PERFORMANCE WORK STATEMENT (PWS) [TEMPLATE]

HQMC DC I IC4 Cybersecurity Support

Instructions for Offerors: Only Section 5 of this Attachment 1: PWS Template needs to be filled out by the Offeror. If the Offeror chooses to edit any other section of this Attachment 1: PWS Template, any change MUST be highlighted in yellow OR changed using track changes to bring it to the Government's attention. The Government will evaluate the changes and if accepted, it will be reflected on the contract conformed copy. If Offerors chose to revise other sections of the PWS besides Section 5, they need to provide a corresponding explanation of why this revision benefits the Government and still meets the overall objectives of this effort. If an adequate explanation is not provided, Offerors are forewarned that PWS revisions beyond Section 5 may be evaluated as weaknesses or deficiencies in not meeting RFP requirements.

Part 1

General Information

1. **GENERAL:** This is a non-personnel services contract to provide cyber security capabilities services to support the Director, Deputy Commandant Information (DC I), Information, Command, Control, Communications, and Computers (IC4). The Government shall not exercise any supervision or control over the contract service providers performing the services herein. Such contract service providers shall be accountable solely to the Contractor who, in turn is responsible to the Government.

1.1 Introduction: The contractor shall provide the best approach, supervision, non-personal services, and other items related to and necessary to perform cyber security capabilities to support the DC IC4 as defined in this Statement of Objectives.

1.2 Purpose: The purpose of this contract action is to provide cyber security capabilities services to support the Director, IC4. The contractor shall detect the strengths and risks associated with the current state of the Marine Corps Enterprise Network (MCEN), systems, applications, software and data through review, analysis, risk assessment, and mitigation recommendations.

1.3 Background: The Marine Corps is committed to pursuing all necessary and prudent steps to ensure that Marine Corps communications and information technology are available to support Marines and civilian Marines, serving in both deployed and garrison environments, without compromising communications.

Without exception, the goal of the Director of the Command, Control, Communications and Computers (IC4) is to securely supply the right information, to the right place, supported by highly skilled personnel delivering power to the edge from the garrison to the tactical end-of-the-wire for today's Marine. The Director, IC4/Chief Information Officer (CIO) is responsible for the development and oversight of policy, plans and guidance of enterprise services and the security of those services. The Director is also responsible for planning, directing, coordinating, and overseeing IC4 and Information Technology (IT) capabilities and defining policy that supports the warfighting and garrison communications functions for the Marine Corps. As the Cybersecurity (CY) portfolio manager for the Marine Corps component of the Department of Defense Information Network (DODIN), the Director, IC4 is the executive agent responsible for planning, directing, coordinating, and overseeing cybersecurity capabilities and defining policy that support the war fighting and garrison communications functions for the Marine Corps.

Specifically, IC4 is responsible for policy oversight and direction of information systems standards, information systems integration internal and external to the Marine Corps, and monitoring IC4 systems development and implementation. This responsibility also applies to DoD, national, and allied systems that impact the Marine Corps Information Technology architecture and corporate enterprise network application. As the manager of the Marine Corps component of the DODIN CY Portfolio, the Director manages, oversees, and directs the DODIN Information Assurance (IA) Capability Areas as defined by the DODIN CY Intelligence Community Directive (ICD), dated 2005., e.g., Defense of the DODIN, Assured Information Sharing, Provide Information Integrity & Non-Repudiation, Assured Mission Management, Information Confidentiality, Ensure a Highly Available Enterprise.

The threat to the Marine Corps systems infrastructure has changed and increased considerably. The total number of vulnerabilities identified annually in operating systems and applications continues to grow. Additionally, the timetable for the hacker community to develop exploitation tools to exploit vulnerabilities has decreased from weeks to days, and often mere hours after vulnerability is known. As a result, the network defense game has changed. The Director, IC4 requires support for independent cybersecurity assessments, risk mitigation and remediation plans, Certification and Authorization (C&A), and Communication Security (COMSEC) efforts.

DoD has fielded vulnerability scanning, monitoring, vulnerability remediation and patch management tools to support both unscheduled and formal readiness assessments. The contractor shall assist the Government in ensuring the application and compliance of these DoD provided tools to Marine Corps Cyberspace defense framework by conducting assessments, analyzing results, recommending remediation actions, and reporting the security configuration efforts through the Department of Navy (DON) to Congress.

Information systems that are vital to the Marine Corps' ability to carry out their mission are targets for our adversaries. DC I IC4, Compliance (ICC) Cybersecurity (CY) Branch is tasked with the responsibility to coordinate Marine Corps wide efforts to safeguard the

network from attack and preserve our ability to provide reliable and effective network services. Policy for cybersecurity implementation rests with DC I IC4. The focus of cybersecurity in the Marine Corps is to ensure policies and procedures are implemented through tasks, standards, conditions, and oversight, to guarantee assured information delivery, assured data integrity, and assured information protection.

IC4's Cybersecurity Team must develop, oversee, and implement cybersecurity policy on all information technology (IT) resources procured, developed, operated, maintained, or managed throughout the Marine Corps. The Branch is also responsible to defend the MCEN through a defense-in-depth strategy that, in coordination with the DON, the Joint Community, Marine Corps Systems Command (MCSC), Marine Forces Cyberspace Command (MARFORCYBER), and the Marine Corps networked domains to achieve strong, effective, and ensure multidimensional protection of our IT environment.

DoD requires all information systems, networks, and applications be reviewed for cybersecurity compliance and lifecycle management. The Marine Corps has enterprise-level system accreditations covering Marine Corps networked domains, e.g., the Marine Corps Community of Interest (COI), the Marine Corps Enterprise Network Non-Classified Internet Protocol (IP) Router Network (MCEN-N), and the Secret IP Router Network (MCEN-S). Service aggregation and system accreditations are connected to the DODIN through these enterprise-level accreditations. The Authorizing Official (AO) requires support for review of authorization packages using the Risk Management Framework (RFM) to ensure cybersecurity compliance. The contractor shall assist the Government in daily management of submitted C&A package review and recommendation processing; and drafting policy, guidance, manuals, and training curriculum.

The Marine Corps COMSEC Program support requirement provides assistance in generation and propagation of policy, guidance, account management, training, and programmatic oversight of secure communications for voice, data, and imagery. This is all in support of the Intelligence Program and Marine Warfighting requirements. The contractor shall assist the Government in daily management of the Marine Corps COMSEC accounts, cryptographic equipment logistics, and account training. Provide status reports on a scheduled basis citing statuses for both legacy Electronic Key Management System (EKMS) and transitioning Key Management Infrastructure (KMI) suites.

1.4 Scope: DC I IC4 requires service to support cybersecurity capability deliverables, including Risk Management Framework (RMF) Authorization and Assessment and Authorization (C&A), cyberspace defense, and Communications Security (COMSEC) Key Management Infrastructure (KMI) management efforts. RMF C&A capability provides the overall management and execution of actions for support to the Authorizing Official (AO) and Security Controls Assessor (SCA) in the final steps of the process as directed by federal law, Department of Defense (DoD), Department of Navy (DON), and Marine Corps policy and directives. Cyberspace defense specialized support capability provides independent active assessment, defense and response to cyber incidents as

directed by DOD, DON, and Marine Corps. COMSEC KMI management capability supports the accounting and management of special cryptographic devices as directed by the National Security Agency (NSA). Capabilities range the Marine Corps enterprise, spanning tactical, garrison, legacy, and cloud-based capabilities on both the unclassified and classified levels. The Contractor will be required to provide all the end user devices to be used in this requirement.

