilateral interface is fully operational, estimated 3rd Qtr FY22, SPS will transmit all contracts data through the GEX to DAI and fully disconnect from the UI.

SPS creates a high volume of annual transactions and is a critical part of annual budget execution. For example, in FY21, the Marine Corps generated over 8,300 contracting actions using SPS with a total expenditure of $3.4 billion in appropriated funds.

The SPS SI provides PDSS support to SPS, there is no PDSS requirement to make changes to the SPS source code or application, all required changes are completed at the JPMO level within DLA. The SPS Marine Corps PMO is responsible for the operation and management of the client-server architecture which consists of four (4) SPS server sites, ~30 SPS-C PD2 laptops, and providing support to an estimated ~550-600 SPS-MC users and SPS-C Expeditionary Contracting Platoons assigned to MLGs.

Department of the Navy (DoN) has an initiative that is replacing SPS. Per the Office of the Under Secretary of Defense, Acquisition & Sustainment Memorandum dated 07 May 2020, SPS is to be migrating to an enterprise Procurement System (ePS). Once migrated, it is anticipated that SPS will be minimally sustained for maximum three years. The activities will include ensuring the Cybersecurity posture is maintained and ensuring old documents are accessible.

Figure 1 depicts SPS High Level Architecture, while Table 3 below provides an overview of the system.



(1) System Handshake Between iProcurement and DAI- DAI returns LOA to iProcurement
- LOA inserted in PR
(2) iProcurement PR - PR transmitted from PR to GEX
(3) PR is transmitted to UI and SPS Adapter pulls PR and inserts it in applicable contracting office database
(4) Pre-Award Validation
-SPS send PDS Validation XML to UI
-UI transmits PDS Validation XML to GEX
-GEX returns validation document to UI → SPS
(5) Awarded Contract
- Award PDS XML transmitted to UI
- ASF server sends EDA idx & ps files to UI
(6) Obligation and EDA files
- Transmits PDS XML and file pairs to GEX
(7) EDA – Post files from GEX and provides management reports
(8) Contractor information Sync between SAM and PD2
(9) CAR reporting to FPDS-NG
(10) PR XML transmitted from Navy ERP to Quantico SPS Adapter then directly to SPS_M67400A_DB
(11) Funds Validation XML is transmitted to Navy ERP, validated and response returned by Navy ERP to SPS
(12) Award XML transmitted from SPS Adapter directly to Navy ERP

Acronyms

LOA	Line of Accounting
SABRS	Standard Accounting & Budget Reporting System
FIP	Financial Instrument Pointer
XML	eXtensible Markup Language
UI	Universal Interface
EDA	Electronic Document Access
UDF	Universal Disk Format
SAM	System for Award Management
FPDS-NG	Federal Procurement Data System – Next Generation
CAR	Contract Action Report
PDS	Procurement Data Standard
Idx	Index file format
Ps	Postscript file format
GEX	Global Exchange
ERP	Enterprise Resource Planning

Figure 1: SPS High Level Architecture

SPS System Overview			
Number of Servers	Three (3) (Virtual): • WebMethods Adapter • Application Server Framework (ASF) • Sybase Database	Hosting Environment	Marine Air Ground Task Force Information Technology Support Center (MITSC)-National Capital Region (NCR) (Quantico)
	Three (3) (Virtual): • WebMethods Adapter • Application Server Framework (ASF) • Sybase Database		MITSC-West (Camp Pendleton)
	Two (2) (Virtual): • WebMethods Adapter and Application Server Framework (ASF) • Sybase Database		MITSC-WestPac (Camp Foster, Okinawa)
	Four (4) (Virtual): • (2) WebMethods Adapters • Application Server Framework (ASF) • Sybase Database		Hybrid Cloud Services (HCS), Kansas City, MO
Interfaces to Other Systems	• UI • DAI • Navy ERP (Quantico and HCS only) • GEX (Future effort)	Environments	Production (3 MITSCs) Pre-Production (HCS)
Interface Transaction Rate Frequency	• UI – Real Time • Navy ERP – Real Time • GEX – Real Time/Near Real Time	Risk Management Framework (RMF) Confidentiality, Integrity, Availability Impact Level	Moderate, Moderate, Low
Storage Requirement	• Production – 1 Terabytes • Pre-Production/Beta – 1 Terabytes	Authority to Operate (ATO) Expiration Date	Reciprocity accreditation ATO through JPMO Expiration: 09/30/2023
System Software			
Operating System: Windows Server 2016			

SPS System Overview
Application Software: Microsoft Word, Procurement Desktop – Defense (PD^2), PD^2 Adapter, PD^2Application Server Framework, PD^2Document Transfer Utility, PD^2Archiving Utility, Cognos, Adobe Reader, PDS Extraction Utility, Web Methods
Database Software: SR17b - Sybase ASE 16.0 SP03 PL04; SR18 – Sybase ASE 16.0 SP03 PL09
System Development Language(s): Java JRE, JavaScript, .NET Framework
System Hardware
No hardware in SPS baseline: No hardware in SPS baseline; all servers are virtualized. SPS does have a requirement to support SPS-C laptops assigned to ECPs.

Table 1: Standard Procurement System Overview

1.3 Production Support System (PSS)

1.3.1 SPS

The SPS PSS Pre-Production is a virtualized instance of SPS that resides in HCS Data Center. The PSS system is used to conduct validation of JPMO released updates before applying these to the Production system and to conduct testing with interface partners. There is an instance at three of the Marine Corps' regional data centers located at Quantico, Virginia; Camp Pendleton, California; and Camp Butler, Okinawa Japan.

1.4 PMO Management Plans

Table 2 identifies the PMO Management Plans that provide overarching guidance for managed projects, now under NABS PMO. These documents form the foundation for the baseline for the PMO's common best business practices. Once formalized, NABS Management Plans will replace PM APPS Management Plans. Until that time, PM APPS Management Plans are still active and to be executed in the maintenance of projects.

Document / Reference	Intended Use
Systems Engineering Plan (SEP)	Describes the systems engineering approach for projects now under NABS PMO.
Configuration Management Plan (CMP)	Describes the processes the PMO follows to define, document, implement, account for and audit changes to requirements and baselines, supporting processes and documents for each of the projects in its portfolio.
System Test & Evaluation Strategy	Defines the Test & Evaluation approach for the PMO.
Performance Measurement Plan	Provides all managed projects with a framework for reporting a set of core and specialized metrics to baseline system element performance and report a standardized set of Key Performance Indicators to Stakeholders.

Document / Reference	Intended Use
Risk Management Plan (RMP)	Provide all managed projects with a framework to identify, assess and mitigate/escalate risks
Requirements Management Plan	Provide all managed projects with information on the systems engineering process to manage and control requirements changes. It is the process of documenting, analyzing, tracing, prioritizing, and agreeing upon all requirements received or generated, including technical/performance (non-functional) and operational (functional) requirements.

Table 2: PMO Management Plans

During the performance of this contract, the Contractor may be required to coordinate certain efforts with other Contractors hired by the Government to assist with program management support.

1.5 Contractor Performance

The contract shall be performed in accordance with (IAW) this PWS, the Government's Quality Assurance Surveillance Plan (QASP), and PMO Management Plans. Additionally, the contract shall be performed IAW the processes and standards in the Contractor's Post Deployment Software Support Plan (PDSSP) (P001), Project Management Plan (PMP) (P002), and Quality Assurance Program Plan (QAPP) (P003).

Post Deployment Software Support Plan (PDSSP) (Deliverable P001)

Project Management Plan (PMP) (Deliverable P002)

Quality Assurance Program Plan (QAPP) (Deliverable P003)

1.6 Objectives

The Contractor shall provide the SPS/PD2 with PDSS services, including migration efforts to an ePS, development and implementation of system enhancements and updates introduced by ECPs via the System Engineering Technical Review (SETR) process. In addition, the Contractor shall address system Cybersecurity issues and manage technical documentation identified as deliverables, including user guides and system manuals. The system is comprised of COTS software.

PDSS, system maintenance, and performance upgrades shall be performed, managed, and monitored to ensure that the Government's cost, schedule, and performance requirements are met. An integrated and defined set of project processes tailored from Capability Maturity Model Integration Level III equivalent or higher set of standard processes will be used in the performance of this effort.

SPS Service Desk shall be available Monday - Friday 0800 to 1630 Eastern Time (ET) for East Coast and Outside Continental United States (OCONUS) users; Monday – Friday 0800 to 1630 Pacific Time (PT) for West Coast users. Training and refresher training will be provided to SPS/PD2 users and SPS-C as required with approval from Contracting Officer Representative (COR).

Accurate and complete system documentation (configuration baselines, technical documentation, cyber security documentation, user documentation, etc.), updates, and any required assessments and authorizations shall precede the deployment of any capabilities, where available, in the Government SharePoint site.

2 Transition

2.1 Post Award Conference/Kick-off Meeting

The Contractor for this effort shall schedule and attend a post award conference with Government team within ten (10) days after contract award. No less than two (2) days prior to the meeting, the Contractor shall provide to the SPS Project Lead their proposed agenda, objectives and projected schedule to ensure seamless transition of duties with incumbent Contractor, SPS support team members and key Points of Contact (POCs) within Contractor leadership, and strategy and key goals to providing PDSS services.

To minimize any decrease in system operational availability and to prevent possible negative impacts on PDSS services, the Government will require a transition period where any incumbent and any incoming Contractors shall transition knowledge and understanding of SPS PDSS efforts and processes. The incoming Contractor will have transition responsibilities both as it transitions in as a new Contractor and if and when it transitions out and transfers support responsibilities to a replacement Contractor. References herein to responsibilities of any “incumbent Contractor” will also apply to the incoming Contractor if a new Contractor assumes responsibilities for performance when this effort ends. The Transition-Out period will occur at the end of the last option year.

2.2 Objectives of the Transition

The objectives of the transition period are to ensure the incoming Contractor is equipped with the knowledge and resources necessary to perform PDSS. This means that the incoming Contractor has a complete understanding of not only SPS but the P2P business process in order to commence performance of critical services at the end of the Transition period. The Government will require any incumbent Contractors to turn over all system documentation to the incoming Contractor for this effort. The incoming Contractor shall accept turnover of all system documentation. The Government will also require any incumbent Contractors to deliver to the Government all source code data, systems administration, and software development documentation; access to these materials by the incoming Contractor shall be coordinated with the Government.

2.3 System Knowledge Transfer

At a minimum, the incoming Contractor shall demonstrate an understanding of the following at the Transition Readiness Review: existing engineering and technical documentation, existing user documentation, and Contractor System Instantiation.

The incoming Contractor shall have the capability to conduct defect management, which includes the ability to replicate system failures, test software patches prior to production release, and test system development efforts. At a minimum, Contractor System Instantiation includes:

2.4 Production System Software

A current copy of the production system software, including source code, will be provided as part of the transition process to support PDSS activities and instantiation of a production representative system.

System / Software Source Code (Deliverable P019)

2.5 Transition-Out Period

In the event a follow-on contract is awarded, the Government may elect to exercise the Optional Transition-Out CLIN. In support of this CLIN, the Contractor shall engage in the following transition activities with the incoming Contractor:

2.5.1 Baseline.

2.5.1.1 The incumbent Contractor shall baseline the system and system documentation.

2.5.1.2 Baseline activities shall, at a minimum, consist of the following:

2.5.1.3 Physical Configuration Audit (PCA) or validation of the PCA deltas.

2.5.1.4 The incumbent Contractor shall support the Government PCA IAW MCSC Technical Review (TR) Handbook v1-04, and all PMO Management Plans in Table 2.

2.5.1.5 Closure of all critical Action Items or critical Requests for Action (RFA).

2.5.1.6 Baseline documentation shall, at a minimum, consist of the following:

2.5.1.6.1.1 Configuration Item Technical Database (CITDB). The CITDB is the Government's tool for the management of the product baseline.

2.5.1.6.1.2 All deliverables as identified in the system CITDB, system contract, and PWS.

2.5.1.6.1.3 When applicable, regression test driver codes and test scripts, test data, and benchmark results matched to software release version number.

2.5.1.6.1.4 Government data in Contractor licensed tools.

2.5.1.7 The incumbent Contractor shall transfer, to the Government, ownership of all hardware

and software items that were purchased by the incumbent contractor on behalf of the Government. The transfer process shall include re-registering all hardware and software components as PEO MLB NABS.

2.5.1.8 The incumbent Contractor shall implement all applicable Information Assurance Vulnerability Alert (IAVA) patches, as well as Government funded ECPs. Open IAVA patches and ECPs designated in the Transition Readiness Review will be the responsibility of the incoming Contractor. The incumbent Contractor shall update the system cyber security Plan of Action and Milestones (POA&M) with all of the applied patches and ECPs.

