PROGRAM MANAGER, APPLICATIONS

INFORMATION TECHNOLOGY SERVICE MANAGEMENT PROGRAM MANAGEMENT SUPPORT SERVICES

PERFORMANCE WORK STATEMENT

PREPARED BY PAMELA DEBERRY

14 July 2017

Table of Contents

Table of Contents

1.0 Scope. The Marine Corps Systems Command (MCSC), Supporting Establishment Systems (SES), Applications, Quantico, VA requires support for the United States Marine Corps (USMC) implementation of common Information Technology (IT) Infrastructure Library (ITIL)-based IT Service Management (ITSM) processes and tools that provide a common framework for managing key network services and infrastructure.

1.1 Background. Effective June 2017, MCSC reorganized and Program Manager Information Systems & Infrastructure (PM IS&I) transitioned to Portfolio Manager Supporting Establishment Systems. Product Manager Marine Corps Network and Infrastructure Services (MCNIS) was split between three separate Program Management Offices; Network & Infrastructure, Applications, and Customer Support & Strategic Sourcing. Currently, MCNIS is responsible for planning and executing the activities needed to sustain and modernize the USMC garrison network. The portfolio of programs and initiatives include overall acquisition and lifecycle management responsibilities for the following programs:

    a. USMC interests in the Department of Navy (DoN) Next Generation Enterprise Network (NGEN) program in support of the Navy Marine Corps Internet (NMCI) garrison unclassified Non-Secure Internet Protocol Routing Network..

    b. Secure Operational Network Infrastructure and Communications (SONIC) Program for the garrison SECRET Internet Protocol Router Network (SIPRNET).

NGEN provides IT services to include manpower support and engineering services to the Marine Corps Cyberspace Operations Group, Marine Forces Cyber Command, the Marine Corps Enterprise Network regions and MCSC to support the unification, modernization and sustainment of the government-owned, government-operated network environment. NGEN is an Acquisition Category (ACAT) I program managed by the DoN Program Executive Office – Enterprise Information Systems.

The SONIC Program was established in 2011 to provide acquisition and sustainment support to the USMC garrison SIPRNET users and network operators. The SONIC Program was initiated at the Operations and Support (O&S) lifecycle phase. SONIC is an ACAT IV program managed by MCSC.

The USMC has chosen to implement an ITSM framework using the ITIL v3 model. MCNIS has been tasked to develop and sustain ITSM processes and tools necessary to implement ITSM within the USMC garrison network.

2.0 General Requirements.

All deliverables shall be submitted to the Contracting Officer's Representative (COR) who is responsible for both the acceptance and approval of the deliverables.

In accordance with DFAR 211.106, there shall be a clear distinction between Government employees and service contractor employees. contractor employees shall identify themselves as contractor personnel by introducing themselves or being introduced as contractor personnel and by displaying distinguishing badges or other visible identification when meeting with Government personnel. In addition, contractor personnel shall identify themselves as contractor employees in telephone conversations and in formal and informal written correspondence.

The contractor shall report contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract via a secure, Government-approved SharePoint site Contracted services excluded from reporting are based on Product Service Codes (PSCs). The excluded PSCs are:

 (1) W, Lease/Rental of Equipment;
 (2) X, Lease/Rental of Facilities;
 (3) Y, Construction of Structures and Facilities;
 (4) S, Utilities ONLY;
 (5) V, Freight and Shipping ONLY.

The contractor is required to completely fill in all required data fields using the following web address https://doncmra.nmci.navy.mil.

Reporting inputs will be for the labor executed during the period of performance during each Government fiscal year (FY), which runs 01 October through 30 September. While inputs may be reported any time during the FY, all data shall be reported no later than 31 October of each calendar year. Contractors may direct questions to the help desk, located at the following Uniform Resource Locator: https://doncmra.nmci.navy.mil.

2.1 Specific Requirements

2.1.1 The Contractor shall develop and maintain a contract management plan and associated schedules, Contract Data Requirements List1.

