PWS

Headquarters United States Pacific Command
(HQ USPACOM)

INFORMATION TECHNOLOGY AND OPERATIONS SUPPORT

Performance Work Statement

Supporting

HQ USPACOM Command, Control, Communications, and Cyber Directorate (HQ USPACOM J6)

PART 1 – GENERAL INFORMATION

1. GENERAL INFORMATION

1.1. Introduction

This is a non-personal services contract to provide 1) Software and Portal Support; 2) Service Desk Support; 3) Network Engineering and System Administration; 4) Telecommunications Support; 5) Electronic Key Management Support; 6) System Integration; 7) Project Management; 8) Computer Network Defense Support; 9) Enterprise Architecture Framework; 10) Assessment, Certification and Authorization; 11) Compliance; 12) Portfolio Program Support; 13) Knowledge and Information Management Support; 14) Video Teleconferencing Support; 15) Audio Visual Support; 16) Asset Management and 17) Configuration Management support to Headquarters, U.S. Pacific Command (HQ USPACOM). Hereafter, these services shall collectively be known as IT & Ops Support. 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.

1.2. Description of Services

The contractor shall provide all personnel, equipment, supplies, facilities, transportation, tools, materials, supervision, and other items and non-personal services necessary to perform IT & Ops Support as defined in this Performance Work Statement (PWS) except for those items specified as incidental property and services. The contractor shall perform to the standards in this contract.

1.3. Background

HQ USPACOM is located at Camp H.M. Smith, Oahu, Hawaii and is responsible for promoting peace, deterring aggression, responding to crisis and, if necessary, fighting and winning, to advance security and stability throughout the Asia-Pacific region.

1.4. Objectives

This PWS describes the performance requirements and quantifiable deliverables to be performed in support of the HQ USPACOM Command, Control, Communications, and Cyber (C4) Directorate (J6).

1.5. Scope

USPACOM seeks a qualified Contractor to provide IT & Ops support services. The services often have no standard process or precedent to follow, and requires research and interpretation of existing government guidance and instructions, as well as commercial business best practices.

1.6. Period of Performance

The period of performances shall be as shown in the Standard Form 1449 delivery schedule.

1.7. General Information

1.7.1. Quality Assurance: The government shall evaluate the contractor's performance under this contract in accordance with the Quality Assurance Surveillance Plan (QASP). 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).

1.7.2. Recognized Holidays: The following holidays will be observed. If the legal public holiday falls on a Sunday, the holiday is observed on the following Monday.

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

1.7.3. Hours of Operation:

Normal government business hours are 0730 through 1600 (Hawaii Standard Time), Monday through Friday, except on 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 at all times maintain an adequate workforce for the uninterrupted performance of all tasks defined within this PWS 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. Specific hours will be coordinated between the contractor and the COR.

Non-Standard Hours of Operation: Occasionally, weekend/on-call work may be required for system/software administration. Historically, this type of system administration support has been required approximately 3 times a month while software support was required once a quarter. Telephonic system support was required approximately 2 times a quarter. Each instance lasted approximately 4 hours.

Place of Performance:

Primary: Nearly all work will be performed at USPACOM/J6, Building 700, Camp H.M. Smith, Hawaii. As required, some tasks will be performed at government facilities located at the Pacific Warfighting Center (PWC) on Ford Island, Hawaii at least once annually during the contract duration. Work locations within building 700 and PWC include workspaces that are designated as Sensitive Compartmented Information Facilities (SCIF)

Alternate: In cases of unforeseen conditions or contingencies (e.g., pandemic conditions, exercises, etc.), the Government will approve operations at an alternate location within the local travel area (an alternate place of performance). Any equipment such as laptops or phones provided to Contractor personnel shall be returned at the termination of the engagement or at another time mutually agreeable to both parties. Contracting Officer Representative (COR) approval is required. To the extent possible, the contractor shall use best efforts to provide the same level of support as stated in the PWS.