2.5.1.9 Assist incoming Contractor with getting required access to support SPS; for example, administrator user Identification (IDs) and passwords, database user IDs and passwords, and all system interfaces.

2.5.1.10 Provide incoming Contractor with all established and current POCs and Stakeholders, to include phone number and email address for the system Stakeholders, programmatic and technical POCs for interfacing system(s), and POCs for current hardware and software maintenance agreements.

2.5.1.11 Provide up to five (5) days of allowing incoming Contractor to observe the incumbent Contractor during the conduct of system maintenance and administration during regular business hours, i.e. 0800 - 1700. Days can be, but are not required to be consecutive. One (1) day is equivalent to a minimum of eight (8) hours, not including lunch.

2.5.1.12 Provide up to five (5) days of incumbent Contractor observing the incoming Contractor during the conduct of system maintenance and administration during regular business operations, i.e. 0800 - 1700. Days can be, but are not required to be consecutive. One (1) day is equivalent to a minimum of eight (8) hours, not including lunch.

2.5.1.13 Attend up to five (5) days of working sessions, meetings or both with the incoming Contractor to facilitate knowledge transfer on system functionality, to include existing automated and manual interfaces. Days can be, but are not required to be consecutive. One (1) day is equivalent to a minimum of eight (8) hours, not including lunch.

2.5.1.14 Allow incoming Contractor access to all system hardware and software within the ATO boundary or Government owned equipment for inspection and audit. The incumbent Contractor shall clarify any discrepancies in hardware and software assets.

2.5.1.15 The incumbent Contractor shall assist the incoming Contractor in preparing for and holding a Transition Readiness Review to support the transition of responsibilities to the incoming Contractor.

Closeout Report (Deliverable P023)

3 PDSS and ECPs

The Contractor shall execute and manage their service support, service delivery, and sustainment logistics IAW the submitted PDSSP. The Contractor shall provide updates to the PDSSP as needed or as directed by the Government. (P001)

The Contractor shall provide a PDSS Support Schedule that shows the anticipated activities the Contractor plans to perform in executing PDSS.

ECPs impact the system baseline and are governed by the ECP process as defined in the PMO Management Plans, SEP and CMP. ECPs are designated with Integer levels defined by the Government. 1st, 2nd and 3rd integer changes are optional Contract Line Item Numbers (CLINs) and will only be exercised if a respective release is required and funding is available. The Contractor shall implement all required 2nd and 3rd integer software upgrades and 4th integer patch release changes as part of the base and optional PDSS awards.

The CLINs will identify the required number of ECPs in optional, separate CLINS for each ECP category and year of expected work in the contract. While the specific description of work for each ECP will be determined at the time of option exercise, each ECP is expected to fit into one of the categories below. Each exercised ECP will be considered Firm Fixed Price for a specific outcome defined at option exercise.

ECP Category	**Category Description**	**Estimated Hours of completion**
ECP I	Maintenance Release	1000 Hours
ECP II	Maintenance Release	1500 Hours
ECP III	Minor Release	2000 Hours

Table 3: ECP Categories (Optional)

3.1 Integer Definitions:

Integer Change	X.0.0.0	1.X.0.0	1.2.X.0	1.2.3.X
Release Definition	-Major Release -A system change driven by changes in capabilities -Can be predicated by a formal requirements documents from the capabilities sponsor. (e.g. SON,CPD,UNS)	- Minor Release. - A significant change driven by enhancement or multiple hardware and/or software upgrades	- Maintenance Release - Change driven by limited enhancements, a hardware / software refresh, or bug fix	- Patch Release - No change to baselines - Documentation update or security vulnerability (e.g. IAVA/IAVB patches)
System Version Definition	- Initial System release - Capability change - Advances in number as additional program/ system level baselines emerge - Changes to an underlying DB engine or operating system change that introduces a new capability - Functional addition(s) that did not previously	- System update - New features - Improves functionality/capability and is within the approved baseline functionality/capability - New features - Database engine operating system change that does not introduce a new capability or add	- Updates without functional additions proposed to resolve known bug fixes/ issues, plug-in packages, patches - Improvements to stability and usability	- Incorporation of site or application specific files or data - SW changes due to IAVA compliance. - Device driver (new/updates) - SW configuration updates - SW corrections found during 1st/2nd digit testing to meet design requirements

Table 4: Release Definition

3.2 Service Desk

The SPS Service Desk is the front facing customer point of contact for worldwide user support. On average, the Service Desk processes more than 200 service requests each month for the SPS. The Service Desk shall be responsible for managing all web, email, phone, voicemail, and ticketing system submitted customer inquiries from receipt to resolution using Government approved tools and ticketing systems such as Remedy. The Contractor shall operate the Service Desk by employing industry best practices. At minimum the contractor shall adhere to the following subsections:

3.2.1 Manage the Service Desk, which is the single point-of-contact for users requesting support and for the reporting of incidents. The Contractor is responsible for the following Service Desk functions:

3.2.2 Disseminating information regarding planned outages or incidents impacting production services.

3.2.3 Providing information to users regarding the status and closure of their respective service requests.

3.2.4 At minimum, resolve 95% of system access issue Service Desk requests in the first call using the Remedy ticketing system.

3.2.5 Upon closure of service requests, the Service Desk shall solicit user feedback regarding the quality of service provided by the Service Desk

3.2.6 Resolving system access issues.

3.2.7 At a minimum, the Service Desk shall provide and consist of the following:

System	Service Desk Tiers Required	Hours of Operation
SPS/PD2 National Capital Region (NCR); Camp Pendleton (West Region); Okinawa	I, II, III	0800-1630 ET/PT; Monday-Friday; Excludes Federal holidays
SPS/PD2 (All other locations)	II, III	0800-1630 ET/PT; Monday-Friday; Excludes Federal holidays
SPS-C	I, II, III	0800-1630 ET; Monday-Friday; Excludes Federal holidays

Table 5: Service Desk Requirements

3.2.7.1 Provide Tier 1 Service Desk support to users worldwide, with onsite support provided to users in Camp Pendleton and NCR. The Service Desk shall be available Monday - Friday 0800 to 1630 ET for East Coast and OCONUS users; Monday – Friday 0800 to 1630 PT for West Coast users.

3.2.7.2 Tier 1 support shall provide first contact support to users and be capable of resolving basic system access issues such as password resets, routing documents, and assisting in end user account management and basic system functions.

3.2.7.3 Tier 1 shall collect information, to include: the caller's name; organization; work location; time of receipt of the call; the nature of the call; the time of resolution; and a brief statement of how the problem was resolved to record each user's Service request/trouble call. The Contractor has the ability to add data it feels is needed to improve its ability to manage service requests.

3.2.7.4 Conduct, track, and monitor the resolution process. This includes capturing, tracking, investigating, escalating, resolving, closing, and reporting user Service requests.

3.2.7.5 Make every effort to resolve Service Desk requests in an expedient manner at the lower Tier support level. However, Tier 1 Service requests shall be elevated to Tier 2 if not resolved within four (4) hours or requires Tier 2 assistance in more advanced system level trouble shooting. Tier 2 support serves as the first level of escalation from Tier 1 and provides more advanced user support including User Administrator issues and basic reporting.

3.2.7.6 Tier 3 support involves escalation to program developers and advanced system administrators to provide support such as advanced reporting, manual database changes, and advanced user support. If Tier 3 support cannot identify a solution within 48 hours of a ticket's creation, the Government Program Office will be notified and a new Change Request/ECP will be created and maintained in the ECP Government approved tracking tool (i.e., SharePoint). (Note: A Common Access Card (CAC) is required to access)

3.2.7.7 Document and maintain answers for common support requests.

3.2.7.8 Provide a bi-weekly Customer Support Update during the IPT and provide updates as part of the Monthly Status Report (MSR).

3.2.7.9 Provide metrics of all Service Desk tickets on a monthly basis that covers all Service Desk calls and tickets from preceding month.

Monthly Status Report (MSR) (Deliverable P006)

Service Desk Metrics (Deliverable P026)

3.3 Incident Management

The primary focus of Incident Management is the restoration of services following an incident. Incident Management is primarily a reactive process; its processes provide guidance on diagnostic and escalation procedures required to quickly restore services. Incident Management processes are closely integrated with Service Desk, problem management, and change management processes. At minimum the contractor shall adhere to the following subsections:

3.3.1 Provide an Incident and Problem Management Plan (P004) that details the processes on diagnostic and escalation procedures required to quickly restore services.

Incident and Problem Management Plan (Deliverable P004)

3.3.2 Detect and record incident details.

3.3.3 Perform incident management including performance monitoring, incident identification, diagnosis, isolating, containment, eradication, recovery, and lessons learned.

3.3.4 Track incidents reported from the users, the host site, and external interfacing systems.

3.3.5 Ensure all availability issues are communicated to the Government team within fifteen minutes of discovery.

3.3.6 Prioritize incidents in terms of impact and urgency with the objective to minimize user impact.

3.3.7 Assess type and severity (e.g., number of users effected) of incident.

3.3.8 Identify incident impact to the Government.

3.3.9 Recommend ratings for the priority and the urgency of each incident.

3.3.10 Inform the Government of the restoration of services and effects of the incident to the user community.

3.3.11 Immediately escalate incidents that require expertise not available in the currently assigned Tier.

3.3.12 Provide Service Desk verification that the incident is closed, and the user is satisfied with the solution.

3.4 Problem Management

The primary focus of Problem Management is to identify the causes of service issues and conduct corrective work to prevent recurrences. Problem Management processes are reactive in responding to incidents and proactive in identifying and preventing future incidents. Ensure that the Contractor's processes are closely integrated with Incident Management, Change Management, and Availability Management. Although Availability Management performs the lead role in component failure and system outage analyses, Problem Management performs an important role in obtaining data and analyzing data in support of the analyses. At a minimum, the Contractor shall adhere to the following subsections:

Incident and Problem Management Plan (Deliverable P004)

3.4.1 Record, manage and escalate service problems as appropriate.

3.4.1.1 Record the escalation, progress status, and final resolution in the established trouble ticketing system.

3.4.1.2 Make every attempt to resolve the service issue at the Tier II level.

3.4.1.3 Escalate the service problem to the Tier III level for resolution if it cannot be resolved at Tier II within 24 hours.

3.4.1.4 Report a summary of service issues in the MSR (P006). Summary information to include how the issue was initially identified, what system service(s) were affected, how long it took to restore service(s), and lessons learned.

Monthly Status Report (MSR) (Deliverable P006)

3.4.1.5 Analyze historical data to support predictive analysis to eliminate potential incidents before they occur and to identify workarounds. At minimum the Contractor shall adhere to the following subsections:

3.4.1.6 Maintain historical data in a Government approved format for all service problems.

3.4.1.7 Use a trouble ticket log to develop an analysis of trends to identify potential problems.

3.4.1.8 Provide the Government the results of problem trends in the MSR (P006)

Monthly Status Report (Deliverable P006)

3.4.1.9 Diagnose root cause and eliminate recurrences.

3.4.1.10 Provide the Government the potential causes of problems in its historical data.

3.4.1.11 Using historical data, provide the Government with the Contractor's approach for preventing problems from recurring.

3.4.1.12 Prioritize problems, in terms of impact and urgency, to minimize system user impact.

3.4.1.13 Assess and provide type and severity (e.g., number of users affected) of problem.

3.4.1.14 Assess and provide impact to data integrity.

3.4.1.15 Reduce unplanned downtime hours.

3.4.1.16 Identify problem impacts to the Government.

3.4.1.17 Recommend the priority and the urgency to be assigned to each problem.

3.4.1.18 Inform the Government of the restoration of services and effects of the incident to the user community.

3.4.1.19 Develop workarounds or other solutions to incidents.

3.4.1.20 Identify potential problems from the analysis of historical data.

3.4.1.21 Develop innovative workarounds and solutions to problems.

3.4.1.22 Present workarounds to the Government for consideration and approval for implementing an ECP.

3.4.1.23 Identify, develop and submit ECPs to Configuration Control Board (CCB) to eliminate known problems.

3.5 Configuration Management

3.5.1 Configuration Management (CM) processes guide the collecting, archiving, and reporting of individual infrastructure component specifications. The CITDB is the single repository of configuration information. In addition to Configuration Item (CI) information, the database contains information regarding the relationships and dependencies among infrastructure components. CM databases are also used by Capacity Management, Availability Management, and IT Service Continuity Management processes to accurately perform their work.

3.5.2 The Government seeks a CM environment that will ensure the baselines are maintained and that only controlled changes are implemented. The Contractor shall implement a CM program and develop and deliver a CMP (P007) that will align with the PMO CMP, in order to provide the basis for performing and managing CM activities for SPS. At minimum the Contractor shall adhere to the following subsections:

Configuration Management Plan (CMP) (Deliverable P007)

3.5.2.1 Maintain the CITDB utilizing the approved PMO CITDB format.

3.5.2.2 Maintain the current database containing the details of each system component. CI contained within the CITDB to include Hardware, Software, Interfaces, Trace links and Documentation. (Note: CAC is required to access the CITDB).