Deliverable 0001: Contract Management Plan

2.1.2 The contractor shall develop, maintain, and submit a company organizational chart depicting a diagram and a directory with the positions and names.

Deliverable 0002: Organizational Diagram

2.1.3 The contractor shall conduct quarterly In-process Reviews (IPRs) that address an overall assessment of contract status, project review, program risk, status of funds, status of vacancies, schedules, completed deliverables, and concerns.

2.1.4 Meeting Support

2.1.4.1 The contractor shall perform the following tasks in support of meetings:

 a) Write and submit calendar invitations
 b) Record minutes, action items, decisions, and executive summaries
 c) Develop, archive and track agendas
 d) Develop meeting presentation slides and supporting reading materials

2.1.4.2 The contractor shall maintain an electronically searchable meeting support library. The meeting support library has already been established and currently is located on a MCSC SharePoint site.

2.1.4.3 The contractor shall provide teleconference support for meetings with over 30 lines and when Government conference lines are not available.

2.1.5 Information Technology Information Library (ITIL) Process Development and Maintenance

2.1.5.1 The contractor shall draft processes, polices and standards related ITSM/ITIL requirements, disseminate for review and comment and then collect and adjudicate government comments and changes for the Marine Corps enterprise processes for Incident Management, Event Management, Service Asset and Configuration Management (SACM), Release and Deployment Management, Service Catalog Management, Problem Management, Knowledge Management, Change Management , Availability Management, Demand Management, Service Level Management, Capacity Management, Access Management , and Service Request Fulfillment in establishment of enterprise process governance.

Deliverable 0003 ITIL Documentation

2.1.5.2 The contractor shall draft an assessment of the implementation of current ITSM processes and supporting capabilities and recommend enhancements and changes.

2.1.5.3 The contractor shall facilitate ITSM meetings and review boards.

2.1.5.4 The contractor shall maintain the existing fourteen (14) USMC Enterprise ITSM Process Guides.

2.1.5.5 The contractor shall coordinate and facilitate adjudication meetings to collect government acceptance or rejection of all Comment Resolution Matrix comments.

2.1.5.6 The contractor shall maintain ITSM process guides, procedure work instructions, and process governance documentation.

2.1.5.7 The contractor shall maintain ITSM process assessment criteria, measurements, checklists and reporting methods.

2.1.5.8 The contractor shall research preliminary assessment findings and develop summary brief(s) to facilitate reviews with Process Owners and Managers.

2.1.5.9 The contractor shall collect and report the Key Performance Indicators (KPIs) within 60 days of the initial delivery by the Government of each Process Guide.

2.1.5.10 The contractor shall research and report process improvements and develop and refine the resulting KPI reports.

2.1.5.11 The contractor shall write and submit, one per process, a reporting guidebook to describe KPIs and enterprise reports including report descriptions and instructions on how to run them.

2.1.5.12 The contractor shall research and report on Continual Service Improvement (CSI) in accordance with ITIL v3 standards.

2.1.5.13 The contractor shall maintain the existing ITSM Procedure Work Instructions.

2.1.5.14 The contractor shall maintain the existing ITSM Standard Operating Procedures.

2.1.5.15 The contractor shall maintain the existing ITSM Process Test Plan.

2.1.5.16 The contractor shall maintain the existing ITSM Technical Data Package.

2.1.5.17 The contractor shall perform the following tasks in support of Service Asset Configuration Management:

    e) Execute asset management policies, procedures and processes as defined by the ITSM SACM process guide
    f) Coordinate with management in utilizing the asset management tools to analyze, review and track asset data
    g) Assist the Process Owner and Process Manager to develop asset control processes to monitor accountability identification, maintenance, location and contracts
    h) Work with USMC commands to manage and document processes in support of asset reconciliation and asset disposal agreements
    i) Work with Process Owner and Process Manager to develop processes in support of configuration identification, configuration item relationship management and audit
    j) Assist in configuration item audit activities
    k) Assist in inventory management, in support of asset procurement and shipment activities
    l) Assist with the monitoring of software licenses to ensure the compliance with license agreements and usage standards