1.7.4. Type of Contract/Order: The government will award a hybrid blend Firm Fixed Price (FFP) task order with a labor hour contract line item (CLIN).

1.7.5. Special Qualification (Information Assurance Workforce): U.S. Department of Defense Directive 8570.1 (August of 2004), requires every full- and part-time defense contractor with privileged access to a DoD system, to obtain a commercial certification credential that has been accredited by the American National Standards Institute (ANSI). Contract individuals supporting subtasks that require privileged access to PACOM system must comply with this requirement; specific certification levels (Information Assurance Manager (IAM) 1-3 and Information Assurance Technician (IAT) 1-3).

1.7.6. Program Management Review (PMR) Meetings: The Contractor agrees to attend any PMR meetings convened by the contracting activity 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.

1.7.7. Post Award Conference/Periodic Progress Meetings: The Contractor agrees to attend any post award conference convened by the contracting activity in accordance with Federal Acquisition Regulation Subpart 42.5. The Contracting Officer, Contracting Officers Representative, 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.

1.7.8. Contracting Officer Representative (COR): The COR will be appointed by a separate letter and identified in the contract award. The COR monitors all technical aspects of the contract and assists in contract oversight. 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 notify both the Contracting Officer and Contractor of any deficiencies; and coordinate site entry of Contractor personnel. A letter of appointment 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 contract.

1.7.9. Technical Advisor (TA): Government Technical Advisors will be assigned, in writing by the COR, for each specified task identified in Part 4, “Specific Tasks”. The TA will be responsible for coordinating with the COR for any contract actions as well as providing contract performance information to the COR. The COR will ensure that monthly reporting and TA training are completed.

1.7.10. 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.

1.7.11. Travel requirements are defined in Part 4, “Specific Tasks”.

1.7.12. Data Rights: All documents and materials, to include locally generated scripts, produced under this contract shall be Government owned and are the property of the Government with all rights and privileges of ownership/copyright belonging exclusively to the Government. These documents and materials may not be used or sold by the contractor without written permission from the Contracting Officer. All materials supplied to the Government shall be the sole property of the Government and may not be used for any other purpose. This right does not abrogate any other Government rights.

1.7.13. Enterprise-wide Contractor Manpower Reporting Application (ECMRA): The contractor shall report all contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the HQ USPACOM J6 via a secure data collection 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 October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each year.

1.8. Security and Access Requirements:

1.8.1. Security requirements are identified in Table 1: "Minimum Requirements for Firm Fixed Priced CLIN" for the minimum requirements and Table 2: "Additional Labor for Labor-Hour CLIN". The security requirement for each task outlined in Section 4, "Specific Tasks" is defined along with the estimated workload.

1.8.2. Contractor Unclassified Access to Federally Controlled Facilities, Sensitive Information, Information Technology (IT) Systems or Protected Health Information: Homeland Security Presidential Directive (HSPD)-12, requires government agencies to develop and implement Federal security standards for Federal employees and contractors. The Deputy Secretary of Defense Directive-Type Memorandum (DTM) 08-006 – "DoD Implementation of Homeland Security Presidential Directive – 12 (HSPD-12)" dated November 26, 2008 (or its subsequent DoD instruction) directs implementation of HSPD-12. This section is in accordance with HSPD-12 and its implementing directives.

1.8.2.1. Applicability: This section applies to contractor employees requiring physical access to any area of a federally controlled base, facility or activity and/or requiring access to a DoN or DoD computer/network/system to perform certain unclassified sensitive duties. This section also applies to contractor employees who access Privacy Act and Protected Health Information, provide support associated with fiduciary duties, or perform duties that have been identified by DoN as National Security Position, as advised by the command security manager. It is the responsibility of the responsible security officer of the command/facility where the work is performed to ensure compliance.