1.5 Period of Performance: The period of performance shall be for one (1) Base Year of 12 months and
four (4) 12-month option years with a six-month extension per FAR 52.217-8. The Period of Performance reads as follows:

Base Year
Option Year 1
Option Year 2
Option Year 3
Option Year 4
6-month extension (FAR 52.217-8)

1.6 General Information

1.6.1 Quality Control The contractor shall develop and maintain an effective quality control program to ensure services are performed in accordance with the approved 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 how he assures himself that his work complies with the requirement of the contract. The QCP is to be delivered, within 30 days after contract award. After acceptance of the quality control plan the contractor shall receive the contracting officer's acceptance in writing of any proposed change to the QC program.

1.6.2 Quality Assurance: The government shall evaluate the contractor's performance under this contract in accordance with the Quality Assurance Surveillance Plan. This plan is primarily focused on what the Government must do to ensure that the contractor has performed in accordance with the performance standards. It defines how the performance standards will be applied, the frequency of surveillance, and the minimum acceptable defect rate(s).

1.6.3 Recognized Holidays

New Year's Day	Labor Day
Martin Luther King Jr.'s Birthday	Columbus Day
President's Day	Veteran's Day
Memorial Day	Thanksgiving Day
Juneteenth	Christmas Day
Independence Day	

1.6.4 Hours of Operation: The contractor is responsible for conducting business, between the hours of 0900 to 1500 Monday thru Friday except Federal holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government directed facility closings. The Contractor must always maintain an adequate workforce for the uninterrupted performance of all tasks defined within this SOO when the Government facility is not closed for the above reasons. When hiring personnel, the Contractor shall keep in mind that the stability and continuity of the workforce are essential.

1.6.5 Place of Performance: The majority of this effort shall take place onsite in the National Capital Region (NCR) Marine Corp Quantico Base with some distributed locations listed below. Core hours of work are 0900 to 1500, Monday through Friday. All deliverables due time are Eastern Time.

- Key Management Infrastructure (KMI) Support — NCMS, Andrews AFB, MD
- Computer Network Depend (CND) Support — Camp Butler, JP
- Computer Network Depend (CND) Support — Camp Smith, HI
- Computer Network Depend (CND) Support — Camp Pendleton, CA
- Computer Network Depend (CND) Support — MARFORRES, New Orleans, LA
- Computer Network Depend (CND) Support — Camp Lejeune, NC

1.6.6 Security Requirements: Contractor personnel performing work under this contract must have a minimum of a Secret clearance at time of the proposal submission and must maintain the level of security required for the life of the contract. Assessment personnel (i.e., all contractor personnel supporting CLINs X002) must have the equivalent of SSBI with Top Secret Eligibility. The security requirements are in accordance with the attached DD 254.

1.6.7.1 Physical Security: The contractor shall be responsible for safeguarding all government equipment, information and property provided for contractor use. At the close of each work period, government facilities, equipment, and materials shall be secured.

1.6.7.2. Key Control. The Contractor shall establish and implement methods of making sure all keys/key cards issued to the Contractor by the Government are not lost or misplaced and are not used by unauthorized persons. NOTE: All references to keys include key cards. No keys issued to the Contractor by the Government shall be duplicated. The Contractor shall develop procedures covering key control that shall be included in the Quality Control Plan. Such procedures shall include turn-in of any issued keys by personnel who no longer require access to locked areas. The Contractor shall immediately report any occurrences of lost or duplicate keys/key cards to the Contracting Officer.

1.6.7.2.1. In the event keys, other than master keys, are lost or duplicated, the Contractor shall, upon direction of the Contracting Officer, re-key or replace the affected lock or locks;

however, the Government, at its option, may replace the affected lock or locks or perform re-keying. When the replacement of locks or re-keying is performed by the Government, the total cost of re-keying or the replacement of the lock or locks shall be deducted from the monthly payment due the Contractor. In the event a master key is lost or duplicated, all locks and keys for that system shall be replaced by the Government and the total cost deducted from the monthly payment due the Contractor.

1.6.7.2.2. The Contractor shall prohibit the use of Government issued keys/key cards by any persons other than the Contractor's employees. The Contractor shall prohibit the opening of locked areas by Contractor employees to permit entrance of persons other than Contractor employees engaged in the performance of assigned work in those areas, or personnel authorized entrance by the Contracting Officer.

1.6.7.3 Lock Combinations. The Contractor shall establish and implement methods of ensuring that all lock combinations are not revealed to unauthorized persons. The Contractor shall ensure that lock combinations are changed when personnel having access to the combinations no longer have a need to know such combinations. These procedures shall be included in the Contractor's Quality Control Plan.

1.6.8 Special Qualifications: The contractor is responsible for ensuring all employees possess and maintain current applicable professional certification outlined in DODM 8140.03 during the execution of this contract.

1.6.9 Post Award Conference/Periodic Progress Meetings: The Contractor agrees to attend any post award conference convened by the contracting activity or contract administration office in accordance with Federal Acquisition Regulation Subpart 42.5. The contracting officer, Contracting Officers Representative (COR), and other Government personnel, as appropriate, 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 problems, if any, being experienced. Appropriate action shall be taken to resolve outstanding issues. These meetings shall be at no additional cost to the government.

1.6.9.1 The contractor shall plan and conduct quarterly contract status meetings. The primary purpose of these meetings is to review contract performance status and address contract-related issues.

These meetings are expected to last no longer than 2 hours. At a minimum, the meeting will include appropriate contractor representative(s), the contracting officer, the contracting officer's representative (COR), and Government technical personnel, as appropriate; however, the contracting officer may choose to include other Government attendees.

The contractor is responsible for setting up the phone conference facilities or the location where the meeting will take place. (Government's site or Contractor's site)

Each meeting will cover the following topics, as appropriate:

- Contract Performance Status:
  - *Status of contract deliverables/tasks (updates since last meeting)*
  - *Performance issues encountered or expected (e.g., potential delays)*
  - *Required Government actions (e.g., delivery of Government Furnished Items and/or Services)*
  - *Compliance with staffing / key personnel requirements*
  - *Discussion on contractor performance against PRS metrics*
- Other Items:
  - *CLIN-related issues. For cost CLINs, address funding status (FAR 52.232-20).*
  - *Address new or in process modifications, requests for out-of-scope work, requests for equitable adjustment, claims, or disputes*
  - *Clause compliance*
  - *Invoice submission and payment status*
  - *Contractor Performance Assessment Report System (CPARS) status (FAR 42.15)*
  - *Continuous improvement ideas for current contract and/or future contract*

1.6.10 Contracting Officer Representative (COR): The (COR) will be identified by 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 assessments 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 regarding 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 order.

1.6.11 Key Personnel: The follow personnel are considered key personnel by the government: contract manager/Alternate contract manager and Senior Capability Lead – CND. The contractor shall provide a contract manager who shall be responsible for the performance of the work. The name of this person and an alternate who shall act for the contractor when the manager is absent shall be designated in writing to the contracting officer. The contract manager or alternate shall have full authority to act for the contractor on all contract matters relating to daily operation of this contract. The contract manager or alternate shall be available between 8:00 a.m. to 4:30p.m. E.T. Monday thru

Friday except Federal holidays or when the government facility is closed for administrative reasons. Qualifications for all key personnel are listed below:

1.6.12.1 Contract Manager and Alternate

1.6.12.1.1 The Contract Manager and Alternate must have 5 years' experience in management of contractors of complex IT projects/operations of a nature similar in size and scope of this SOO.

1.6.12.1.2 The Contract Manager and Alternate must have 5 years' experience in management of employees of various labor categories and skills in projects similar in size and scope of this SOO.

1.6.12.2 Senior capability lead – CND,

1.6.12.2.1 The Senior capability lead – CND, must have a high degree of expertise coordination of the assessment tasks through subordinates and designated Government personnel. Responsibilities include technical advice for planning complex network, platform and system assessments and reviews

1.6.12.2.2 The Senior Capability Lead – CND must have five (5) years conducting DoD network assessments.

1.6.12.2.3 The Senior Capability Lead – CND must have three (3) years of experience conducting code reviews.

1.6.12 Identification of Contractor Employees: All contract personnel attending meetings, answering Government telephones, and working in other situations where their contractor status is not obvious to third parties are required to identify themselves as such to avoid creating an impression in the minds of members of the public that they are Government officials. They must also ensure that all documents or reports produced by contractors are suitably marked as contractor products or that contractor participation is appropriately disclosed. Contractor personnel will be required to obtain and wear CAC as visual identification in the performance of this service when not at government NIPR workstation.