m) Collaborate and provided feedback to define cost savings, asset compliances and service improvements
n) Ensure audit compliance for IT assets and configuration items
o) Analyze current metric reports to improve accuracy of the Configuration Management Database (CMDB) working with USMC Commands.
p) Guide IT asset associate in the daily administration of the asset management activities, tools, processes, and policies
q) The contractor shall have a strong background in BMC Remedy; specifically, within the asset management module
r) The contractor shall have a strong background in ITIL v.3 and understanding of the interrelation between ITIL/ITSM process areas.

2.1.5.18 The contractor shall perform the following tasks in support for Change Management:

a) Execute change management policies, procedures and processes as defined by the ITSM Change Management guide
b) Work with the Change Management Process Owner to capture processes and procedures for Change Control Boards (CCBs) and Change Advisory Boards (CABS) to include:
   o Agenda and meeting minutes
   o Status action items tracking
   o Change record establishment
   o Relating of service requests
   o Change priorities, impacts, and affected work products
   o Targeted environments
   o Dependencies with other changes
c) Work with the Change Management Process Owner and the Release Management Process Owner to document the processes detailing the coordination with release management
d) Work with Change Management Process Owner, Service Asset and Configuration Management Process Owner, Development and Infrastructure Teams to develop process necessary to maintain the integrity of the software development and controlled environments, assures consistent implementation of:
   o CCB decisions
   o Hardware changes
   o New requirements
   o Code fixes
   o Data fixes
   o Configuration fixes
   o Design changes
   o Test scripts
   o Test configurations

e) Working with Definitive Media Library (DML) Librarian, establish and maintain detailed procedures for all software reproduction and distribution and ensure they are tied back to official releases.

f) Provide recommendation for process improvement implementation within the Enterprise ITSM tool suite.

g) Analyze current metric reports to improve accuracy and cost savings.

h) Provide assistance to Enterprise in the daily administration of the Change Management activities, tools, processes, and policies.

i) The contractor shall have a strong background in BMC Remedy; specifically, within the change and release management module.

j) The contractor shall have a strong background in ITIL v. 3 and the interrelation between ITIL/ITSM process areas.

2.1.5.19 The contractor shall provide ITIL/ITSM expert support to the ITSM PMO/Center of Excellence team to help establish, implement, and execute ITSM processes and capabilities across the USMC.

2.1.6 ITSM Project Support

2.1.6.1 The contractor shall outline and submit ITSM IT system requirements for the 14 ITSM processes related to ITSM development and deployment.

2.1.6.2 The contractor shall support HQMC C4 in the development of requirements for ITSM systems in accordance with ITSM policy directives related to ITSM development and deployment.

2.1.6.3 The contractor shall support the ITSM Project Office with implementation of the ITSM processes, capabilities, and governance.

Optional Objective 1: ITIL Process Development and Maintenance for any additional ITSM processes beyond those which are developed and implemented during the period of performance.

3.0 Period and Place of Performance

3.1 Period of Performance. The period of performance for this effort shall consist of one, 12-month base period and three, 12-month option periods. The optional objective will be exercised at the sole discretion of the Government.

3.2 Place of Performance. Work efforts in support of this task effort will be accomplished primarily at the contractor's facilities

4.0 Other Direct Costs (ODCs), and Travel Requirements.

Laptops, cellular equipment and services, and other items of convenience are not reimbursable as ODCs. Contractor facility must be within 15 miles of Quantico, VA.