3.5.2.3 Identify new CIs and enter them into the CITDB.

3.5.2.4 Provide identification, collection, tracking, and maintenance of each unique CI comprising the system and sub-systems.

3.5.2.5 Perform change control processes that enable definition of the functional and physical characteristics of CIs in sufficient detail that they may be categorized.

3.5.2.6 Enable and implement the identification of the system items, components, and related work products that will be placed under CM.

3.5.2.7 Record, track, and maintain Government submitted CIs in the CITDB.

3.5.2.8 Propose CIs which the Contractor deems necessary or offer significant benefits to the Government.

3.5.2.9 Establish and implement configuration control and approval processes required to change a CI's attributes and re-baseline the CIs.

3.6 Change Management

3.6.1 Change Management assesses risks of individual changes, uses configuration information to identify dependencies and other impacted applications and systems, and after analyzing the information, authorizes or denies change requests. The goal of Change Management is to identify application code, functional and performance defects, and intercept them

before users are impacted.

3.6.2 SPS infrastructure instances are located at three different sites: Marine Corps Base (MCB) Quantico, MCB Camp Pendleton, and MCB Butler in Okinawa, Japan; with Zone A test environment hosted at HCS. Assessment of changes to the infrastructure requires coordination between the host site, the user community, MARCORSYSCOM, Marine Corps Cyberspace Operations Group, and the Contractor. At minimum the Contractor shall adhere to the following subsections:

3.6.3 Prepare written system change approaches, estimated costs, and schedules for the Engineering Review Board (ERB) and CCB. The authoritative source of all system ECPs is the Government's ECP Tracker System. (Note: A CAC is required to access the ECP Tracker System). The Contractor may propose changes but must receive approval from the CCB and written direction from the Contracting Officer to execute ECPs.

3.6.4 Provide and ensure that its change management processes align with the PMO Management Plans listed in Table 2.

3.6.5 Contribute and record decisions and updates to any relevant products in SETR events, Functional Review Boards, ERBs, CCBs, and all RFAs. The Contractor shall ensure that all RFAs are adjudicated.

3.6.6 Perform ECP assessments for risk, complexity, and potential user benefits.

3.6.7 Maintain and update CIs and data elements in the Government's ECP Tracker System.

3.6.8 Provide an estimate, which will include labor categories and specific life cycle hours for ECPs at the ERB. Provide a Rough Order of Magnitude (ROM), which will include labor categories and specific number of labor hours per category for those ECPs presented to the CCB for approval.

3.6.9 Identify application code defects as well as functional and performance defects received from service desk escalation and problem management, and submit ECPs as appropriate.

3.6.10 Identify and resolve the defect and ensure the system is working as designed.

3.6.11 Use quality assurance processes to reduce software defects.

3.6.12 Utilize software development processes to reduce software defects.

3.7 Release Management

3.7.1 Release Management is closely integrated with Change Management. Release Management manages changes to the environment such as installing vulnerability patches, software changes, and refreshing technology. At minimum the Contractor shall adhere to the following subsections:

3.7.1.1 Perform all technical and non-technical aspects of a release in accordance with the PMO SEP and MCSC SETR Handbook, including the update and maintenance of system baselines, system documentation, Version Description Document (VDD) (P008), user documentation, training documentation, and supply support materials for TRs.

Version Description Document (VDD) (Deliverable P008)

3.7.1.2 Provide technical aspects such as: regression testing; testing documentation; remediation of identified defects; the update of system documentation, configuration status, and accounting data; and information assurance system scanning.

3.7.1.3 Provide non-technical aspects such as: coordinating system changes with the host facility; identifying the needed training; updating user documentation including training documentation; and preparing release notes and VDD.

3.7.1.4 Plan and support the successful roll-out of software and related hardware including the required Contractor Test and Evaluation and Government Acceptance Testing (GAT) processes.

3.7.1.5 Provide a repeatable training, test, and deployment strategy and schedule for planned enhancements and upgrades.

3.7.1.6 Create and deliver Test Plans, Test Scripts, and Scorecards (P009 and P010) that are traceable to requirements.

GAT Scorecard (Deliverable P009)

Test Report and Defects (Deliverable P010)

3.7.1.7 Monitor GAT and collect Test Incident Reports (TIRs).

3.7.1.8 Create and deliver Developmental Testing Scorecards reflecting all completed test scripts, remaining test scripts, number passed, number failed, and status of failed tests.

3.7.1.9 Resolve all Severity 1 (Showstopper) and 2 (High) TIRs and other critical issues and update system documentation prior to test completion.

3.7.1.10 Manage, integrate, and deploy upgrades upon Government acceptance (including production environment regression testing).

3.7.1.11 Schedule releases in coordination with the Government Program Office to determine optimal release window to minimize impact to end users.

3.7.1.12 Design, implement, and support efficient procedures for the distribution, installation, and verification of changes including the client application.

3.7.1.13 Coordinate with and prepare the Stakeholders and system user community for new release capabilities.

3.7.1.14 Ensure implementations are traceable, secure, and that only correct, authorized, and tested versions are installed.

3.7.1.15 Coordinate and plan releases IAW Change Management processes.

3.7.1.16 Provide master copies of all software and update the CITDB.

3.7.1.17 Document release plans in a Release Deployment Plan (P011) that at a minimum contains anticipated changes to be deployed (e.g., vulnerability patches, software upgrades, defect patches), POA&M leading up to deployment, CIs that need to be updated (e.g., technical documentation, System Maintenance and System Administration Manual (P012), CITDB, and a Contingency Plan.

Release Deployment Plan (Deliverable P011)

System Maintenance and System Administration Manuals (Deliverable P012)

3.7.1.18 Support and participate in the Government Post Implementation Review (PIR) IAW PMO Management Plans.

3.7.1.19 SPS does implement a 4th Qtr moratorium for system changes. No changes, including patch management, shall be conducted during the 4th Qtr of each FY.

3.8 Cybersecurity Management

3.8.1 The objective of Cybersecurity / Information Security Management is to protect Marine Corps critical information from internal and external threats and attacks, while ensuring the confidentiality, integrity, and availability of information.

3.8.2 SPS is augmented by select Information Technology (IT) controls as described in the Cybersecurity Workforce Guide. The RMF Levels for SPS are Moderate, Moderate, Low as described in Department of Defense Instructions (DoDI) 8500.01 RMF for Defense IT Systems).

3.8.3 To achieve cybersecurity objectives, the Contractor shall adhere to the requirements of Marine Corps Order (MCO) 5239.2B and DODI 8510.01 as appropriate for SPS. The Contractor shall have knowledge of and support all Assessment and Authorization (A&A) activities throughout the system lifecycle IAW the latest releases or revisions of the cybersecurity policies. At minimum the Contractor shall adhere to the following subsections:

3.8.3.1 Maintain the system's ATO, review and update documentation (including, but not limited to, the Systems Security Plan (SSP) and the RMF for DoD IT), and fulfill all annual cybersecurity requirements for a low, moderate, low impact for SPS.

3.8.3.2 Maintain and report the systems' A&A status and issues.

3.8.3.3 Ensure the SSP is developed and maintained for assigned systems.

3.8.3.4 Conduct the continuous monitoring of assigned systems and provide continuous monitoring artifacts and checklists.

3.8.3.5 Conduct scan reviews (to include, but not limited to, Assured Compliance Assessment Solution (ACAS) and Security Content Automation Protocol (SCAP)) and conduct any manual Security Technical Implementation Guide (STIG) checklist items any time the system changes.

3.8.3.6 Ensure all DoD information system Cybersecurity-related documentation is current and accessible to properly authorized individuals.

3.8.3.7 Conduct automated static code review scans prior to delivery and implementation in production for any system code changes. The Contractor shall ensure static code review findings are remediated prior to delivery to the Government.

3.8.3.8 Provide awareness and prevention of cybersecurity risk through assessment and implementation of best practices (code reviews, system scans, vulnerability alerts, Contractor notifications, and STIGs.

3.8.3.9 Facilitate, participate in, and provide timely completion of Annual Security Reviews, Annual Security Control testing, Annual Contingency Plan testing, and Quarterly update and submission of POA&M updates in compliance with the Federal Information Security Management Act (FISMA).

3.8.3.10 Use the Government's Cybersecurity tool, Marine Corps Certification and Accreditation Support Tool (MCCAST), to submit, maintain, and review A&A documentation and workflow. The Government will assist in gaining access to the tool, as well as training for the tool.

3.8.3.11 Work with the Government engineering team to register any software implemented on the systems for Marine Corps use in Department of the Navy Application and Database Management System (DADMS) prior to any system upgrade. The Contractor shall complete and submit DADMS questionnaire as required.

3.8.3.12 Facilitate the protection of United States Government sensitive unclassified and classified information by working closely with the Government Information Systems Security Manager (ISSM), Information Systems Security Officer, and staff.

3.8.3.13 Implement vulnerability assessment remediation, tracking, and report per IAVA, Information Assurance Vulnerability Bulletins (IAVB), Information Assurance Vulnerability Management (IAVM), and Operational Directives (OPDIRs).

3.8.3.14 Ensure annual Cybersecurity awareness training, located on MarineNet (Government provided access), is completed once a year. Report status of compliance to the Government.

3.8.3.15 Review vulnerability assessment scans, provide technical guidance on remediation

(including use of STIGS), and develop POA&Ms.

3.8.3.16 Conduct cybersecurity risk analysis to include identification and mitigation of cybersecurity risks to COTS software.

3.8.3.17 Fully support Command Cyber Readiness Inspection events. This includes the review of systems security documentation, performance of pre-assessment scans, testing and application of patches to software and operating systems, review of vulnerability scan results, evaluation of test results, preparation and review of POA&Ms, and remediation of findings.

3.8.3.18 Provide and update the Cybersecurity Integrated Master Schedule (IMS) on a monthly basis.

Cybersecurity IMS (Deliverable P024)

3.8.3.19 Provide and update Cybersecurity Action Tracker on a biweekly basis.

Cybersecurity Action Tracker (Deliverable P025)

3.9 Service Delivery

Service Delivery processes assist in the identification of delivered or provided services, tailoring of services, and the timely provision of services, resources, capabilities, and capacities to meet SPS needs.

3.9.1 Service Level Management (SLM) processes provide a framework by which services are defined, levels of service required to support business processes agreed upon, and SLAs developed to satisfy the agreements. SLM processes can clearly define IT and business roles and responsibilities and establish clear goals for service delivery so success factors can be established, measured, and reported. At minimum the Contractor shall adhere to the following subsections:

3.9.2 Manage and provide system performance in support of SLAs, Interface Control Documents (ICDs), System Interface Agreements (SIAs), and/or Interface Control Agreements (ICAs).

3.9.3 Support the Government's development and maintenance of SLAs, ICDs, SIAs, and/or ICAs for new interfaces as required.

3.9.4 Plan for changes to SLAs, ICDs, SIAs, and/or ICAs when there is a change to the system or external interfacing systems.

3.9.5 Manage and provide performance of system interfaces including web services.

3.9.6 Measure performance, report results as part of the MSR.

Monthly Status Report (MSR) (Deliverable P006)

3.9.7 Perform the Contractor role and responsibilities per approved SLAs, ICDs, SIAs, and/or ICAs and participate in the update of respective document as needed

3.10 Data Interfaces, Transfers and Exchanges

SPS planning and execution functions are designed to interface with external data sources to either obtain data, translate data, or a combination of both, as needed to perform the necessary job function. The Interface Agreement documents are established for each application interface to define the automated interface and the specific data and data formats to be exchanged. Interfaces will be maintained in the Government owned CITDB and presented in the System/Subsystem Design Description as defined in the Marine Corps SETR Handbook.