1.6.13 Contractor Travel: Contractor will be required to travel CONUS, OCONUS and within the NCR during the performance of this contract to attend meetings, conferences, and training. The contractor may be required to travel to off-site training locations and to ship training aids to these locations in support of this PWS. Contractor will be authorized travel expenses consistent with the substantive provisions and in accordance with FAR Part 31.205-46 and only up to the NTE amount identified in each period or as modified by the Government and the limitation of funds specified in this contract. All travel requires COR approval/authorization. A not to exceed amount for travel will be established for planning purposes, historically there has been an average of 8 CONUS and 1 OCONUS trips per year; each trip lasting an average of five (7) days with four (4) travelers.

1.6.14 Status of Forces Agreement: Contractor Personnel who are U.S. citizens may apply for Status of Forces Agreement (SOFA) status as necessary for the execution of

this contract. The determination of SOFA Status is processed by the Office of the Staff Judge Advocate from the applicable Marine Corps Installation to COMUSJAPAN. The Contractor shall be responsible for submitting necessary paperwork to the Office of the Staff Judge Advocate for determination of designation of SOFA status. A breech of regulations and directives outlined in COMUSJAPAN Theater clearance procedures / instruction documents issued by the installation commander or withdrawal of any or all these privileges by the Office of the Staff Judge Advocate for reasons cited, will not affect nor constitute grounds for delay in or nonperformance of any portion of any contract, nor will such action form the basis for any claim against the U.S. Government, based upon the contract or any portion thereof.

The following are those services that may be authorized only for OCONUS locations and shall be based on approval of SOFA status.

- APO/FPO/MPO/Postal Services
- Common Access Card (CAC)
- Local Access Badge
- Commissary
- MWR Facilities
- Military Banking

- Exchange

1.6.15 Other Direct Costs this category in limited to travel (outlined in 1.6.13).

1.6.16 Data Rights The Marine Corps shall be granted unrestricted access and use of all deliverables upon delivery and will receive and maintain full data rights to all products and deliverables. The Contractor will be required to provide all deliverables in a version, format, and media used/useable and modifiable by the Marine Corps. In addition, all pertinent data rights clauses will be incorporated into the solicitation and subsequent contract award. These deliverables shall be included in the firm fixed price of the required services and the Government does not anticipate the requirement of data for this contract to impede future competition given that the required data will be made

accessible to potential offerors in any future solicitations and will be made available to any contractor awarded a follow-on contract.

The following Data Rights clauses are incorporated into the solicitation and will remain incorporated in the resultant contract award document.

252.227-7000 – Non-Estoppel
252.227-7008 – Computation of Royalties
252.227-7012 – Patent License and Release Contract
252.227-7013– Rights in Technical Data--Noncommercial Items
252.227-7014– Rights in Noncommercial Computer Software and Noncommercial Computer Software
Documentation
252.227-7015– Technical Data–Commercial Items
252.227-7017– Identification and Assertion of Use, Release, or Disclosure Restrictions
252.227-7020– Rights in Special Works
252.227-7027– Deferred Ordering of Technical Data or Computer Software
252.227-7037– Validation of Restrictive Markings on Technical Data

1.6.17 Organizational Conflict of Interest: The Contractor shall notify the Contracting Officer immediately whenever it becomes aware that such access or participation may result in any actual or potential OCI and shall promptly submit a plan to the Contracting Officer to avoid or mitigate any such OCI. The Contractor's mitigation plan will be determined to be acceptable solely at the discretion of the Contracting Officer and in the event the Contracting Officer unilaterally determines that any such OCI cannot be satisfactorily avoided or mitigated, the Contracting Officer may affect other remedies as he or she deems necessary, including prohibiting the Contractor from participation in subsequent contracted requirements which may be affected by the OCI.

1.6.18 Phase In /Phase Out Period To minimize any decreases in productivity and to prevent possible negative impacts on additional services, the Contractor shall have personnel on board, during the ten (10) day phase in/ phase out periods. During the phase in period, the Contractor shall become familiar with performance requirements to commence full performance of services on the contract start date.

PART 2
DEFINITIONS & ACRONYMS

2. **DEFINITIONS AND ACRONYMS:**

2.1. DEFINITIONS:

2.1.1. CONTRACTOR. A supplier or vendor awarded a contract to provide specific supplies or service to the government. The term used in this contract refers to the prime.

2.1.2. CONTRACTING OFFICER. A person with authority to enter into, administer, and or terminate contracts, and make related determinations and findings on behalf of the government. Note: The only individual who can legally bind the government.

2.1.3. CONTRACTING OFFICER'S REPRESENTATIVE (COR). An employee of the U.S. Government appointed by the contracting officer to administer the contract. Such appointment shall be in writing and shall state the scope of authority and limitations. This individual has authority to provide technical direction to the Contractor as long as that direction is within the scope of the contract, does not constitute a change, and has no funding implications. This individual does NOT have authority to change the terms and conditions of the contract.

2.1.4. DEFECTIVE SERVICE. A service output that does not meet the standard of performance associated with the Performance Work Statement.

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

2.1.6. KEY PERSONNEL. Contractor personnel that are evaluated in a source selection process and that may be required to be used in the performance of a contract by the Key Personnel listed in the PWS. When key personnel are used as an evaluation factor in best value procurement, an offer can be rejected if it does not have a firm commitment from the persons that are listed in the proposal.

2.1.7. PHYSICAL SECURITY. Actions that prevent the loss or damage of Government property.

2.1.8. QUALITY ASSURANCE. The government procedures to verify that services being performed by the Contractor are performed according to acceptable standards.

2.1.9. QUALITY ASSURANCE Surveillance Plan (QASP). An organized written document specifying the surveillance methodology to be used for surveillance of contractor performance.

2.1.10. QUALITY CONTROL. All necessary measures taken by the Contractor to assure that the quality of an end product or service shall meet contract requirements.

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

2.1.12. WORKDAY. The number of hours per day the Contractor provides services in accordance with the contract.

2.1.12. WORK WEEK. Monday through Friday, unless specified otherwise.

2.2. ACRONYMS:

ACOR	Alternate Contracting Officer's Representative
AFARS	Army Federal Acquisition Regulation Supplement
AO	Authorizing Official
AR	Army Regulation
C&A	Certification and Accreditation
CCE	Contracting Center of Excellence
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CND	Computer Network Defense
COI	Community of Interest
COMSEC	Communications Security
CONUS	Continental United States (excludes Alaska and Hawaii)
COR	Contracting Officer Representative
COTR	Contracting Officer's Technical Representative
COTS	Commercial-Off-the-Shelf
CY	Cybersecurity / Cyber Security
DA	Department of the Army
DC I	Deputy Commandant Information
DD250	Department of Defense Form 250 (Receiving Report)
DD254	Department of Defense Contract Security Requirement List
DFARS	Defense Federal Acquisition Regulation Supplement
DMDC	Defense Manpower Data Center
DOD	Department of Defense
DODIN	Department of Defense Information Network
DON	Department of the Navy
EKMS	Electronic Key Management System
FAR	Federal Acquisition Regulation
HIPAA	Health Insurance Portability and Accountability Act of 1996
HQMC	Headquarters Marine Corps
IC4	Information, Command, Control, Communications, and Computers
ICC	DC I IC4 Compliance Branch
IA	Information Assurance