All Government printing requirements MUST be done by, or through, the local Document Automation and Production Service. Phone 703-784-2206, Bldg 1001

The contractor shall conduct all travel in direct support of this task order in accordance with the Federal Acquisition Regulation (FAR), Part 31, and consistent with the limits established in the Joint Travel Regulations. The contractor shall present a detailed list of all travel expenses. The contractor shall not apply any G&A or profit to travel costs. Any travel costs shall be pre-approved by the COR prior to incurring the cost and will be handled as a cost reimbursable for no profit Contract Line Item Number (CLIN). Failure to obtain pre-approval may result in rejection of the expenditure. Additionally, travel costs in excess of the CLIN ceiling value shall not be reimbursed. The Contractor shall maintain a file of all travel authorizations as provided by the COR and include copies in invoice documents submitted for travel reimbursement. Costs for local travel (i.e., travel within the DC Metro area radius as defined in Table 4) shall not be reimbursed.

The COR must approve all travel, and a signed copy of approval will be provided verifying the authority for travel. Failure to comply with these deadlines and procedures may impact timely approval of the request. Local travel (i.e. travel within the DC metro area) will not be reimbursed by the Government. Maximum use of technology should be utilized to minimize travel costs.

Work efforts in support of this requirement will be performed primarily at the contractor's facilities, or on-site at MCSC. Laptops, cellular equipment/services, and other items of convenience are not reimbursable as ODCs.

The estimated travel requirement (Table 1) for this effort is provided in the below chart. The contractor must obtain COR approval prior to conducting travel for this effort. CONUS and OCONUS travel must be reimbursed in accordance with FAR part 31.

LOCATION	Number of Trips (Base)	Number of Trips (Option 1)	Number of Trips (Option 2)	Duration	Number of Travelers
Camp Pendleton, CA	2	2	2	1 week each	2
Camp Lejeune, SC	2	2	2	1 week each	2
MCEITS, MO	4	4	4	1 week each	2
Local Travel	N/A	N/A	N/A	N/A	N/A

Table 1 – Travel Requirement

5.0 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 DoD Directive 5220.22-M. All personnel identified to perform on this contract shall maintain compliance with Department of Defense, Department of the Navy, 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 Form 254) as an attachment. The contractor shall provide

written notification to the Government within twenty-four hours of any contractor personnel added or removed from the contract that have been granted classified access, issued a Common Access Card and/or MCSC building access card. Notification via e-mail is acceptable.

COMMON ACCESS CARD (CAC) REQUIREMENT. The COR will identify and approve those contractor employees performing on this contract that require CACs in order to perform their job function. In accordance with Headquarters, United States Marine Corps issued guidance relative to Homeland Security Presidential Directive – 12 (HSPD-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 Joint Personnel Adjudication System (JPAS) 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 National Agency Check with Written Inquiries If a contractor employee's open investigation closes and is not favorably adjudicated; the CAC must be immediately retrieved and revoked.

Facility Security Officers (FSOs) are responsible for notifying the MCSC Security Director if any contractor performing on this contract receives an unfavorable adjudication after being issued a CAC. The FSO must also notify the MCSC Security Director of any adverse/derogatory information associated with the 13 Adjudicative Guidelines/Factors concerning any contractor issued a CAC, regardless of whether a JPAS Incident Report is submitted.

Each CAC is issued with a "ctr.usmc.mil" e-mail account that the individual contractor is responsible to keep active by logging in on a regular basis (at least twice a month), sending an e-mail and clearing any unneeded e-mails. Contractors *are prohibited* from "auto-forwarding" their .mil e-mail account to their .com e-mail account. If the ctr.usmc.mil e-mail account is not kept active, the G-6 will deactivate the account and CAC will lose its functionality.

CACs will only be issued to those contractors supporting this contract that have been authorized by the COR. The COR will only authorize CACs for those contractors that meet current Homeland Security Presidential Directive – 12 (HSPD-12) criteria and have a definitive requirement.

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. CACs are not issued for convenience.