Number	Interface Transaction	Interface Frequency	Interface Description
1	Application Advice	Upon failure of SPS XPR	Upon a failed delivery of the SPS xProc document, a PD2 adapter will push a PD2 App Advice XML to UI, which contains the reason for the failure. The document is posted to Trading Networks and DAI is updated with the reason for the failure.
2	Award and Award Modifications	Real time	PD2 Award and Award Modifications XMLs are pushed to the UI from a PD2 Adapter. The Award/Award Modification is locally published in Trading Networks. Information is extracted from the award to form three other file types: PDS Award, GEX/EDA Award, and DAI obligation. Those files are posted to Trading Networks and pushed to their respective Trading Partners (GEX/EDA). DAI is updated with information from the Award/Modification.
3	Contract Closeout Notifications	Real time	A DD1594 XML is pushed to the UI from a PD2 Adapter. The file is posted in Trading Networks and pushed to the Trading Partner GEX/EDA. A DD1594 XML is

			pushed to the UI from PIEE via the GEX to a PD2 Adapter. The file is posted in Trading Networks and pushed to the SPS PD2 Adapter.
4	PD2 Pre-Release Award and Award Modifications	Sixty second intervals	PD2 Pre-Release Award and Modification XMLs are pushed to the UI from a PD2 Adapter. The Pre-Release Award/Award Modification is locally published in Trading Networks. Information is extracted from the award to form another file type: Pre-Release Award PDS. These files are posted to Trading Networks and pushed to the GEX. A response is received synchronously from GEX as a Validation Response and pushed back to SPS.
5	PR Award Status	Hourly	PD2 Adapters run an extraction of award status updates of PRs and Awards every sixty seconds if there is a status available. The information is extracted into a PD2 PrAwardStatus XML and that data is pushed to the UI. The XML is posted in Trading Networks and the respective documents' statuses are updated in DAI.
6	Transfer Documents	Five minute intervals	A PS-IDX file pair or an attachment are pushed to the UI from a PD2 Adapter. The file pair or attachment is locally published in Trading Networks. These files are then posted to the GEX.

Table 6: SPS External Interface with UI

3.11 Continuity Management

3.11.1 IT Service Continuity Management provides a framework for developing IT infrastructure recovery plans in support of business continuity management. The Contingency Plan

outlines the roles, responsibilities and processes to be enacted in the case of circumstances preventing the continuity of the system. Ensure RMF Confidentiality, Integrity, and Availability impact levels for SPS meet the availability thresholds expectation following a downing event. In addition, the system has a Recovery Point Objective of 24 hours and a Recovery Time Objective of 72 hours. Information regarding system recovery plans is found in MCCAST.

3.11.2 Maintain a system recovery plan that meets with Government approval.

3.11.3 Conduct risk assessment of IT services to identify the assets, threats, vulnerabilities and countermeasures for each service as part of the RMP.

3.11.4 Evaluate options for recovery.

3.11.5 Conduct risk assessments in conjunction with Cybersecurity Management on a scheduled basis.

3.11.6 Identify and notify the Government of threats and vulnerabilities upon completion of the risk assessments as identified in the system recovery plan.

3.11.7 In the Risk Mitigation Plan, provide the Government with risk mitigation strategies for identified program risks. Monitor processes and include in the MSR an evaluation of the impact of mitigation efforts and the effectiveness of risk mitigation strategies.

Monthly Status Report (MSR) (Deliverable P006)

3.11.8 Review and revise the continuity section within the System Maintenance and System Administration Manuals (P012) as needed.

3.11.9 Utilize the results of the Government approved test in Cybersecurity as required by the DoDI 8500.2 and provide corrective actions for analysis to the Government.

3.12 Capacity Management

3.12.1 The Contractor shall be responsible for ensuring that IT infrastructure resources are in place or available to satisfy planned needs and that those infrastructure assets are effectively used. The Contractor shall be responsible for ensuring that Random Access Memory, Compute, and Storage are in place to ensure effective operations of the system. Where deficiencies are identified, the Contractor shall submit tickets to have the capacity increased / decreased where necessary. At a minimum, the Contractor shall:

3.12.1.1 Monitor the performance and throughput of the system.

3.12.1.2 Perform analysis of measurement data, including analysis of the impact of new releases on capacity and system performance. Provide the evaluation of the analysis in the MSR.

Monthly Status Report (MSR) (Deliverable P006)

3.12.1.3 Conduct performance analysis and monitoring activities to facilitate performance tuning activities and to ensure the most efficient use of existing IT resources.

3.12.1.4 Monitor the demands on the system and future plans for growth or reduction.

3.12.1.5 Respond when performance falls below acceptable performance levels.

3.12.1.6 Analyze demand on current computing resources and propose recommended change requests to the Government to meet current and future needs.

3.12.1.7 Submit change proposals in support of modifications to system resources to meet user demand.

3.12.1.8 Identify system software and network capacity and capability requirement thresholds in order to sustain system usability and maintainability levels.

3.12.1.9 Conduct risk assessment of infrastructure and planned capacity needs to be integrated into the Contractor's overall risk management process.

3.12.1.10 Integrate Capacity Management information within the Contractor risk processes.

3.12.1.11 Provide the Government with results of risk assessments in the MSR.

Monthly Status Report (MSR) (Deliverable P006)

3.13 Availability Management

3.13.1 Availability Management is responsible for ensuring application systems are up and available. The process ensures Government system availability requirements are being achieved and ensures the most cost-effective contingency plans are put in place and tested on a regular basis to ensure Government availability needs are met. Availability Management also provides a lead role in the Failure Reporting and Corrective Action System (FRACAS) (P016).

FRACAS (DELIVERABLE P016)

3.13.2 SPS has a Production requirement for 98% Ao based on an operational time of 24/7/365. In addition, based on the systems' ATO designation, the SPS applications must be available within five days after an outage. Pre-production and Training Environments must be operational when needed to support a particular event. At minimum the Contractor shall adhere to the following subsections:

3.13.2.1 Provide service (system) availability that meets user's expectations.

3.13.2.2 Maintain system operational availability at 98%.

3.13.2.3 After award, within the Systems Maintenance Plan and Administration Manual, prepare

and provide for planned outages and restoration after an unplanned outage.

3.13.2.4 Identify potential service availability issues.

3.13.2.5 Integrate information from other areas of the PWS effort to create a higher-level of understanding of potential availability issues.

3.13.2.6 Provide recommended resolutions to the Government.

3.13.2.7 Provide FRACAS (Deliverable P016): the examination of past outages to identify related CIs, the CI's impact on availability, and future corrective action(s).

FRACAS (Deliverable P016)

3.13.2.8 Collect outage data, rank the outages, determine causes, and provide resolutions to either eliminate or reduce outage frequency.

3.13.2.9 Escalate problematic CIs and recommended resolutions to the Government.

3.13.2.10 Provide Obsolescence Management. Comprehensive obsolescence management should integrate processes, methods, and procedures to ensure that products can be supported over their complete lifetime.

3.13.2.11 Conduct system maintenance IAW the System Maintenance and System Administration Manual.

3.13.2.12 Maintain the System Maintenance Plan. The System Maintenance Plan shall identify and ensure system software is maintained IAW manufacturer specifications. If manufacturer specifications do not exist, the Contractor shall perform maintenance in accordance with industry best practices.

3.13.2.13 Support the technical requirements of the System Maintenance Plan during the lifecycle of the system.

3.13.2.14 Support the maintenance of all software required for the system. This includes all technology refreshes, software upgrades, patch releases, and maintenance releases as defined in the PMO CMP 3rd and 4th integer changes.

3.14 Sustainment Logistics

Sustainment logistics requirements focus on lifecycle supportability. At minimum the Contractor shall adhere to the following subsections:

3.14.1 Ensure the CITDB is maintained, this includes documenting the location, condition, and ownership of all GFE provided by this contract.

3.14.2 Maintain and update all logistical data elements within the CITDB.

3.14.3 Develop and maintain a comprehensive Hardware and Software Refresh Plan (P017) in the Government provided format. The plan shall cover a rolling five-year period for assets.

Software / Hardware Refresh Plan (Deliverable P017)

3.14.4 Track the lifecycle of hardware, software, warranties, and licenses; notify the Government PMO at least 180 days prior to any expiration date. The Contractor shall notify the Government PMO of announced product end of life, loss or impending loss of manufacturers of items or suppliers of items or raw materials date, expiring warranty, or software sun setting. The Contractor shall provide recommendations for upgrades or migrations to mitigate obsolescence issues.

3.14.5 Provide a monthly status in the MSR that includes expirations of licenses and warranties at intervals of 30, 60, 90, 120, and 180 days and recommended action plans. Assessments should at minimum include the following elements:

- Alternatives sources, parts, and materials
- Implementation costs
- Source data to support forecasting of obsolescence risks

Monthly Status Report (MSR) (Deliverable P006)

3.14.6 Assist the Government in disposal and disposition of assets.

3.14.7 Provide planned/un-planned outage data to satisfy external reporting requirements/taskers.

3.15 Sustainment and Difference Training

The Contractor shall provide a plan to develop and deploy an innovative solution that provides SPS users sustainment and difference training on the usage of USMC SPS.

Training Plan (Deliverable P018)

3.16 Sustainment Training

3.16.1 Sustainment training is required for SPS users. At a minimum the Contractor shall adhere to the following subsections:

3.17 User Training Delivery

The objective of user training is to provide quality training to enhance user performance that promotes efficiencies and effectiveness to help meet policies and requirements for the SPS User community. SPS currently has one course.

At a minimum, the Contractor shall adhere to the following subsections:

3.17.1 Develop a Training Plan (P018) and schedule for delivering training materials via viral and on-site. Provide the Government with proposed training material and a training schedule for review 60 days prior to first training event. The Government will verify and validate training materials and provide feedback to finalize training material development.

Training Plan (Deliverable P018)

3.17.2 Provide on-site training via Instructor Led Training, Interactive Courseware, Computer Based Training, and blended training solutions at the locations listed in Table 12 as approved by the COR.

3.17.3 Be responsible for providing all necessary equipment and material to conduct training.

3.17.4 Update and maintain training material to reflect technical and functional changes to SPS/PD2 that impact the user.

3.17.5 Develop, conduct, and maintain Virtual Training via Government Microsoft Teams by subject matter experts using Contractor developed and Government approved training materials that effectively communicate updates on the latest SPS releases in need of instruction (e.g., slide presentations, live demos, handouts). Live or Virtual demos will be dependent on completing SETR production readiness reviews.

3.17.6 Maintain attendance rosters and deliver training course completion certificates.

3.17.7 Provide the Government with a trip report that identifies actions of each training day, training attendance rosters, deviations from training schedule, plan and future plans to address training deviations as necessary. The Contractor shall provide recommendations to enhance future training evolutions in each trip report.

3.18 Audit Support

The prime objective of audit support is to ensure SPS complies with current Financial and IT Audit Readiness and Accountability.

The NABS Program Manager is responsible for improving program financial efficiency and accountability of system internal controls, business processes, and supporting documentation of financial statements. To enable SPS to perform effective DoD IT audit compliance, the Contractor shall describe their approach, in the proposal, to implementing audit compliance, and once implemented, sustaining financial and IT audit compliance. The Contractor shall include a description of the tools and processes used for audit compliance, performing audit readiness and reporting, and providing applications with the ability to trace contracting transactions and financial statements (capture and retain transaction data).

SPS is currently participating in the DoD Inspector General IT Audit. On an annual basis, SPS Program Office manages responses to an estimated 18 DoN-Tracker taskers, 15 Corrective Action Plans (CAP), and several dozen Provided by Client (PBC) requests related to the audit. In addition,

SPS performs audit site visits and several validation events with the audit team throughout the year.

3.19 Audit Meetings and Documentation

At minimum the Contractor shall adhere to the following subsections:

3.19.1 Participate in weekly SPS Audit Integrated Product Team (IPT), status teleconference calls, and ad hoc meetings with MCSC Internal Controls Division and Internal Controls Audit Readiness Team (ICART).

3.19.2 Conduct system analysis to identify potential gaps in audit compliance and present resolutions to strengthen audit posture.

3.19.3 Support the assessment of PBC requests, which includes:

3.19.4 Participate in scheduled PBC status teleconference calls.

3.19.5 Review the PBC requests security controls to determine where the impact occurs.

3.19.6 Develop recommended responses to the PBC request.

3.19.7 Maintain a PBC Request Tracking log for capturing of requests and submissions of responses to requests.

3.19.8 Track response times per request, estimated no more than five (5) working days turn around response time.

3.19.9 Support the responses to Follow-Up-Questions, estimated no more than five (5) working days turn around response time.

3.19.10 Support the responses to Observation requests, estimated no more than five (5) working days turn around response time.

3.19.11 Support site visits and meeting requests by ICART and the audit team to include, but not limited to, observation events, walkthrough demonstrations, and validation testing.

3.19.12 Support development of Government responses to Notice of Findings and Recommendations (NFRs) which includes:

- Assessing the NFR and provide recommended responses.
- Supporting the drafting of the CAP to include identifying key milestones for the plan.

3.19.13 Evaluation of assessments against identified PBC, Observation, and NFR requests. At minimum the Contractor shall adhere to the following subsections:

3.19.13.1 Conduct an evaluation of the PBC, Observation, and NFR requests.

3.19.13.2 Prepare draft responses for approval by the Government.

3.19.13.3 Prepare CAPs for final NFR presented by the Audit team.

3.19.13.4 Generate reports for approval by the Government.

3.19.13.5 Deliver monthly metrics, in the MSR, which include, at a minimum, the number of PBCs, Observations, and NFRs responded to during the reporting period, and number of hours executed by Contractor resources.