IT	Information Technology
KMI	Key Management Infrastructure
KO	Contracting Officer
MARFORCYBER	Marine Corps Forces Cyberspace Command
MCEN	Marine Corps Enterprise Network
MCEN-N	Marine Corps Enterprise Network – Non-Classified Internet Protocol (IP) Router Network
MCEN-S	Marine Corps Enterprise Network – Secret Internet Protocol (IP) Router Network
MCSC	Marine Corps Systems Command
NIPR	Non-Classified Internet Protocol (IP) Router Network
OCI	Organizational Conflict of Interest
OCONUS	Outside Continental United States (includes Alaska and Hawaii)
ODC	Other Direct Costs
PIPO	Phase In/Phase Out
POC	Point of Contact
PRS	Performance Requirements Summary
PWS	Performance Work Statement
QA	Quality Assurance
QAP	Quality Assurance Program
QASP	Quality Assurance Surveillance Plan
QC	Quality Control
QCP	Quality Control Program
SCA	Security Controls Assessor
SIPR	Secret Internet Protocol (IP) Router Network
TE	Technical Exhibit

PART 3
GOVERNMENT FURNISHED PROPERTY, EQUIPMENT, AND SERVICES

3. GOVERNMENT FURNISHED ITEMS AND SERVICES:

3.1. Services: The Government will provide administrative support to facilitate and maintain the necessary credentials, installation and building access, and network accounts.

3.2 Facilities The Government will provide the necessary workspace for the contractor staff to provide the support outlined in the PWS to include desk space, telephones, SIPR computer access, and other items necessary to maintain an office environment.

3.3 Utilities: The Government will provide, utilities in the facility for the contractor's use in performance of tasks outlined in this PWS. The Contractor shall instruct employees in utilities conservation practices. The contractor shall be responsible for operating under conditions that preclude the waste of utilities, which include turning off the water faucets or valves after using the required amount to accomplish cleaning vehicles and equipment.

3.4 Equipment: The Government will provide access to shared multi-functional devices for scanning and printing.

PART 4
CONTRACTOR FURNISHED ITEMS AND SERVICES

4. CONTRACTOR FURNISHED ITEMS AND RESPONSIBILITIES:

4.1 General : The Contractor shall furnish all supplies, equipment, facilities and services required to perform work under this contract that are not listed under Section 3 of this PWS.

4.2 Equipment). The Contractor shall provide and maintain MCEN compatible end-user devices (e.g., laptops/workstations, with monitors and all peripheral equipment) for imagining and sole use on government unclassified networks.

PART 5
SPECIFIC TASKS

Instructions to Offerors: Offeror shall fill out this section describing the tasks/subtasks they propose for this effort in order to meet the Statement of Objectives (SOO) provided in the RFP. The "Contract Overall Objectives" listed in SOO Section 3.0 must be covered by the Offerors proposed tasks/subtasks. This section shall include a proposed Work Breakdown Structure (WBS). An example of a WBS is:

- *Task 1 "XXXXXXX"*
  - *Subtask 1.1 "XXXXXX"*
  - *Subtask 1.2 "XXXXXX"*
- *Task 2 "XXXXXXX"*
  - *Subtask 2.1 "XXXXXX"*
  - *Subtask 2.2 "XXXXXX"*
- *Task 3 "XXXXXXX"*
  - *Subtask 3.1 "XXXXXX"*
  - *Subtask 3.2 "XXXXXX"*

5. Specific Tasks:

5.1. Basic Services. The contractor shall provide services for [*Insert the services and/or tasks to be provided by the contractor*].

5.2. Task Heading. **(***If applicable) [Insert the specific task to be provided in sequential order, i.e.,5.2, 5.3, etc. by the contractor]*

PART 6
APPLICABLE PUBLICATIONS

6. **APPLICABLE PUBLICATIONS (CURRENT EDITIONS)** *(If applicable)*: *(In this section list any publications, manuals, and/or regulations that the contractor must abide by. See example provided below.)*

6.1. The contractor shall apply, as appropriate, Marine Corps, DON and the DoD policies, procedures, and technical communication requirements as defined under the following or most recent version publications., which can be found through the Defense Technical Information Center (DTIC) portal at www.dtic.mil.

Federal

Title 10 of the United States Code, §2010
Title 10 of the United States Code, Chapter 47, §2010
Title 18 of the United States Code, §2006
Title 5 United States Code, Section 552a
Title 10 of the United States Code
Title 18 of the United States Code
Title 5 United States Code
Public Law 107-347, Section 208, E-Government Act of 2002, 17 December 2002
Public Law No: 113-283, Federal Information Security Modernization Act of 2014, 28 December 2014
Executive Order 12333, United States Intelligence Activities, 4 December 1981
Homeland Security Presidential Directive-7, Critical Infrastructure Identification, Prioritization, and Protection
ICD 705, Sensitive Compartmented Information Facilities, 26 May 2010
ICD 503, Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation, 15 September 2008
FIPS 140-2, Security Requirements for Cryptographic Modules, 25 May 2001
CNSS Instruction,1253, Security Categorization and Control Selection for National Security Systems, October 2009
CNSS Instruction 4009, Committee on National Security Systems (CNSS) Glossary, April 6, 2015
Executive Order 13556, Controlled Unclassified Information, November 04, 2010
NIST Special Publication 800-18, Revision A, Guide for Developing Security Plans for Federal Information Systems
NIST Special Publication 800-27, Revision A, Engineering Principles for Information Technology Security
NIST Special Publication 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems
NIST Special Publication 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems
NIST Special Publication 800-40 Revision 3, Guide to Enterprise Patch Management Technologies

NIST Special Publication 800-53, Revision 3, Recommended Security Controls for Federal Information Systems
NIST Special Publication 800-54A, Guide for Assessing the Security Controls in Federal Information Systems
NIST Special Publication 800-60, Revision 1, Guide for Mapping Types of Information and Information Systems to Security Categories
NIST Special Publication 800-61, Revision 1, Computer Security incide3nt Handling Guide
NIST Special Publication 800-128, Guide for Security-Focused Configuration Management of Information Systems
NIST 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations, September 2011
OMB Memorandum 04-04, E-Authentication Guidance for Federal Agencies
OMB Memorandum 06-16, Protection of Sensitive Agency Information
OMB Memorandum 06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments, 12 July 2006
OMB Circular A-123, Management's Responsibility for Internal Control Systems, Revised 21 December 2004
OMB Circular A-130 Appendix III, Security of Federal Automated Information Resources, 28 November 2000

DoD

DoDI 8500.01, Cybersecurity, 14 March 2014
DoDI 8500.1, Risk Management Framework (RMF) for DoD Information Technology (IT), 14 March 2016
DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), 24 May 2016, as amended
DODD 5205.02E, DoD Operations Security (OPSEC) Program, June 20, 2012 September
DODD 8000.1, Management of the Department of Defense Information Enterprise (DoD IE), March 17, 2016
DoDD 8100.2, Use of Commercial Wireless Devices, Services, and Technologies in the DoD Global Information Grid (GIG), 14 Apr 2004
DoDI 8580.1, Information Assurance3 (IA) in the Defense Acquisition System, 09 July 2004
DoDI 8580.02, Security of Individually Identifiable Health Information in DoD Health Care Programs, 12 August 2015
DoDI 8530.01, Cybersecurity Activities Support to DoD Information Network Operations, 07 March 2016
DoD Information System Certification and Accreditation Reciprocity Memo, 23 July 09
DoDM 5200.01 Vol 1, DoD Information Security Program: Overview, Classification and Declassification,
February 24, 2012
DoDM 5200.01 Vol 2 (Ch2), DoD Information Security Program: Marking of Classified Information, March 19, 2013