6.0 CONTRACT DELIVERABLES AND PERFORMANCE MEASURES

6.1 Contract Deliverables
The Government COR will evaluate the contractor's performance. The contractor shall incorporate Government review comments on contract deliverables (Table 2) for acceptance. The Government will have fifteen (15) working days to review deliverables and provide comments. The contractor shall correct and resubmit products and deliverables found unacceptable within ten (10) working days of initial rejection. The contractor shall provide all deliverables to the Government COR. The COR and/or Project Lead will provide instructions for uploading deliverables to a Government-approved SharePoint site.

Paragraph	Deliverables	Initial Submission	Subsequent Submission(s)	Format	Copies
2.1.1	Contract Management Plan	60 DAC	AS REQ	Electronically delivered-reproducible in Microsoft format. Compatible with the version in use by the USMC.	1
2.1.2	Organizational Diagram	30 DAC	MTHLY	Electronically delivered-reproducible in Microsoft format. Compatible with the version in use by the USMC.	1
2.1.5.1	ITIL Documentation	AS REQ	AS REQ	Electronically delivered-reproducible in Microsoft format. Compatible with the version in use by the USMC.	1

Table 2 - Deliverables

6.2 Quality Assurance Surveillance Plan (QASP)

6.2.1 Objective: This QASP serves as the principal basis for assessing overall performance quality associated with the PWS. This document will be used by the Government to assess the effectiveness of the contractor's management and technical services. The QASP provides the methodology by which the contractor's performance will be monitored to determine compliance with established performance objectives and to establish performance benchmarks that ensure a quantifiable basis for measuring effectiveness. The plan is designed so that surveillance is limited to that which is necessary to verify the Contractor is performing management and technical services satisfactorily and relates directly to performance objectives delineated in the PWS.

6.2.2 Quality Assurance Plan (QAP): The contractor shall develop and maintain an effective quality control program to ensure services are performed in accordance with this PWS. The contractor shall develop and implement procedures to identify, prevent, and ensure non-recurrence of defective services. The contractor's quality control program is the means by which the contractor assures work complies with the requirements of the contract. The Contractor shall implement a quality assurance process that will improve all products delivered to the Government. The contractor's Quality Control effort shall be described in a QAP and shall address the areas identified in the Performance Requirements Summary (Table 3).

6.2.3 Government Surveillance: The Government will identify an individual to function as the Contracting Officer Representative (COR) for this contract. Her/his authority will be limited to administering specific technical aspects of the contract.

6.2.4 Contracting Officer Representative (COR): The COR will be identified by the Contracting Officer in separate letter. The COR monitors all technical aspects of the contract

and assists in contract administration. The COR is authorized to perform the following functions: assure that the contractor performs the technical requirements of the contract: perform inspections necessary in connection with contract performance: maintain written and oral communications with the contractor concerning technical aspects of the contract: issue written interpretations of technical requirements, including Government drawings, designs, specifications: monitor contractor's performance and notifies both the Contracting Officer and contractor of any deficiencies; coordinate availability of government furnished property, and provide site entry of contractor personnel. A letter of designation issued to the COR, a copy of which is sent to the contractor, states the responsibilities and limitations of the COR, especially with regard to changes in cost or price, estimates or changes in delivery dates. The COR is not authorized to change any of the terms and conditions of the resulting contract.

6.2.5 Surveillance Methods: Surveillance of contractor performance is the method used by the Government to determine whether the contractor is effectively and efficiently complying with all terms and conditions of the task order. In addition to statistical analysis, the functional expertise of the COR plays a critical role in adequately evaluating Contractor performance. The Government may use any of the methods of surveillance listed below, or any reasonable measure in the administration of this QASP. The PRS contains the performance objectives that are being measured.