Monthly Status Report (MSR) (Deliverable P006)

4 Software

All software configuration and deployment objectives shall be developed and fielded IAW the PMO Management Plans. Additional supporting documentation includes the Supplement Guidebook for Acquisition of Naval Software Intensive Systems and the MCSC TR Handbook - SIAT-HDBK-001, 06 August 2014.

The ECPs CLINs are optional objectives and are subject to availability of funds.

Additionally, all software initiatives impact the system baseline and are governed by the CM process as defined in the CMP, SEP, and PMO Management Plans. The CMP and SEP lays out the process required to develop, modify, or upgrade Government software and describes the details of each step along with any considerations that need to be addressed. The PMO SEP defines the 4-integer ECP classification system that is used to assign ECPs as either a capability change, major change, minor change, or a maintenance change; it details how the SETR process, as defined in the MCSC SETR Handbook, is tailored based on this classification level.

The Contractor shall develop and maintain a PDSSP (P001) that correlates with the processes, products, functions, and objectives described in the PMO SEP. This PDSSP is considered a living document that will be updated as necessary to support evolving SPS user requirements and maturing products and processes. New capability requirements (classified as a first octet capability change) shall provide the following IAW the specified level of SETR tailoring based on the ECP classification level:

4.1.1 Derived requirements.

4.1.2 Development schedule.

4.1.3 Test software.

4.1.4 Deploy Software.

4.1.5 Supporting artifacts that are based on the recommended methodology in the Supplement

to Guidebook for Acquisition of Naval Software Intensive Systems: Software Criteria and Guidance for SETRs; PMO Management Plans; and the MCSC SETR Handbook, v1.4 dated April 2009.

4.1.6 Areas where cost savings will be realized through reusability, reliability, and maintainability.

4.1.7 Research and analysis support new capability requirements to include any potential migration to an enterprise system.

4.1.8 At minimum, migration support in transitioning capability to ePS to include the following sections:

4.1.8.1 Conduct GAP Analysis between SPS and ePS specifically for USMC

4.1.8.2 From GAP Analysis identify business process changes, technology limitations/capabilities, and interface requirements

4.1.8.3 Perform analysis of existing data in SPS to determine migration eligibility

4.1.8.4 Support IPT with ePS SI support and USMC stakeholders

4.1.8.5 Work with ePS SI and USMC stakeholders to develop a migration schedule/roadmap and SOPs

4.1.8.6 Set up SPS Archiving capability

4.1.8.7 Assist ePS SI with data migration

4.1.8.8 Establish read-only SPS databases after data migration

4.1.8.9 Disable interfaces where necessary

4.1.8.10 Consolidate SPS server sites, if necessary

4.1.8.11 Ensuring the Cybersecurity posture is maintained and ensuring old documents are accessible.

4.1.9 A strategy for integrating CM, Human Systems Integration (HSI), Logistics, and Cybersecurity into each stage of the software test and deployment process.

4.2 Requirements Analysis Phase

The key objective of the Requirements Analysis Phase is to transform the SPS user(s) needs into a technical view of a required product that could deliver those needs. Efforts involve defining SPS user(s) needs and requirements in the context of planned use environments and identified system characteristics to determine requirements for system functions.

The Contractor shall elicit derived requirements and produce and maintain a Requirements Traceability Matrix (RTM) (Deliverable P021) that establishes a hierarchy of requirements and traceability to design and test plans, documents, and artifacts. The RTM shall contain the title of each requirement and a reference to the document and section where the details can be found. The relevant design document and test plans shall be listed along with the relevant section and title within the design document and test plans. At minimum the Contractor shall adhere to the following subsections:

Requirements Traceability Matrix (RTM) (Deliverable P021)

4.2.1 Conduct requirements elicitation with system Stakeholders to support requirements analysis activities.

4.2.2 Perform an iterative process of decomposing requirements into system functional requirements and establishing traceability.

4.2.3 Maintain traceability between the derived and Government-provided requirements.

4.2.4 Align requirements analysis efforts with MARCORSYSCOM acquisition requirements (PMO Management Plans and SETR process).

4.2.5 Provide documentation needed to support the MARCORSYSCOM SETR process for System Requirements Reviews and System Functional Reviews (SFR), or Requirements Review brief to gain Government approval of the requirements at the identified TR.

4.2.6 Document the functional baseline.

4.3 System Design Phase

The objective for the System Design Phase is the on-time delivery to the Government of Government-approved documentation that provides the detailed design of each configuration item in the approved product baseline. The System Design phase produces a design that is based on the functional descriptions and products developed during the Requirements Analysis phase. The design is reflected in the System Design Document (SDD) (P022) and Sub-System Design Document (SSDD) (P022) products developed and delivered by the Contractor.

System/ Subsystem Design Document (SDD/SSDD) (Deliverable P022)

At minimum the Contractor shall develop and document a system design for review at the Preliminary Design Review (PDR), Critical Design Review (CDR), or Design Review (DR) to gain Government approval at the identified SETR event. At minimum the Contractor shall adhere to the following subsections:

4.3.1 Describe the Contractor's design process, analyses, and tradeoffs.

4.3.2 Conduct design demonstrations prior to the PDR, CDR, or DR in order to demonstrate system designs and gain Government feedback.

4.3.3 Align the Contractor's process with the PMO Management Plans and the MARCORSYSCOM SETR process for DRs. The required technical DRs are specified for each change.

4.3.4 Provide inputs to the TR brief in support of the Government PDR, CDR, or DR.

4.3.5 Provide documentation needed to support the required technical DRs.

4.3.6 Provide a draft software test plan and software test description to support follow-on planning.

4.3.7 Provide new or update existing system design documentation to address new system changes.

4.3.8 Document the Allocated and Product baselines.

4.4 Development Phase

The prime objective for the Development Phase is the on-time delivery of a Government-tested and accepted capability solution. At minimum the Contractor shall adhere to the following subsections:

4.4.1 Integrate, assemble, and test capability.

4.4.2 Conduct unit testing to verify the parts and components of each system change functions prior to system or software integration.

4.4.3 Conduct software integration to compile system code into a functional product.

4.4.4 Generate software test scripts to prepare for overall system integration and GAT.

4.4.5 Provide In-Process Reviews.

4.4.6 Align to the MARCORSYSCOM SETR process and the PMO Management Plans process for TRs.

4.4.7 Provide documentation (Software Test Plan with System/ Software Test Description with Test Scripts (P020)) needed to support the required TRs.

Software Test Plan with System/ Software Test Description with Test Scripts (Deliverable P020)

4.4.8 Support the Government in conducting GAT to review the final software product in support of a deployment decision.

4.4.9 Conduct cybersecurity scans, Independent Validation & Verification (IV&V), HSI reviews and testing, code review, and cyber-penetration testing (Software Metrics (P005)).

Software Metrics (Deliverable P005)

4.5 Test and Evaluation

4.5.1 The Contractor shall plan and support the successful roll-out of software and related hardware including the required Contractor test and evaluation and GAT processes.

4.6 Deployment Phase

The prime objective for the Deployment Phase is the deployment of the approved capability into the production environment in accordance with the established performance standards. At minimum the Contractor shall adhere to the following subsections:

4.6.1 Document the Contractor's deployment process.

4.6.2 Ensure all system user support materials are updated to reflect the changes being introduced.

4.6.3 Validate that all assessments and authorizations are in place prior to deployment.

4.6.4 Prepare the user community to receive and use capability.

4.6.5 Support a System Verification Review (SVR) demonstrating verification that the developed solution meets requirements.

4.6.6 Coordinate and deliver the deployment package within the PDSS Release Management process.

4.6.7 Provide input to the release management team for the VDD that identifies final Configuration Item change.

4.6.8 Support a PIR to gain Government approval to close the release.

5 Project Management

5.1 Project Management

The Contractor shall execute and manage their project management plan when planning, acquiring staff and other resources, training staff, designing and implementing process improvement, managing risk, and related processes inherent with the requirements in this PWS. The Contractor shall provide updates to the PMP as needed or as directed by the Government.

5.1.1 Project Management Plan (PMP)

The Contractor shall prepare a PMP (Deliverable P002). The Government approved PMP serves as the common understanding between the Government and the Contractor on how the contract will be managed. The Government fully realizes that the Contractor shall need to periodically revisit and update the PMP to ensure that it accurately reflects the dynamics of managing a contract

of this magnitude. At minimum, the PMP shall be updated as necessary and resubmitted to the Government for approval. The Contractor has the latitude to build upon the document content to ensure all aspects of the Contractor's collaborative project management processes are addressed. All additional updates will require approval from the Government.

At a minimum, the PMP shall define and describe the Contractor's processes:

Project Management Plan (Deliverable P002)

5.1.1.1 Processes.

5.1.1.2 Identify the types of skill sets and skill levels that will be needed and provided and the strategies that will be used to ensure that the right amount of the right skills will be available when needed.

5.1.1.3 Describe the process for periodically assessing the contract, determining areas for improvement, gaining Government approval, and implementing improvement plans (Process Improvement).

5.1.1.4 Describe the process to develop, update, and monitor the project schedule using Microsoft Project 2010 and to provide an IMS (P013) derived schedule and supporting data to the Government.

Integrated Master Schedule (IMS) (Deliverable P013)

5.1.1.5 The Contractor shall have, and provide evidence of, individual clearances of team members as necessary and appropriate for work those team members are required to perform.

5.2 Risk Management

The contractor shall prepare a Risk Management Plan (RMP) (P014). The RMP shall describe the Contractor's approach to determining, reporting, rating and monitoring risks within the project. At minimum the contractor shall adhere to the following subsections:

Risk Management Plan (RMP) (Deliverable P014)

5.2.1 Execute risk management IAW the PMO RMP.

5.2.2 Develop, and include in the MSR (P006), risk reports summarizing the risks and identifying the likelihood and consequence of each risk.

Monthly Status Report (MSR) (Deliverable P006)

5.3 Reporting and Monitoring

The Contractor shall describe the metrics, reporting mechanisms, and control procedures it will use to measure, report, and manage requirements, the schedule, resources, and quality assurance.

Information gathered will be presented to the COR via the MSR, or other reporting requirements (P015). At minimum the contractor shall adhere to the following subsections:

Other Reports, Analysis, Papers, Trip Reports and Presentations including SETR Briefs (Deliverable P015)

Monthly Status Report (MSR) (Deliverable P006)

5.3.1 Include in the MSR, performance monitoring efforts (e.g., performance metric monitoring, risk analysis) that shall identify and support the determination of performance variances within sufficient time to allow the Contractor the ability to implement corrective action before Contractor and/or system performance falls below acceptable thresholds.

Monthly Status Report (MSR) (Deliverable P006)

5.3.2 Include in the MSR, all Priority 1 metrics from the PMO Performance Measurement Plan, previous month's activities, updated risk register, upcoming activities, all incidents, summary of service issues, problem trends, progress towards the Performance Standard and Acceptable Quality Levels (AQLs), and anticipated travel (with a justification for the travel). The metrics submitted for the MSR shall be IAW the PMO Performance Measurement Plan.

Monthly Status Report (MSR) (Deliverable P006)

5.3.3 Participate in SPS IPT meetings and Working Groups where program status will be reported. The Contractor shall aid in the development of meeting materials such as the Meeting Agenda and Meeting Minutes for the meetings listed in Table 7 below.

Production and Development Meetings	Frequency
Engineer Review Board	Monthly
Configuration Control Board	Monthly
Cyber Security Status Review	Weekly
Cyber Security Document Review	Semi-annually
System Engineering Technical Interchange Meetings	Weekly (as determined by the IPT SE)
SETR Reviews	For each Production release / upgrade
Requirements Elicitation	For each Production release / upgrade
Monthly Status Review Meeting	Monthly
SPS IPT Meeting	Bi-Weekly
Audit Status Meeting	Weekly
Audit Observation Meeting	Weekly (as determined by the PjO)

Table 7: Meeting Requirements

5.4 Quality Assurance and Control

5.4.1 Within the PMP, the Contractor shall prepare a QAPP (P003). The QAPP shall describe the Contractor's approach to ensuring quality performance for all aspects of the contract. The Government shall evaluate the Contractor's performance under this contract IAW the QASP. The QASP is a Government plan that focuses on what the Government will do to ensure that the Contractor has performed IAW the performance standards. The QASP defines how the performance standards will be applied, the frequency of surveillance, and the AQLs. The AQLs are also listed in Section 9 below.

The QAPP shall include:

5.4.2 The Contractor's quality assurance program which shall provide a total quality management system approach to the SPS efforts and shall include program and technical management, quality assurance, quality control, and performance management to achieve the control of product and service quality to the DoN, inclusive of the Marine Corps, throughout contract performance.