DoDM 5200.01 Vol 3, DoD Information Security Program: Protection of Classified Information, March 19, 2013
DoDM 5200.01 Vol 4, DoD Information Security Program: Controlled Unclassified Information (CUI), February 24, 2012
DoDM 8570.1-M Change 4, Information Assurance Workforce Improvement Program, 10 November 2015
DoDI 8551.01, Ports, Protocols, and Services Management (PPSM), 13May 28, 201413 August
9 March
DoDI 8530.01, Cybersecurity Activities Support to DoD Information Network 9Operations, 7 March, 2016
DoD O-8530.2-M, Department of Defense Computer Network Defense (CND) Service Provider Certification and Accreditation Process, 17 December2003

Joint Chiefs of Staff
CJCSI 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND), 9 February 2011 (Current as of 9 Jun 2015)
CJCSI 6211.02D, DISN Responsibilities, 24 January 2014 (Current as of 4 Aug 2015)

SECNAV/DON
SECNAV Instruction 5510.36A, Department of the Navy (DON) Information Security Program (ISP) Instruction, 6 October 2006
SECNAVINST 5239.C3C, Department of the Navy Cybersecurity Policy02Policy, 02 May, 2016
May16SECNAV M-5510.30, Department of the Navy Personnel Security Program, June 2006
SECNAVINST 5000.36A, Department of the Navy Information Technology Applications and Data Management, 19 December 2005
EKMS 1B, Electronic Key Management System (EKMS) Policy and Procedures for Navy EKMS Tiers 2 & 3, 10 June 2017
EKMS 1B SUPP-1A, Interim Policy and Procedures for Accounts Transitioning to the Key Management Infrastructure, June 2019
EKMS 3D, Communications Security (COMSEC) Material System (CMS) Central Office of Record (COR) Audit Manual, 06 February 2015
EKMS 5A, Cryptographic Equipment Information/Guidance Manual, June 2017
EKMS for Commanding Officer's Handbook, February 2015

Marine Corps
MCO 5239.B2B, Marine Corps Cybersecurity, 05 November 2015
MCO 5400.52, DON Deputy Chief Information Officer Marine Corps Roles and Responsibilities, 5 January 2010
MCO 2281.1A, Marine Corps EKMS Policy, June 2017
Marine Corps Enterprise Cybersecurity Manual Series:
ECSM 001 Computer Security Incident Handling, version 2, 8 August2012
ECSM 002 Firewalls, version 2.1, 11 June2012
ECSM 003 Routers, version 2.0, 30 September2011

ECSM 004 Remote Access Systems (RAS), version 2.0, 1 December2013
ECSM 005 Portable Electronic Devices, version 2.0, 15 March2012 (need to update)
ECSM 006 Virtual Private Networks, version 2.0, 15 September 2011
ECSM 009 NATO Information Handling on the MCEN, version 3.0, 15 August2012
ECSM 011 Personally Identifiable Information, version 4.0, 30 April2013
ECSM 013 Public Key Infrastructure (PKI), version 1, 28 February 2017
ECSM 018 Marine Corps Certification and Accreditation Process, version 3.0, 7 December 2012
ECSM 020 Marine Corps Information Assurance Vulnerability Management Program, version 1.0, 31 December2013
ECSM 021 Ports, Protocols, and Services Management, version 1.0, 15 May2012
ECSM 023 Cross Domain Solutions, version 1.0, 31 March2012
ECSM 026 CONOP for Host Based Security Service, version 1.0, 15 October2012

NATO

NATO Directive on Security C-M (2002) 49, July 2007
DUSD Memorandum 05 DEC 2001, Facilitating Necessary Access to NATO Classified Information
Memorandum for all U.S. NATO Sub Registry Control Officers, Handling of NATO Restricted Information, 28 July 1988
JSDJ6 Message, R141927Z MAY 02, Implementation Message Authorizing NATO Information on SIPRNET (Corrected Copy)

PART 7
ATTACHMENT/TECHNICAL EXHIBIT LISTING

7. <u>Attachment/Technical Exhibit List</u>:

7.1. Attachment 1/Technical Exhibit 1 – Performance Requirements Summary
7.2. Attachment 2/Technical Exhibit 2 – Deliverables Schedule
7.3 Attachment 3/Technical Exhibit 3 – Estimated Workload Data

TECHNICAL EXHIBIT 1

Performance Requirements Summary

The contractor service requirements are summarized into performance objectives that relate directly to mission essential items. The performance threshold briefly describes the minimum acceptable levels of service required for each requirement. These thresholds are critical to mission success.

Performance Objective (The Service required—usually a shall statement)	**Standard**	**Performance Threshold** (This is the maximum error rate. It could possibly be "Zero deviation from standard")	**Method of Surveillance**
PRS #1: A&A package assessment	The contractor shall provide a completed assessment within 10 business day of package receipt with documented analysis and recommendation.	The maximum error rate tolerance will be 10%. The PRS shall be on time, legible, updated and complete with 90% accuracy.	The method of surveillance will be based upon random sampling of work product by government SMEs and evaluation of effectiveness based upon metrics.
PRS #2: The contractor shall provide documented guidance, workflows change request proposal, and reports of risk status associated with those changes to the C&A process for the review, analysis, and recommendations for target activities to obtain Authorization to Operate (ATO) on the Marine Corps Enterprise Network (MCEN).	The contractor shall provide a completed change request proposal (CRP) within 3 business day of the contractor completion quality control review. The completed CRP shall be delivers with less than 10% errors. The error shall be define as CRP which lack of quality control, documented assumption, analysis, risk, alternatives, and impacts.	The maximum error rate tolerance will be 10%. The PRS shall be on time, legible, updated and complete with 90% accuracy.	The method of surveillance will be based upon random sampling of work product by government SMEs and evaluation of effectiveness based upon metrics.

PRS #3: Plan, develop and maintain training, including the competency standards, key objectives, qualifications, and curriculum in a training framework on the USMC implementation and processing of the Risk Management Framework (RMF) standard.	The contractor shall provide a plan including the schedule and milestones of development and maintenance of the training within 120 business day of contract award. The contractor shall provide an approved training within 364 business day of contract award. If required, any updates shall be submitted no more than 90 days.	The maximum error rate tolerance will be 10%. The PRS shall be on time, legible, updated and complete with 90% accuracy.	The method of surveillance will be based upon random sampling of work product by government SMEs and evaluation of effectiveness based upon metrics.
PRS #4: The contractor shall provide services support to Communication Security (COMSEC) Key Management Infrastructure (KMI) equipment accounting, inventory reconciliation, equipment disposition, and replacement of Marine Corps cryptographic equipment.	The contractor shall provide each report on a monthly basis within 5 business day from the end of the previous month.	The maximum error rate tolerance will be 10%. The PRS shall be on time, legible, updated and complete with 90% accuracy.	The method of surveillance will be based upon random sampling of work product by government SMEs and evaluation of effectiveness based upon metrics.
PRS #5: Cyber assessment to analyze MCEN cybersecurity controls	The contractor shall provide initial findings report within 5 business days of end of assessment and final recommendation report within 10 business days of end of assessment.	The maximum error rate tolerance will be 10%. The PRS shall be on time, legible, updated and complete with 90% accuracy.	The method of surveillance will be based upon random sampling of work product by government SMEs and evaluation of effectiveness based upon metrics.
PRS #6: Assessment of the MCEN (NIPR, SIPR, legacy, tactical)	The contractor shall provide initial findings report within 5 business days of end of assessment and final recommendation report within 10 business days of end of assessment.	The maximum error rate tolerance will be 10%. The PRS shall be on time, legible, updated and complete with 90% accuracy.	The method of surveillance will be based upon random sampling of work product by government SMEs and evaluation of effectiveness