- Demonstration. A qualification method that is carried out by operation and relies on observable functional operation. It does not require the use of instrumentation or special test equipment.
- 100 Percent Inspection. A qualification method that is carried out by visual examination of software code, data captured in special test equipment, documentation, or hard copy printouts. The Government will inspect software drops for bugs and content on a monthly base, entering summary results into the Surveillance Activity Checklist.
- Periodic Inspection: A qualification method that is carried out by visual examination of software code, data captured in special test equipment, documentation, or hard copy printouts. The Government will inspect software drops for bugs and content on a monthly basis.
- Random Monitoring: A qualification method that is carried out by visual examination of software code, data captured in special test equipment, documentation, or hard copy printouts. The Government will randomly inspect software for bugs and content.
- Analysis: A qualification method that is carried out by examining and assessing the application of techniques in order to determine if they are appropriate and sufficient.

The Offeror shall meet or exceed performance standards in the Government provided QASP in Table 3 below.

PWS Paragraph	Performance Standard	Acceptable Quality Level (AQL)	Surveillance Methods
2.1.5 Information Technology Information Library (ITIL) Process Development and Maintenance	Acceptable performance has been met when quality standards consistently produce acceptable projects 90 percent of the time when the Information Technology Service Management (ITSM) processes assessment, maintaining of ITSM guides, development of ITSM documentation, collection and reporting of Key Performance Indicators (KPIs), and reporting of CSI based upon quantitative and qualitative factors have been accepted by the Government.	Acceptable performance has been met when quality standards consistently produce acceptable projects 80percent of the time when the Information Technology Service Management (ITSM) processes assessment, maintaining of ITSM guides, development of ITSM documentation, collection and reporting of Key Performance Indicators (KPIs), and reporting of CSI based upon quantitative and qualitative factors have been accepted by the Government.	100% Inspection

Table 3 – Performance Standard

7.0 Acronym List

ACAT   Acquisition Category
AM   Access Management
AQL   Acceptable Quality Level
AvM   Availability Management
CAB   Change Advisory Board
CACs   Common Access Cards
CCB   Change Control Board
ChM   Change Management
CLIN   Contract Line Item Number
CM   Capacity Management
CMDB   Configuration Management Database
COR   Contracting Officers Representative
CRM   Comment resolution Matrix
CS3   Customer Support and Strategic Sourcing
CSI   Continual Service Improvement
CUI   Controlled Unclassified Information
DAPS   Document Automation and Production Services
DM   Demand Management
DML   Definitive Media Library
DOD   Department of Defense
DoN   Department of Navy
EM   Event Management

FY	Fiscal Year
FSOs	Facility Security Officers
GOGO	Government-Owned. Government-Operated
HSPD	Homeland Security presidential Directive
IM	Information Management
IS&I	Information Systems & Infrastructure
ITIL	Information Technology Infrastructure Library
ITSM	Information Technology Service Management
JTR	Joint Travel Regulation
KM	Knowledge Management
KPIs	Key Performance Indicators
MCCOG	Marine Corps Cyberspace Operations Group
MCEN	Marine Corps Enterprise Network
MCEITS	Marine Corps Enterprise Information Technology Services
MCNIS	Marine Corps Network and Infrastructure Services
MCSC	Marine Corps Systems Command
MFCC	Marine Forces Cyber Command
N&I	Network and Infrastructure
NACI	National Agency Check with Written Inquiries
NGEN	Next Generation Enterprise Network
O&S	Operations and Support
ODCs	Other Direct Costs
PbM	Problem Management
PdM	Product Manager
PEO EIS	Program Executive Office – Enterprise Information Systems
PfM	Portfolio Manager
PM	Program Manager
PRS	Performance Requirements Survey
PWS	Performance Work Statement
PSC	Product Service Codes
PSI	Personnel Security Investigation
RDM	Release and Deployment Management
RqF	Service Request Management
SACM	Service Asset and Configuration Management
SCM	Service Catalog Management
SES	Supporting Establishment Systems
SIPRNET	Secret Internet Protocol Router Network
SLM	Service Level Management
SONIC	Secure Operational Network Infrastructure and Communications
QAP	Quality Assurance Plan
QASP	Quality Assurance Surveillance Plan