5.4.3 The Contractor's systems engineering, quality assurance, and quality control efforts shall comply with Government policy and instructions. These efforts shall be reflected in the Contractor's PDSS, system maintenance, and performance, and will ensure both existing and new/enhanced capabilities meet the Government's objectives for quality, as defined in the AQLs.

Quality Assurance Program Plan (QAPP) (Deliverable P003)

5.5 Performance Management

The Contractor shall attend all Interim Program Reviews convened by the contracting activity or contract administration office IAW Federal Acquisition Regulation (FAR) Subpart 42.5. The Contracting Officer, COR, and other Government personnel may meet periodically with the Contractor to review the Contractor's performance. At these meetings, the Contracting Officer will apprise the Contractor of how the Government views the Contractor's performance and the Contractor will apprise the Government of any problems being experienced. Appropriate action shall be taken to resolve outstanding issues.

6 Contract Closeout

Provide orderly closeout of the contract including final delivery of any remaining Government products, hardware, software, and preparation of a final Closeout Report (P023) to include lessons learned and analysis of the task. The Contractor shall provide a migration plan for any open Service Desk tickets not already contained within the Government provided tool.

Closeout Report (Deliverable P023)

7 Integrated Master Schedule (IMS)

The Contractor shall develop and maintain an overall SPS IMS (P013) throughout the PoP of the contract. The SPS IMS shall provide information sufficient to the Government to demonstrate how the Contractor intends to manage the proposed effort.

The Contractor shall incorporate PDSS and ECP tasks into the Contractor IMS for SPS and shall provide the ability to understand how it intends to manage PDSS and ECPs with visibility of:

- Tasks.
- Activities.
- Schedule.
- Deliverables.

At a minimum, the Contractor shall develop an IMS using Microsoft Project version 2010 compatible or a version otherwise approved by the Government.

Integrated Master Schedule (Deliverable P013)

8 Performance Standards

8.1 Contractor performance shall be monitored against the following performance standards and AQLs:

Performance Standard	Methods of Surveillance	Acceptable Quality Levels
Service Desk support will be available M-F, Hours 0800-1630	• Service Desk ticket logs • Weekly Technical Interchange Meeting (TIM) • MSR	• Exceptional: Greater than or equal to 99% • Satisfactory: Greater than or equal to 98% • Unsatisfactory: Less than 98%
Service Desk tickets resolved at Tier I within 15 minutes or elevated to next Tier if unable to resolve	• Service Desk ticket logs • Weekly TIM • MSR	• Satisfactory: Greater than or equal to 95% • Unsatisfactory: Less than 95%

Performance Standard	Methods of Surveillance	Acceptable Quality Levels
Timely delivery of specified deliverable	• MSR • Deliverable • Transmittals	• Exceptional: Earlier than the identified date • Satisfactory: On time or less than 24 hours past the identified date • Unsatisfactory: More than 24 hours past the identified date
All availability issues are communicated to Government within 1 hour of discovery	• Service Desk ticket logs • Weekly TIM • MSR	• Satisfactory: Communicated in 1 hour or less • Unsatisfactory: Not communicated within 1 hour
CITDB is updated within 10 business days of a change	• Periodic Government PCAs based on the CITDB	• Exceptional: Updated within 7 days • Satisfactory: Updated within 8 – 10 days • Unsatisfactory: Not updated within 10 days
ATO is maintained	• Identity & Access Management Cybersecurity Status Reports	• Exceptional - 100% of IAVAs and OPDIRS, applicable to the system, are remediated in accordance with the respective remediation timeline. 100% of un-remediated IAVA and OPDIRS are added to the IAVA and OPDIR POA&M. • Satisfactory - 98% of IAVAs and OPDIRS, applicable to the system, are remediated in accordance with the respective remediation timeline. 100% of un-remediated IAVA and OPDIRS are added to the IAVA and OPDIR POA&M. • Unsatisfactory – Less than 98% of IAVAs and OPDIRS, applicable to the system, are remediated in accordance with the respective remediation timeline. 100% of un-remediated IAVA and OPDIRS

Performance Standard	Methods of Surveillance	Acceptable Quality Levels
Minimize unplanned downtime Any down-time on weekends or attributed to the Government will not count as unplanned down-time Planned down-time that exceeds the agreed upon window will count as unplanned downtime	• Service Desk ticket logs • FRACAS • MSR	• Exceptional: Operational Availability is greater 98% • Satisfactory: Operational Availability equal to 98% • Unsatisfactory: Operational Availability less than 98%
Ensure timely restoration of services. Mean Time to Restore: 24 hours after downtime	• Service Desk ticket logs. • FRACAS • MSR	• Exceptional: Operational Availability is greater 97% • Unsatisfactory: Operational Availability less than 97%

Execution of Government Assessment Testing. The software has no Severity 1 and 2 defects as defined in the PMO System Test and Evaluation Strategy.	• GAT Scorecard
	• SETR results
		• Exceptional:
		  ○ Zero severity 1 defects
		  ○ Two or fewer severity 2 defects
		• Satisfactory:
		  ○ Zero Severity 1 defects
		  ○ Three severity 2 defects
		• Unsatisfactory:
		  ○ Any severity 1 defect
		  ○ Four or more severity 2 defects

Table 8: Performance Standards

9 Applicable Documents and References

The following tables provide programmatic and technical information for the Contractor to consider in preparation of a response to this PWS at the solicitation phase and during contract performance post-award.

Document / Reference	Intended Use
SLA with Hosting Environment; Operational Document MOC-033 HCS Service Level Agreement	Identifies agreements and coordination POCs with the system hosting environment
Interface Control Documents and/or System Interface Agreements	Documents the roles/responsibilities and data exchange information between SPS and other systems
Contingency Plan	Provides guidance on the decision-making process and its timely response to any disruptive or extended interruption of normal business operations and services
Risk Register	Contains all risks
ECP Tracker Database	Contains tracking of all system ECPs
Trouble Ticket Database	Contains all system Trouble Tickets
Requirements Traceability Matrix	Government requirements document
System Maintenance and Administration Manual	Describes the administrative functions to maintain the system
Configuration Item Technical Database (CITDB)	Describes the hardware and software configuration items
Database Architecture	Describes the system database architecture
Training Material	Instructor training material to support classroom training
Test Scripts	Set of instructions executed by a person to ensure the system is functioning correctly
Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01G / Joint Capabilities Integration and Development System	Requirements Guidance
CJCSI 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND), 9 Feb 11	Cybersecurity
MARADMIN 657/13 Requirements for Network Security Source Code Review dated 13 December 2013	Cybersecurity

Document / Reference	Intended Use
Department of the Navy, DoD Information Assurance Certification and Accreditation Process (DIACAP), dated 28 November 2007	Cybersecurity
Department of Defense Instruction (DODI) 8510.01 Risk Management (RMF) for DoD Information Technology, dated 12 March 2014	Cybersecurity
DoD 5200.2-R, Personnel Security Program dated January 1987, Incorporating Change 3, dated 23 February 1996	Cybersecurity
DoD 8570.01-M, Information Assurance Workforce Improvement Program, Incorporating Change 4, 10 November 2015	Cybersecurity
DoD Memorandum, Department of Defense Guidance on Protecting Personally Identifiable Information, 18 August 2006	Cybersecurity
DoD Regulation 5200.1-R, Information Security Program, Volume 1, dated 24 February 2012	Cybersecurity
Dept. of Defense Directive (DoDD) 5000.01 / Defense Acquisition System dated, 20 November 2007	Acquisition Guidance
DoDD 8000.01, Management of the DoD Information Enterprise, dated 10 February 2009	Cybersecurity
DoDD 8500.01E, Information Assurance (IA), dated 23 April 2007	Cybersecurity
DoDI 5000.02 / Operation of the Defense Acquisition System, dated 7 January 2015	General Acquisition Execution Guidance
DoDI 8500.2, Information Assurance Implementation, dated 6 February 2003	Cybersecurity
Federal Acquisition Regulation (FAR)	Contracting

Document / Reference	Intended Use
Federal Information Security Modernization Act (FISMA), dated 18 December 2014	Cybersecurity
IEEE/EIA 12207 / Standard for Information Technology Software Life Cycle Processes	Industry Standard for Software Support
Marine Corps Systems Command Technical Review Handbook, v2, October, 2014	Systems Engineering Technical Review (SETR)
MCO 5239.2, Marine Corps Cybersecurity Program (MCCSP), dated 18 July 2012	Cybersecurity
Marine Corps Systems Command Order (MARCORSYSCOMO) 4130.1 / Configuration Management Policy	CM Policy
MARCORSYSCOMO 5400.5 / Naval SYSCOM Systems	SETR
MIL-HDBK-61 / Configuration Management	CM Guidance
MIL-STD-881 / Work Breakdown Structures	Guidance on building WBS
National Defense Authorization Act for Fiscal Year 2016, S. 1356, 25 November 2015	Requirements Guidance
OMB Circular A-130 Appendix III, Security of Federal Automated Information Resources, dated November 28, 2000	Cybersecurity
SECNAV Instruction 5211.5E, DoN Privacy Program, 28 December 2005	Cybersecurity
SECNAVINST 5000.2E, Implementation and Operation of the Defense Acquisition System and the Joint Capabilities Integration and Development System, 01 Oct 2011	Cybersecurity
SECNAVINST 5000.36A, Department of the Navy Information Technology Applications and Data Management, 19 December 2005	Cybersecurity

Document / Reference	Intended Use
USMC Enterprise Cybersecurity Directive (ECSD) 018, Marine Corps Certification and Accreditation Process Version 3.0, dated 7 December 2012	Cybersecurity
USMC ECSD 011, Personally Identifiable Information Version 4.0, dated 30 November 2013	Cybersecurity
USMC ECSD 021, Ports, Protocols, and Services Management version 1.0, 15 May 2012	Cybersecurity
USMC ECSD 008, Secure Data Transfer Version 2.0, 17 December 2012	Cybersecurity
USMC ECSD 026, Concept of Operations for Host Based Security System Version 1.0, 15 October 2012	Cybersecurity
MCSCO 5530.2A - Access Control Order	Security Requirements

Table 5: System Documentation

10 Deliverables

All Deliverables shall be delivered to the Government's electronic repository (SharePoint) with a notification to the Contracting Officer, COR, and the SPS Project Officer. All Deliverables must adhere to new guidance per publication of DoDI 5200.48 and 5230.24. See Section 14 Security Requirements for additional information. (Note: SharePoint requires a CAC for access)

Table 11 provides a comprehensive list of the deliverables:

1063

Deliverable Number	Deliverable Title	Format	Date of first submission	Subsequent Submission
P001	Post Deployment Software Support (PDSS) Plan	Government approved Contractor Format	60 days after Contract award	ASREQ
P002	Project Management Plan (PMP)	Government approved Contractor Format	60 days after Contract award	ASREQ
P003	Quality Assurance Program Plan (QAPP)	Government approved Contractor Format	30 Days after Contract Award	ASREQ
P004	Incident and Problem Management Plan	Government approved Contractor Format	60 days after Contract award	ASREQ
~~P005~~	~~Software Metrics~~	~~Government approved Contractor Format~~	~~Ten business days prior to the SETR event~~	~~Ten business days after receipt of Government comments~~
P006	Monthly Status Report (MSR)	Government approved Contractor Format	15 days after completion of the first calendar month	NLT than 15th of Every month thereafter
P007	Configuration Management Plan (CMP)	Government approved Contractor Format	60 days after Contract award	ASREQ
P008	Version Description Document (VDD)	Government Approved Contractor Format	Five business days before Deployment	ASREQ
P009	GAT Scorecard (To include a summary to the Government)	Government Approved Contractor Format	Weekly scorecards for Integration testing, daily scorecards for GAT	ASREQ

Deliverable Number	Deliverable Title	Format	Date of first submission	Subsequent Submission
P010	Test Report and Defects	Government Approved Contractor Format	Ten business days prior to Test Readiness Review (TRR)	Ten business days prior to update at SVR
P011	Release Deployment Plan	Government Approved Contractor Format	Ten business days after the start of the contract month	First week of every month thereafter
P012	System Maintenance and System Administration Manuals	Government Approved Contractor Format	ASREQ, depending upon the release and ECP at TRR	Two working days after receipt of Government comments
P013	Integrated Master Schedule (IMS)	Microsoft Project 2010 or newer version	45 days after Contract award	NLT 15th of each month for previous month or after each release and ECP award
P014	Risk Management Plan (RMP)	Government approved Contractor Format	60 days after Contract award	N/A
P015	Other reports, analysis, papers, trip reports and presentations including (SETR briefs)	Government Approved Contractor Format	ASREQ	ASREQ
P016	FRACAS	Government Approved Contractor Format	ASREQ	Ten working days after receipt of Government comments
P017	Software / Hardware Refresh Plan (5	Government Approved Contractor	90 days after contract award	10 working days after receipt of

Deliverable Number	Deliverable Title	Format	Date of first submission	Subsequent Submission
	Years)	Format		Government comments
P018	Training Plan	Government approved Contractor Format	45 business days after contract award	N/A
P019	System / Software Source Code	Government Provided Format	Within five days following scheduled release	Final 15 working days before the end of the PoP
P020	Software Test Plan with System/ Software Test Description with Test Scripts	Government Approved Contractor Format	Ten business days before DR	Five business days after receipt of Government comments
P021	Requirements Traceability Matrix (RTM)	Government Provided Format	Final due ten days before each SSR, SFR and contract closure	Update for DRs and for contract closure
P022	System/ Subsystem Design Document (SDD/SSDD)	Government Provided Format	Delivery as required by PMO and based upon the complexity of the subject changes. Otherwise no less than thirty business days before the end of the TO	Five business days after receipt of Government comments
P023	Closeout Report	Government Approved Contractor	30 days prior to Contract Closeout date	ASREQ
P024	Cybersecurity IMS	MS Excel 2010 or newer version	30 days after Contract Award	Every month thereafter
P025	Cybersecurity Action Tracker	Government Provided Format	30 days after Contract Award	Biweekly thereafter

Deliverable Number	Deliverable Title	Format	Date of first submission	Subsequent Submission
P026	Service Desk Metrics	Government Provided Format	30 days after Contract Award	First Thursday of every month thereafter

Table 6: Deliverables

Submission dates above that show "ASREQ" ("As Required"), will be based on dates assigned and mutually agreed upon at the time the requirement for the deliverable arises since it is difficult to predict when the need to create/update these artifacts will occur.