			based upon metrics.
PRS #7: Identification of cybersecurity risks	The contractor shall provide initial findings report within 5 business days of end of assessment and final recommendation report within 10 business days of end of assessment.	The maximum error rate tolerance will be 10%. The PRS shall be on time, legible, updated and complete with 90% accuracy.	The method of surveillance will be based upon random sampling of work product by government SMEs and evaluation of effectiveness based upon metrics.
PRS #8: On site and remote compliance checking of systems and applications, and security reviews of application hosting environments	The contractor shall provide initial findings report within 5 business days of end of assessment and final recommendation report within 10 business days of end of assessment.	The maximum error rate tolerance will be 10%. The PRS shall be on time, legible, updated and complete with 90% accuracy.	The method of surveillance will be based upon random sampling of work product by government SMEs and evaluation of effectiveness based upon metrics.
PRS #9: Conducting security documentation reviews, physical and traditional security assessments, compliance checking of applicable technology areas, systems and applications both remote and on-site	The contractor shall provide initial findings report within 5 business days of end of assessment and final recommendation report within 10 business days of end of assessment.	The maximum error rate tolerance will be 10%. The PRS shall be on time, legible, updated and complete with 90% accuracy.	The method of surveillance will be based upon random sampling of work product by government SMEs and evaluation of effectiveness based upon metrics.
PRS #10: Assessment of Industrial Control Systems/Supervisory Control and Data Acquisition (ICS/SCADA) and Facility-Related	The contractor shall provide initial findings report within 5 business days of end of assessment and final recommendation report within 10 business days of end of assessment.	The maximum error rate tolerance will be 10%. The PRS shall be on time, legible,	The method of surveillance will be based upon random sampling of work product

Control Systems (FRCS) systems on the MCEN.		updated and complete with 90% accuracy.	by government SMEs and evaluation of effectiveness based upon metrics.
PRS #11: Automated source code review for web based systems and application on MCEN analyze results	The contractor shall provide initial findings report within 5 business days of end of assessment and final recommendation report within 10 business days of end of assessment.	The maximum error rate tolerance will be 10%. The PRS shall be on time, legible, updated and complete with 90% accuracy.	The method of surveillance will be based upon random sampling of work product by government SMEs and evaluation of effectiveness based upon metrics.
PRS #12: Application and web application penetration testing analyze results	The contractor shall provide initial findings report within 5 business days of end of assessment and final recommendation report within 10 business days of end of assessment.	The maximum error rate tolerance will be 10%. The PRS shall be on time, legible, updated and complete with 90% accuracy.	The method of surveillance will be based upon random sampling of work product by government SMEs and evaluation of effectiveness based upon metrics.
PRS #13: Harvest, review, and report metadata about Marine Corps on MCEN and public internet on known exploit posting sites and report Marine Corps exploits	The contractor shall provide initial findings report within 5 business days of end of assessment and final recommendation report within 10 business days of end of assessment.	The maximum error rate tolerance will be 10%. The PRS shall be on time, legible, updated and complete with 90% accuracy.	The method of surveillance will be based upon random sampling of work product by government SMEs and evaluation of effectiveness based upon metrics.

PRS #14: Develop, maintain and delivery of Cybersecurity Assessment Methodology training	The contractor shall provide a plan including the schedule and milestones of development and maintenance of the training within 120 business day of contract award. The contractor shall provide an approved training within 364 business day of contract award. If required, any updates shall be submitted no more than 90 days.	The maximum error rate tolerance will be 10%. The PRS shall be on time, legible, updated and complete with 90% accuracy.	The method of surveillance will be based upon random sampling of work product by government SMEs and evaluation of effectiveness based upon metrics.
PRS #15: Proposed Project Plan	The contractor shall provide the plan of work no later than five (5) business days after contract award	The maximum error rate tolerance will be 10%. The PRS shall be on time, legible, updated and complete with 90% accuracy.	The method of surveillance will be based upon random sampling of work product by government SMEs and evaluation of effectiveness based upon metrics.
PRS #16: Personnel Management Plan	The contractor shall provide the management plan for staffing, directing, and reporting no later than five (5) business days after contract award and update every 365 days from initial submission.	The maximum error rate tolerance will be 10%. The PRS shall be on time, legible, updated and complete with 90% accuracy.	The method of surveillance will be based upon random sampling of work product by government SMEs and evaluation of effectiveness based upon metrics.
PRS #17: Weekly Status Report	The contractor shall provide activity reports weekly every Friday, by 3:00 pm (ET) unless until the contract expires	The maximum error rate tolerance will be 10%. The PRS shall be on time, legible, updated and complete with 90% accuracy.	The method of surveillance will be based upon random sampling of work product by government SMEs and evaluation of effectiveness

			based upon metrics.
PRS #18: Monthly Status Report	The contractor shall provide summary monthly reports by 3:00 pm (ET) on 10th calendar day after end of previous month	The maximum error rate tolerance will be 10%. The PRS shall be on time, legible, updated and complete with 90% accuracy.	The method of surveillance will be based upon random sampling of work product by government SMEs and evaluation of effectiveness based upon metrics.
PRS #19: Monthly Regional Assessment Reports	The contractor shall provide cumulative monthly reports by 3:00 pm (ET) on 10th calendar day after end of previous month	The maximum error rate tolerance will be 10%. The PRS shall be on time, legible, updated and complete with 90% accuracy.	The method of surveillance will be based upon random sampling of work product by government SMEs and evaluation of effectiveness based upon metrics.
PRS #20: Mitigation and Remediation Recommendation Report	The contractor shall provide cumulative monthly reports by 3:00 pm (ET) on 10th calendar day after end of previous month	The maximum error rate tolerance will be 10%. The PRS shall be on time, legible, updated and complete with 90% accuracy.	The method of surveillance will be based upon random sampling of work product by government SMEs and evaluation of effectiveness based upon metrics.
PRS #21: Marine Corps Web Risk Assessment Cell (MCWRAC) Report	The contractor shall provide initial findings report within 5 business days of end of assessment and final recommendation report within 10 business days of end of assessment.	The maximum error rate tolerance will be 10%. The PRS shall be on time, legible,	The method of surveillance will be based upon random sampling of work product

		updated and complete with 90% accuracy.	by government SMEs and evaluation of effectiveness based upon metrics.
PRS #22: Web Application Penetration Testing Result Memo	The contractor shall provide initial findings report within 5 business days of end of assessment and final recommendation report within 10 business days of end of assessment.	The maximum error rate tolerance will be 10%. The PRS shall be on time, legible, updated and complete with 90% accuracy.	The method of surveillance will be based upon random sampling of work product by government SMEs and evaluation of effectiveness based upon metrics.
PRS #23: Web Application Penetration Testing Remediation and Mitigation Memo	The contractor shall provide initial findings report within 5 business days of end of assessment and final recommendation report within 10 business days of end of assessment.	The maximum error rate tolerance will be 10%. The PRS shall be on time, legible, updated and complete with 90% accuracy.	The method of surveillance will be based upon random sampling of work product by government SMEs and evaluation of effectiveness based upon metrics.
PRS #24: Accreditation Documentation	By package initial report of status due 2 business days of assignment with final recommendation within 2 business days of final documentation updates submitted by requestor.	The maximum error rate tolerance will be 10%. The PRS shall be on time, legible, updated and complete with 90% accuracy.	The method of surveillance will be based upon random sampling of work product by government SMEs and evaluation of effectiveness based upon metrics.

PRS #25: Marine Corps CY Assessment Team Schedules	30 days after contract award with quarterly updates until the contract expires	The maximum error rate tolerance will be 10%. The PRS shall be on time, legible, updated and complete with 90% accuracy.	The method of surveillance will be based upon random sampling of work product by government SMEs and evaluation of effectiveness based upon metrics.
PRS #26: COMSEC Inventory Management, Tracking & Reviews Daily Report	Daily by 5:00 pm (ET) unless until the contract expires	The maximum error rate tolerance will be 10%. The PRS shall be on time, legible, updated and complete with 90% accuracy.	The method of surveillance will be based upon random sampling of work product by government SMEs and evaluation of effectiveness based upon metrics.
PRS #27: COMSEC Account Reconciliation Report	Weekly, every Friday by 3:00 pm (ET) unless until the contract expires	The maximum error rate tolerance will be 10%. The PRS shall be on time, legible, updated and complete with 90% accuracy.	The method of surveillance will be based upon random sampling of work product by government SMEs and evaluation of effectiveness based upon metrics.
PRS #28: Documentation of status of account and inventory for KMI program.	The contractor shall provide cumulative monthly reports by 3:00 pm (ET) on 10th calendar day after end of previous month	The maximum error rate tolerance will be 10%. The PRS shall be on time, legible, updated and complete with 90% accuracy.	The method of surveillance will be based upon random sampling of work product by government SMEs and evaluation of effectiveness

			based upon metrics.
PRS #29: COMSEC Error & Reconciliation Logs	Weekly, every Friday by 3:00 pm (ET) unless until the contract expires	The maximum error rate tolerance will be 10%. The PRS shall be on time, legible, updated and complete with 90% accuracy.	The method of surveillance will be based upon random sampling of work product by government SMEs and evaluation of effectiveness based upon metrics.
PRS #30: COMSEC Records Clearance Certificates (RCC)	Weekly, every Friday by 3:00 pm (ET) unless until the contract expires	The maximum error rate tolerance will be 10%. The PRS shall be on time, legible, updated and complete with 90% accuracy.	The method of surveillance will be based upon random sampling of work product by government SMEs and evaluation of effectiveness based upon metrics.
PRS #31: Training Plan	30 days after contract award with quarterly updates unless/until the contract expires	The maximum error rate tolerance will be 10%. The PRS shall be on time, legible, updated and complete with 90% accuracy.	The method of surveillance will be based upon random sampling of work product by government SMEs and evaluation of effectiveness based upon metrics.
PRS #32: After Action Report	The contractor shall provide reports by 3:00 pm (ET) on 5th calendar day after end of previous month	The maximum error rate tolerance will be 10%. The PRS shall be on time, legible,	The method of surveillance will be based upon random sampling of work product

		updated and complete with 90% accuracy.	by government SMEs and evaluation of effectiveness based upon metrics.
PRS #33: Standard Operating Procedures (SOP)	120 days after contract award with 180 day updates unless/until the contract expires	The maximum error rate tolerance will be 10%. The PRS shall be on time, legible, updated and complete with 90% accuracy.	The method of surveillance will be based upon random sampling of work product by government SMEs and evaluation of effectiveness based upon metrics.
PRS #34: Training Status	The contractor shall provide reports by 3:00 pm (ET) on 10th calendar day after end of previous month	The maximum error rate tolerance will be 10%. The PRS shall be on time, legible, updated and complete with 90% accuracy.	The method of surveillance will be based upon random sampling of work product by government SMEs and evaluation of effectiveness based upon metrics.

TECHNICAL EXHIBIT 2

DELIVERABLES SCHEDULE

Item No.	Deliverable	Objective	Due
1	Proposed Project Plan	Defining the responsibilities, timeline, risks, and milestones of contract objectives.	No later than five (5) business days after contract award

2	Personnel Management Plan	Managerial plan for personnel planning, organizing, directing and controlling based upon the PWS and implementation of all these managerial activities.	No later than five (5) business days after contract award
3	Weekly Status Report	Report documenting tasks & issues weekly.	Weekly, every Friday, by 3:00 pm (ET) unless until the contract expires
4	Monthly Status Report	Monthly project report documenting tasks issues and status of ODCs identified during the month	10th calendar after end of previous month
5	Monthly Regional Assessment Reports	Monthly cumulative of all assessments by region Cumulative statistics of assessments by region since beginning of the contract	10th calendar after end of previous month
6	Mitigation and Remediation Recommendation Report	Report of all new mitigation and remediation recommendations Cumulative status of all mitigation and remediation recommendations Metrics associated with mitigation and remediation recommendations	10th calendar after end of previous month
7	MCWRAC Report	Report of assessment of individual application, site, or system	5th calendar day after end of assessment
8	Web Application Penetration Testing Result Memo	Report of assessment of individual application site or system	5th calendar day after end of assessment
9	Web Application Penetration Testing Remediation and Mitigation Memo	Memo of mitigation and remediation recommendations by individual application or system	5th calendar day after end of assessment
10	Accreditation Documentation	Report of evaluation of system, application or exercise with recommendation for approval determination.	Weekly, every Friday, by 3:00 pm (ET) unless until the contract expires
11	Security Evaluation	Report of evaluation of system, application or exercise with recommendation for approval determination.	Weekly, every Friday, by 3:00 pm (ET) unless until the contract expires
12	Marine Corps CY Assessment Team Schedules	Plan of schedule assessments and review planning to include time, scope and follow up actions.	30 days after contract award with quarterly updates unless/until the contract expires
13	COMSEC Inventory Management, Tracking	Documentation of status of account and inventory for KMI program.	Weekly, every Friday, by 3:00 pm (ET) unless until the contract expires

	& Reviews Daily Report		
14	COMSEC Account Reconciliation Report	Documentation of status of account and inventory for KMI program.	Weekly, every Friday, by 3:00 pm (ET) unless until the contract expires
15	COMSEC Error & Reconciliation Logs	Documentation of status of account and inventory for KMI program.	Weekly, every Friday, by 3:00 pm (ET) unless until the contract expires
16	COMSEC Records Clearance Certificates (RCC)	Required COMSEC document for the KMI program.	Weekly, every Friday, by 3:00 pm (ET) unless until the contract expires
17	Training Plan	Document that communicates to management and stakeholders details of the. proposed training program	30 days after contract award with quarterly updates unless/until the contract expires
18	After Action Report	Document to codify the purpose, background, situation, outcome and proposed next steps or actions.	5 days after need of action
19	Standard Operating Procedures (SOP)	Document which codifies set of written instructions that describes the step-by-step process that must be taken to properly perform a	120 days after contract award with 180 day updates unless/until the contract expires
20	Training Status	Report of capability training development, implementation and schedule.	10th calendar day after the end of the previous month
21	Quality Control Plan	A final QCP shall be developed, maintained and submitted after contract award.	30 days after contract award.

TECHNICAL EXHIBIT 3

ESTIMATED WORKLOAD DATA

This technical exhibit lists the historical workload data, on the previous contract and the projected estimated workload data for this RFP requirement. It is noted that this information being provided is ONLY ESTIMATES; actual workload may vary during performance. Adjustments in actual workload during performance will not be subject to changes in contract price.

ITEM # and Name	Historical Workload Data	Estimated Workload Data
PRS #1: A&A package assessment	- 12 Package Accreditation Support Decision Documents monthly - 12 concurrent package reviews in progress monthly - 22 monthly Customer Support Request tickets processed	- 13 final Package Accreditation Support Decision documents monthly - 13 concurrent package reviews in progress monthly -24 completed Customer Support request tickets monthly
PRS #2: The contractor shall provide documented guidance, workflows change request proposal, and reports of risk status associated with those changes to the A&A process for the review, analysis, and recommendations for target activities to obtain Authorization to Operate (ATO) on the Marine Corps Enterprise Network (MCEN).	- 9 concurrent reviews monthly - 22 monthly Customer submitted Support Request Tickets requiring research, analysis, and response resulting in progress toward the accreditation goals of the command	-10 concurrent reviews monthly -23 monthly Customer submitted Support Request Tickets requiring research, analysis, and response resulting in progress toward the accreditation goals of the command
PRS #3: Plan, develop and maintain of training including the competency standards, key objectives, qualifications, and curriculum in a training framework on the USMC implementation and processing of Risk Management Framework (RMF) standard.	- 10 Information Systems Support Personnel courseware periods of instruction for 10 to 100 personnel per course - 4 curriculum updates per year to reflect changes to RMF policy, practice, and implementation	11 Information Systems Support Personnel courseware periods of instruction for 10 to 100 personnel per course - 5 curriculum updates per year to reflect changes to RMF policy, practice, and implementation
PRS #4: The contractor shall provide services support to Communication Security (COMSEC) Key Management Infrastructure (KMI) equipment accounting, inventory reconciliation, equipment disposition, and replacement of Marine Corps cryptographic equipment.	88 KMI Accounts 1 NSA Account 295,000 devices	90 KMI Accounts 295,000 devices
PRS #5: Cyber assessment to analyze MCEN cybersecurity controls	-12 NIPR Enterprise Assessments (1 per month)	-12 NIPR Enterprise Assessments (1 per month)