10.1 Inspection and Acceptance

The COR shall inspect all services and deliverables. Final acceptance of deliverables is the responsibility of the COR.

11 Government Furnished Information (GFI) and Contractor Furnished Equipment (CFE)

The Government will provide other necessary GFI which will include: system documentation, system manuals, and web-based training source code.

Per MCSC Order 4400.201, the Contractor shall provide their own laptop, docking station, other peripherals, and power cords. The government Logistician will receive a list of machine types authorized on the MCEN from MCSC AC/S G6 and provide to the Contractor. Contractor provided assets must meet the hardware/software compliance requirements identified by the AC/S G-6 and the Contractor must comply with MCSC IT policies. All hardware/software requiring connectivity to the MCEN will be turned over to AC/S G-6, Electronics Maintenance Facility (EMF) Team, by Contractor personnel, in order to make Contractor provided assets network ready. The Contractor will complete all required MCEN user agreements prior to CFE being imaged and placed on the MCEN. With approval from the COR, the government Logistician will coordinate this effort. All software and software updates, including the Operating System will be provided by the Government. Any Government Furnished Equipped (GFE) currently assigned and being utilized by the vendor to perform system sustainment activities until MCEN imaged CFEs are ready is permitted with the approval of the COR and the government Logistician. Once CFEs are MCEN imaged and provided to the vendor, any fielded GFEs will be returned to government Logistician. The timeframe for permitting currently used GFEs and status of CFEs being MCEN imaged will be relayed to and approved by the COR and government Logistician.

The Government provides the shared data environment where all SPS information resides. The shared data environment includes repositories to support the SPS's configuration control process, baseline documentation, CITDB, action items, risk management, etc.

HCS provides the hosting facility for SPS Pre-Production instances in a virtual environment.

The Government will supply the necessary licenses for the following: The JPMO provides the Sybase licenses for SPS and access is coordinated with Deputy Assistant Secretary of the Navy.

The Government will provide the Contractor with laptops for system integration, maintenance, software development, testing, and training.

12 Access to Government Facilities

The Contractor must seek prior approval of the COR for access to 105 Tech Parkway or 1000 Quantico Corporate Center in the execution of their duties. Any unclassified Contractor-furnished laptops must be logged with the laboratory entry control point sentry.

13 Marine Corps Enterprise Network (MCEN)

Contractor personnel performing IT sensitive duties are subject to investigative and assignment requirements. DoDD 8570.01, and DoD 8570.01-M requires DoD civilian, DoD consultants, and Support Contractor Personnel performing work on sensitive automated information systems to be assigned to positions that are designated at one of three sensitivity levels (IT-I, IT-II, or IT-III).

MCEN IT resources, if provided, are designated For Official Use Only (FOUO) and other limited authorized purposes. DoD military, civilian personnel, consultants, and contractor personnel performing duties on MCEN information systems may be assigned to one of three position sensitivity designations.

MCEN Computer Access - Contractor personnel accessing MARCORSYSCOM computer systems shall maintain compliance with United States Marine Corps Enterprise Cybersecurity Manual 007 Resource Access Guide. Contractor personnel will submit a DD 2875, and completion certificates for the CYBERC course located on MarineNet located at https://www.marinenet.usmc.mil. The CYBERC course consists of the DOD Cyber Awareness Challenge and Department of the Navy Annual Privacy Training (PII). Contractors will have to create a MarineNet account in order to acquire the required training.

MCEN Official E-mail usage – MCEN IT resources are provided FOUO and other limited authorized purposes. Authorized purposes may include personal use within limitations as defined by the supervisor or the local Command. Auto forwarding of e-mail from MCEN-N to commercial or private domains (e.g., Hotmail, Yahoo, Gmail, etc.) is strictly prohibited. E-mail messages requiring either message integrity or non-repudiation are digitally signed using DoD Public Key Infrastructure (PKI). All e-mail containing an attachment or embedded active content must be digitally signed.

MCEN users will follow specific guidelines to safeguard Controlled Unclassified Information (CUI). Non-official e-mail is not authorized for and will not be used to transmit CUI to include PII and Health Insurance Portability and Accountability Act (HIPAA) information. Non-official e-mail is not authorized for official use unless under specific situations where it is the only mean

for communication available to meet operational requirements. This can occur when the official MCEN provided e-mail is not available but must be approved prior to use by the Marine Corps Authorizing Official (AO).

All Contractor personnel shall read, understand, and comply with policy and guidance to protect classified information and CUI, and to prevent unauthorized disclosures IAW United States Marine Corps Enterprise Cybersecurity Manual 007 Resource Access Guide and CJCSI 6510.01F.

14 Security Requirements

This contract will require the contractor to have a Secret Facility Clearance and will require certain contractors to obtain and maintain classified access eligibility. The Contractor shall have a valid Secret Facility Clearance prior to classified performance. The Prime Contractor and all sub-contractors (through the Prime Contractor) shall adhere to all aspects of 32 CFR Part 117 NISPOM and DoD Manual 5220.22 Volume 2. All personnel identified to perform on this contract shall maintain compliance with DoD, DoN, and Marine Corps Information and Personnel Security Policy to include completed background investigations (as required) prior to classified performance. This contract shall include a DoD Contract Security Classification Specification (DD-254) as an attachment. Certain Contractors will be required to perform IT-I/II duties that will require favorably adjudicated Tier 5/3 Level investigations. The Defense Counterintelligence Security Agency will not authorize Contractors to submit the necessary Tier Level investigations solely in support of IT level designation requirements, but are required to submit investigations for those employees requiring both Secret access and IT-II designation. The Government Contracting Activity Security Office (GCASO) is required to submit any required investigations in support of IT-I level designations. The Contractor Facility Security Officer (FSO) is however required to establish, populate and own the DISS record of every Contractor processed for and/or issued a CAC or submitted for IT level duties. The Contractor is required to provide a roster of prospective Contractor employees performing IT-I duties to the MCSC Contracting Officer's Representative (COR). This roster shall include: full names, Social Security Numbers, e-mail address and phone number for each contractor requiring investigations in support of IT Level designations. The COR will verify the IT-I requirements and forward the roster to the GCASO. Contractors found to be lacking required investigations will be contacted by the GCASO. This contract shall include a DoD Contract Security Classification Specification (DD-254) as an attachment.

FSOs are responsible for notifying the MCSC AC/S G-2 Personnel Security Office (PERSEC Office) at 703-432-3952/3490/3374 if any Contractor performing on this contract receives an unfavorable adjudication as any issued CAC would need to be Revoked and Retrieved. Due to Insider Threat concerns, the FSO is also requested to notify the PERSEC Office, within 24 hours, of any adverse/derogatory information associated with the 13 Adjudicative Guidelines concerning any Contractor performing on this contract, if they have been granted an IT designation, issued a CAC and/or a MCSC Building Badge. The FSO shall notify the Government (written notice) within 24 hours of any Contractor personnel added or removed from the contract if they have been granted classified access, granted IT designations, and issued a CAC and/or a MCSC Building Badge.

Publication of DoDI 5200.48 "DoD CUI Program" has eliminated FOUO in marking documentation; therefore, neither the term nor the acronym will be used to describe sensitive unclassified information. The only approved term is CUI, which is unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended. The contractor shall consider the contents of the deliverable and when the deliverable includes CUI, assign markings as appropriate in compliance with DoDI 5200.48 and the following:

The CUI category "Controlled Technical Information (CTI)," as defined in DFARS clause 252.227-7013 and clarified in the CUI Registry is technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Examples include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identification, data sets, studies and analyses and related information, and computer software executable code and source code.

Information determined to be CTI shall be marked in accordance with the DoDI 5200.48 guidance and shall include a distribution statement consistent with the DoDI 5230.24.

15 Common Access Card

The COR will identify and only approve those Contractor employees performing on this contract that require a CAC in order to perform their job function. In accordance with Headquarters, USMC issued guidance relative to Homeland Security Presidential Directive – 12, all personnel must meet eligibility criteria to be issued a CAC. In order to meet the eligibility criteria, Contractor employees requiring a CAC must obtain and maintain a favorably adjudicated Personnel Security Investigation (PSI). Prior to authorizing a CAC, the employee's Defense Information System for Security (DISS) record must indicate a completed and favorably adjudicated PSI or (at a minimum) that a PSI has been submitted and accepted (opened). The minimum acceptable investigation is a T-1 or a National Agency Check with Written Inquiries (NACI). If a Contractor employee's open investigation closes and is not favorably adjudicated, the CAC must be immediately retrieved and revoked. CACs are not issued for convenience.

FSOs are responsible for notifying the MCSC AC/S G-2 PERSEC Office at 703-432-3490/3952 if any Contractor performing on this contract receives an unfavorable adjudication after being issued a CAC. The FSO must also immediately notify the PERSEC Office of any adverse/derogatory information associated with the 13 Adjudicative Guidelines concerning any Contractor issued a CAC, regardless of whether a DISS Incident Report is submitted.

Each CAC is issued with a "ctr@usmc.mil" e-mail account that the individual Contractor is responsible to maintain as active by logging in on a regular basis (at least twice a month), sending an e-mail and clearing any unneeded e-mails. Contractors issued a CAC are prohibited from "auto-forwarding" e-mail from their .mil e-mail account to their .com e-mail account. If the

"ctr@usmc.mil" e-mail account is not kept active, G-6 will deactivate the account and the CAC will also lose its functionality. Contractor employees shall solely use their government furnished "ctr@usmc.mil" e-mail accounts for work supporting the USMC, conducted in fulfillment of this contract, and shall not use a Contractor supplied or personal e-mail account to conduct official U.S. government business. The use of a Contractor or personal e-mail account for Contractor business or personal use is allowed, but only when using cellular or a commercial internet service provider.

If a Contractor loses their eligibility for a CAC due to an adverse adjudicative decision, they have also lost their eligibility to perform on MCSC contracts.

16 Place of Performance

For cost-efficiency reasons, the Government expects the Contractor management team and lead engineers to be located within a 50 mile commuting distance from Marine Corps Base Quantico, VA. The Government will not pay travel costs for Contractor staff to commute to the Contractor facility or for any travel within a 50-mile radius of the Contractor's facility. Any reimbursable travel costs incurred during the performance of the contract shall not include travel for day-to-day work activities.

The work to be performed under this contract shall be performed at the Contractor's facility.

The Contractor is expected to attend meetings and participate in telephone conferences in the Quantico, Virginia area.

17 Hours of Work

Contract support is required to be available, at minimum, during core hours Monday through Friday, 0900 to 1500 EST daily for contractor personnel not supporting the Service Desk.

The exceptions include Office of Personnel Management (OPM) US Federal Holidays, and as directed by the Government, due to closing of Government facilities (i.e., administrative closings or similar Government directed facility closings). The Contractor shall provide Service Desk support Monday through Friday, 0800-1630.

18 Contractor Employee Identification

All Contractor personnel working on a Government installation shall possess and wear an identification badge that displays his or her name and his or her "Contractor" status. The Contractor shall ensure that Contractor personnel identify themselves as Contractors when attending meetings, sending emails, answering Government telephones, providing any written correspondence, or working in situations where his or her actions could be construed as official Government acts. All documents or reports produced by Contractors are to be suitably marked as Contractor-produced products or that Contractor participation is appropriately disclosed. While performing in a Contractor capacity, Contractor personnel shall refrain from using his or her retired or reserve component military rank or title in all written and verbal communications.

19 Period of Performance

The PoP will be four years (including options). The Base is a six-month PoP. Options 1, 2 and 3 are twelve-month PoPs, and Option 4 is a six-month PoP. Each PoP, if awarded, will require PDSS support services. ECPs that arise during those PoPs, if any, will be exercised as options at that time, subject to the availability of funding.

20 Travel and Other Direct Costs (ODC)

No travel is authorized without the Contracting Officer's or COR's preapproval. The Contracting Officer or COR will be the approval authority for all Contractor travel request, submitted in writing and in advance of all travel. Travel details, including estimated costs, must be provided to the COR for approval prior to the commencement of any travel. Travel shall be in direct support of tasks assigned within this PWS. Local travel to or within the Quantico commuting area as defined in Marine Corps Base Order 7220.1C is not reimbursable. Local travel is considered travel within a 50-mile radius from the home station to perform official duties such as attending meetings, conferences, etc. Continental United States and OCONUS travel (transportation, per diem, air fare, auto rental, out of pocket expenses, and other allowable expenses) is reimbursable IAW FAR 31.205-46 and within the limitation of funds specified in the contract. Any travel or per diem costs that exceed the rates in the Joint Travel Regulations will be found unreasonable. ~~No profit shall be allowed on travel or Other Direct Costs (ODCs)~~. Relevant information can be found at the Joint Travel Regulation web site: https://secureapp2.hqda.pentagon.mil/perdiem/

ALL OCONUS travelers must comply with DoD, Department of the Navy and MARCORSYSCOM travel regulations to include completing required training, endorsements, and authorizations prior to travel. Except in unusual circumstances, the Contractor shall provide, no later than 10 working days from the proposed Temporary Additional Duty (TAD), a travel TAD request for approval through the COR. The Contractor shall provide within five (5) working days, a written EXSUM (Executive Summary) or AAR (After Action Review) on all meetings and conferences attended on behalf of the Government to the COR. Contractor personnel are required to complete the Synchronized Pre-deployment Operational Tracker (SPOT) training.

ODCs: In the course of performance, pursuant to this contract, the Contractor may be required to purchase incidental items at the request of the Government. The Contractor shall acquire necessary items of ODCs associated with the services on the contract only with written, advanced, approval of the COR. The Contractor will retain title to all ODC items that are not identified as deliverables, and any repair, maintenance, or replacement of items will be at the Contractor's expense.

Notional Travel locations are listed in Table 11.

Planned Annual Training For SPS		
LOCATION	**Projected # of Training Events per 12 month PoP**	**SPS/PD2 Training Duration per each Training Event**
MCB Camp Lejeune, NC	2	5
MARFORRES New Orleans, LA	2	5
MCB Camp Pendleton, CA	2	5

Table 7: Notional Travel Locations

21 Organizational Conflict of Interest (OCI)

To the extent that the work under this contract requires access to proprietary, business confidential, or financial data of other companies, and as long as these data remain proprietary or confidential, the Contractor shall protect the data from unauthorized use and disclosure and agrees not to use it to compete with those other companies.

(a) "Organizational Conflict of Interest" means that because of other activities or relationships with other persons, a person is unable or potentially unable to render impartial assistance or advice to the Government, or the person's objectivity in performing the contract work is or might be otherwise impaired, or a person has an unfair competitive advantage. "Person" as used herein includes corporations, partnerships, joint ventures, and other business enterprises.

(b) The Contractor warrants that to the best of its knowledge and belief, and except as otherwise set forth in the contract, the Contractor does not have any organizational conflict of interest(s) as defined in paragraph (a).

(c) It is recognized that the effort to be performed by the Contractor under this contract may create a potential organizational conflict of interest on the instant contract or on a future acquisition. In order to avoid potential conflict of interest, and at the same time to avoid prejudicing the best interest of the Government, the right of the Contractor to participate in future procurement of equipment and/or services that are the subject of any work under this contract shall be limited as described below IAW the requirements of FAR 9.5.

(d)(1) The Contractor agrees that it shall not release, disclose, or use in any way that would permit or result in disclosure to any party outside the Government any information provided to the Contractor by the Government during or as a result of performance of this contract. Such information includes, but is not limited to, information submitted to the Government on confidential basis by other persons. Further, the prohibition against release of Government provided information extends to cover such information whether or not in its original form (e.g., where the information has been included in Contractor generated work or where it is discernible

from materials incorporating or based upon such information). This prohibition shall not expire after a given period of time. See also, DFARS 252.204-7000, Disclosure of Information, incorporated by reference in this included in the contract.

(2) The Contractor agrees that it shall not release, disclose, or use in any way that would permit or result in disclosure or any party outside the Government any information generated or derived during or as a result of performance of this contract.

(3) The prohibitions contained in subparagraphs (d)(1) and (d)(2) shall apply with equal force to any affiliate of the Contractor, any Subcontractor, Consultant, or employee of the Contractor, any joint venture involving the Contractor, any entity into or with which it may merge or affiliate, or any successor or assign of the Contractor.

(e) The Contractor further agrees that during the performance of this contract and for a period of three years after completion of performance of this contract, the Contractor; any affiliate of the Contractor; any Subcontractor, Consultant, or employee of the Contractor; any joint venture involving the Contractor; any entity into or with which it may subsequently merge or affiliate; or any other successor or assign of the Contractor, shall not furnish to the Marine Corps, either as a Prime Contractor or as a Subcontractor, or as a Consultant to a Prime Contractor or as a Subcontractor, any system, component, or services which are the subject of the work to be performed under this contract. During the course of performance of this contract or before the three year period following completion of this contract has lapsed, the Contractor may, with the authorization of the cognizant Contracting Officer, participate in a subsequent procurement for the same system, component, or service. In other words, the Contractor may be authorized to compete for procurement(s) for systems, components or services subsequent to an intervening procurement.

(f) The Contractor agrees that, if after award, it discovers an actual or potential organizational conflict of interest; it shall make immediate and full disclosure in writing to the Contracting Officer. The notification shall include a description of the actual or potential organizational conflict of interest, a description of the action, which the Contractor has taken or proposes to take to avoid, mitigate, or neutralize the conflict, and any other relevant information that would assist the Contracting Officer in making a determination on this matter. Notwithstanding this notification, the Government may terminate the contract for the convenience of the Government if determined to be in the best interest of the Government.

(g) Notwithstanding paragraph (f) above, if the Contractor was aware, or should have been aware, of an organizational conflict of interest prior to the award of this contract or becomes, or should become aware of an organizational conflict of interest after award of this contract and does not make an immediate and full disclosure in writing to the Contracting Officer, the Government may terminate this contract for default.

(h) If the Contactor takes any action prohibited by this requirement or fails to take action required by this requirement, the Government may terminate this contract by default.

(i) The Contracting Officer's decision as to the existence or nonexistence of the actual or potential organization conflict of interest shall be final and is not subject to the clause of this contract entitled "DISPUTES" (FAR 52.233.1).

(j) Nothing in this requirement is intended to prohibit or preclude the Contractor from marketing or selling to the United States Government its product lines in existence on the effective date of this contract; nor, shall this requirement preclude the Contractor from participating in any research and development. Additionally, sale of catalog or standard commercial items are exempt from this requirement.

(k) The Contractor shall promptly notify the Contracting Officer, in writing, if it has been tasked to evaluate or advise the Government concerning its own products or activities or those of a competitor in order to ensure proper safeguards exist to guarantee objectivity and to protect the Government's interest.

(l) The Contractor shall include this requirement in subcontracts of any tier which involve access to information or situations/conditions covered by the preceding paragraphs, substituting "Subcontractor" for "Contractor" where appropriate.

(m) The rights and remedies described herein shall not be exclusive and are in addition to other rights and remedies provided by law or elsewhere included in this contract.

Appendix A. Acronyms

Acronym	Definition
A&A	Assessment & Authorization
ACAS	Assured Compliance Assessment Solution
Ao	Operational Availability
AQL	Acceptable Quality Level
ATO	Authority to Operate
BEA	Business Enterprise Architecture
CAC	Common Access Card
CAP	Corrective Action Plan
CCB	Configuration Control Board
CDR	Critical Design Review
CFE	Contractor Furnished Equipment
CI	Configuration Item
CITDB	Configuration Item Tracking Database
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CLIN	Contract Line Item Number
CM	Configuration Management
CMP	Configuration Management Plan
COR	Contracting Officers Representative
COTS	Commercial Off the Shelf
CTI	Controlled Technical Information
CUI	Controlled Unclassified Information
DADMS	Department of the Navy Application and Database Management System
DLA	Defense Logistics Agency
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DR	Design Review
DoN	Department of the Navy
ECP	Engineering Change Proposal
ECSD	Enterprise Cybersecurity Directive
EDA	Electronic Document Access
ePS	electronic Procurement System
ERB	Engineering Review Board
ERP	Enterprise Resource Planning
FAR	Federal Acquisition Regulation

Acronym	Definition
FISMA	Federal Information Security Management Act
FRACAS	Failure Reporting and Corrective Action System
FSO	Facility Security Officer
GAT	Government Acceptance Test
GCASO	Government Contracting Activity Security Office
GEX	Global Exchange
GFE	Government Furnished Equipment
GFI	Government Furnished Information
HCS	Hybrid Cloud Services
HSI	Human System Integration
IAVA	Information Assurance Vulnerability Alert
IAVB	Information Assurance Vulnerability Bulletins
IAVM	Information Assurance Vulnerability Management
IAW	In Accordance With
ICART	Internal Controls Audit Readiness Team
ICD	Interface Control Document
ID	Identification
IMS	Integrated Master Schedule
IPT	Integrated Product Team
ISSM	Information Systems Security Manager
IT	Information Technology
IV&V	Independent Validation and Verification
JPMO	Joint Program Management Office
MCSC/ MARCORSYSCOM	Marine Corps Systems Command
MCCAST	Marine Corps Certification and Accreditation Support Tool
MCB	Marine Corps Base
MCCSP	Marine Corps Cybersecurity Program
MCO	Marine Corps Order
MITSC	Marine Air Ground Task Force Information Technology Support Center
MLG	Marine Logistics Group
MSR	Monthly Status Report
NABS	Naval Applications and Business Services
NACI	National Agency Check with Written Inquiries
NFR	Notice of Findings and Recommendations
OCONUS	Outside Continental United States
ODC	Other Direct Costs

Acronym	Definition
OPDIR	Operational Directive
P2P	Procure 2 Pay
PA	Paperless Acquisition
PBC	Provided By Client
PCA	Physical Configuration Audit
PD2	Procurement Desktop Defense
PDR	Preliminary Design Review
PDS	Procurement Data Standard
PDSS	Post Deployment Software Support
PDSSP	Post Deployment Software Support Plan
PEO MLB	Program Executive Officer, Manpower, Logistics and Business Solutions
PERSEC	Personnel Security Office
PKI	Public Key Infrastructure
PIR	Post Implementation Review
PIEE	Procurement Integrated Enterprise Environment
PM	Program Manager
PM APPs	Program Manager Applications
PMP	Project Management Plan
POC	Point of Contact
POA&M	Program of Action and Milestones
PoP	Period of Performance
PR	Purchase Request
PRDS	Purchase Requirements Data Standard
PSI	Personnel Security Investigation
PSS	Production Support System
PWS	Performance Work Statement
QAPP	Quality Assurance Program Plan
QASP	Quality Assurance Surveillance Plan
RFA	Request for Action
RMF	Risk Management Framework
RMP	Risk Management Plan
ROM	Rough Order of Magnitude
RTM	Requirements Traceability Matrix
SCAP	Security Content Automation Protocol
SDD	System Design Document
SE	Systems Engineering
SEP	System Engineering Plan

Acronym	Definition
SETR	Systems Engineering Technical Review
SFR	System Functional Review
SI	Systems Integrator
SIA	System Interface Agreement
SLA	Service Level Agreement
SLM	Service Level Management
SPS	Standard Procurement System
SR	Service Release
SSDD	Sub-System Design Document
SSP	Systems Security Plan
STIG	Security Technical Implementation Guide
SVR	System Verification Review
TIM	Technical Interchange Meeting
TIR	Test Incident Report
TR	Technical Review
TRR	Test Readiness Review
UI	Universal Interface
USMC	United States Marine Corps
VDD	Version Description Document