	- 12 SIPR Enterprise Assessments (1 per month) - 52 ACAS Regional assessments (1 per week) - 10 ad hoc system or application vulnerability assessments annually (4-10 days each)	- 12 SIPR Enterprise Assessments (1 per month) - 52 ACAS Regional assessments (1 per week) - 10 ad hoc system or application vulnerability assessments annually (4-10 days each) - 5 SCADA or FRCS assessments: estimate is 3-6 assessments per year, 3-7 days each.
PRS #6: Assessment of the MCEN risk (NIPR, SIPR, legacy, tactical)	-12 NIPR Enterprise Assessments (1 per month)- 12 SIPR Enterprise Assessments (1 per month) - 52 ACAS Regional assessments (1 per week per region) - 10 ad hoc system or application vulnerability assessments annually (4-10 days each)	-12 NIPR Enterprise Assessments (1 per month) - 12 SIPR Enterprise Assessments (1 per month) - 52 ACAS Regional assessments (1 per week) - 10 ad hoc system or application vulnerability assessments annually (4-10 days each) - 5 ICS per SCADA or FRCS assessments annually, 3-7 days each - 3 Tactical enclave assessments, annually (3-7 days each)
PRS #7: Identification of cybersecurity risks	-12 NIPR Enterprise Assessments (1 per month)- 12 SIPR Enterprise Assessments (1 per month) - 52 ACAS Regional assessments (1 per week) - 10 ad hoc system or application vulnerability assessments annually (4-10 days each)	-12 NIPR Enterprise Assessments (1 per month) - 12 SIPR Enterprise Assessments (1 per month) - 52 ACAS Regional assessments (1 per week per region) - 10 ad hoc system or application vulnerability assessments annually (4-10 days each) - 4SCADA/FRCS assessments annually, 3-7 days each
PRS #8: On site and remote compliance checking of systems and applications, and security reviews of application hosting environments	-12 NIPR Enterprise Assessments (1 per month) - 12 SIPR Enterprise Assessments (1 per month) - 52 ACAS Regional assessments (1 per week)	-12 NIPR Enterprise Assessments (1 per month) - 12 SIPR Enterprise Assessments (1 per month) - 52 ACAS Regional assessments (1 per week)
PRS #9: Conducting security documentation reviews, physical and traditional security assessments, compliance checking of applicable technology areas, systems and applications both remote and on-site	- 2 formalized site/command cyber assessments, 1-2 week long. - 2 annual, targeted or requested assessments, in response to emerging threats or risks.	- 4 formalized site/command cyber assessments, 1-2 week long. - 2 annual, targeted or requested assessments, in response to emerging threats or risks.
PRS #10: Assessment of Industrial Control Systems per Supervisory Control and Data Acquisition (ICS per SCADA) and Facility-Related Control	N/A	4 system assessments annually (3-7 days each)

Systems (FRCS) systems on the MCEN.		
PRS #11: Automated source code review for web- based systems and application on MCEN analyze results	3 Source Code Reviews of web applications	4 Source Code Reviews of web applications
PRS #12: Application and web application penetration testing analyze results	- 5 public-facing web-based systems per month - - 3-4 targeted web system assessments annually	- 5-10 public-facing web-based systems per month - 4 formalized site/command cyber assessments, 1-2 week long. - 3-4 targeted web system assessments annually
PRS #13: Harvest, review, and report metadata about Marine Corps on MCEN and public internet on known exploit posting sites and report Marine Corps exploits	- 5-10 sites per systems per month Included as part of scheduled monthly assessments.	- 5-10 sites per systems per month Included as part of scheduled monthly assessments.
PRS #14: Develop, maintain and delivery of Cybersecurity Assessment Methodology training	- 4 curriculum updates per year to reflect changes to policy, practice, and implementation - 3 Formal training sessions (on site, 1-week) annually - 312 Ad hoc local requested training (2-4 hours per week per region.	- 4 curriculum updates per year to reflect changes to policy, practice, and implementation - 3 Formal training sessions (on site, 1-week) annually - 312 Ad hoc local requested training (2-4 hours per week per region
PRS #15: Proposed Project Plan	1 per contract award	1 per contract option period award
PRS #16: Personnel Management Plan	1 per contract award	1 per contract award
PRS #17: Weekly Status Report	1 per task weekly	1 per task weekly
PRS #18: Monthly Status Report	12 per year	12 per year
PRS #19: Monthly Regional Assessment Reports	12 Monthly Global Vulnerability Assessment Reports	12 Monthly Global Vulnerability Assessment Reports
PRS #20: Mitigation and Remediation Recommendation Report	12 Monthly Global Vulnerability Assessment Reports include mitigation and remediation recommendations.	12 Monthly Global Vulnerability Assessment Reports include mitigation and remediation recommendations
PRS #21: MCWRAC Report	12 Monthly Web Risk Assessment reports (5-10 system assessments each) - Targeted or requested systems assessments (5-10 per year).	12 Monthly Web Risk Assessment reports (5-10 system assessments each) - Targeted or requested systems assessments (5-10 per year).
PRS #22: Web Application Penetration Testing Result Memo	- Pen testing results included in 12 Monthly MCWRAC Report - Individual reports per targeted or requested systems assessment (5-10 per year).	- Pen testing results included in 12 Monthly MCWRAC Report - Individual reports per targeted or requested systems assessment (5-10 per year).

PRS #23: Web Application Penetration Testing Remediation and Mitigation Memo	- Pen testing remediation and mitigation recommendations included in 12 Monthly MCWRAC Report. - Individual reports per targeted or requested systems assessment (5-10 per year).	- Pen testing remediation and mitigation recommendations included in 12 Monthly MCWRAC Report. - Individual reports per targeted or requested systems assessment (5-10 per year).
PRS #24: Accreditation Documentation	48 Accreditation Documents per year	51 Accreditation Documents per year
PRS #25: Marine Corps CY Assessment Team Schedules	1 report input provided monthly	1 report input provided monthly
PRS #26: COMSEC Inventory Management, Tracking & Reviews Daily Report	1 report update weekly	1 report update weekly
PRS #27: COMSEC Account Reconciliation Report	1 report update weekly	1 report update weekly
PRS #28: Documentation of status of account and inventory for KMI program.	1 report input provided monthly	1 report input provided monthly
PRS #29: COMSEC Error & Reconciliation Logs	Daily transitional report	Daily transitional report
PRS #30: COMSEC Records Clearance Certificates (RCC)	Weekly report 5 per week	Weekly report 5 per week
PRS #31: Training Plan	- 3 Formal training sessions (on site, 1-week) annually - 52 Ad hoc per targeted per requested local training (2-4 hours per week per region. - 6 A&A package Assessor 3 day via TEAMS	- 3 Formal training sessions (on site, 1-week) annually - 52 Ad hoc per targeted per requested local training (2-4 hours per week per region. - 9 A&A package Assessor 3 day via TEAMS
PRS #32: After Action Report	1 per event, assessment, or meeting	1 per event, assessment, or meeting
PRS #33:Standard Operating Procedures (SOP)	1 per Regional Assessment location 1 MCWRAC 1 A&A Package Assessor 1 per training package 1 KMI Account and Inventory Management	1 per Regional Assessment location 1 MCWRAC 1 A&A Package Assessor 1 per training package 1 KMI Account and Inventory Management
PRS #34: Training Status	N/A	Integrated into Master Schedule reported monthly