1.8.2.2. Each contractor employee providing services at a Navy Command under this contract is required to obtain a Department of Defense Common Access Card (DoD CAC). Additionally, depending on the level of computer/network access, the contract employee will require a successful investigation as detailed below.

1.8.2.3. Access to Federal Facilities: Per HSPD-12 and implementing guidance, all contractor employees working at a federally controlled base, facility or activity under this clause will require a DoD CAC. When access to a base, facility or activity is required contractor employees shall in-process with the Navy Command's Security Manager upon arrival to the Navy Command and shall out-process prior to their departure at the completion of the individual's performance under the contract.

1.8.2.4. Access to DoD IT Systems: In accordance with SECNAV M-5510.30, contractor employees who require access to DoN or DoD networks are categorized as IT-I, IT-II, or IT-III. The IT-II level, defined in detail in SECNAV M-5510.30, includes positions which require access to information protected under the Privacy Act, to include Protected Health Information (PHI). All contractor employees under this contract who require access to Privacy Act protected information are therefore categorized no lower than IT-II. IT Levels are determined by the requiring activity's Command Information Assurance Manager. Contractor employees requiring privileged or IT-I level access, (when specified by the terms of the contract) require a Single Scope Background Investigation (SSBI) which is a higher level investigation than the National Agency Check with Law and Credit (NACLC) described below. Due to the privileged system access, a SSBI suitable for High Risk public trusts positions is required. Individuals who have access to system control, monitoring, or administration functions (e.g. system administrator, database administrator) require training and certification to Information Assurance Technical Level 1, and must be trained and certified on the Operating System or Computing Environment they are required to maintain.

Access to sensitive IT systems is contingent upon a favorably adjudicated background investigation. When access to IT systems is required for performance of the contractor employee's duties, such employees shall in-process with the Navy Command's Security Manager and Information Assurance Manager upon arrival to the Navy command and shall out-process prior to their departure at the completion of the individual's performance under the contract. Completion and approval of a System Authorization Access Request Navy (SAAR-N) form is required for all individuals accessing Navy Information Technology resources. The decision to authorize access to a government IT system/network is inherently governmental. The contractor supervisor is not authorized to sign the SAAR-N; therefore, the government employee with knowledge of the system/network access required or the COR shall sign the SAAR-N as the "supervisor".

The SAAR-N shall be forwarded to the Navy Command's Security Manager at least 30 days prior to the individual's start date. Failure to provide the required documentation at least 30 days prior to the individual's start date may result in delaying the individual's start date.

When required to maintain access to required IT systems or networks, the contractor shall ensure that all employees requiring access complete annual Information Assurance (IA) training, and maintain a current requisite background investigation. The Contractor's Security Representative shall contact the Command Security Manager for guidance when reinvestigations are required.

1.8.2.5. Interim Access: The Navy Command's Security Manager may authorize issuance of a DoD CAC and interim access to a DoN or DoD unclassified computer/network upon a favorable review of the investigative questionnaire and advance favorable fingerprint results. When the results of the investigation are received and a favorable determination is not made, the contractor employee working on the contract under interim access will be denied access to the computer network and this denial will not relieve the contractor of his/her responsibility to perform.

1.8.2.6. Denial or Termination of Access: The potential consequences of any requirement under this section including denial or termination of physical or system access in no way relieves the contractor from the requirement to execute performance under the contract within the timeframes specified in the contract. Contractors shall plan ahead in processing their employees and subcontractor employees. The contractor shall insert this section in all subcontracts when the subcontractor is permitted to have unclassified access to a federally controlled facility, federally-controlled information system/network and/or to government information, meaning information not authorized for public release.

1.8.2.7. Contractor's Security Representative: The contractor shall designate an employee to serve as the Contractor's Security Representative. Within three work days after contract award, the contractor shall provide to the requiring activity's Security Manager, in writing, the name, title, address and phone number for the Contractor's Security Representative. The Contractor's Security Representative shall be the primary point of contact on any security matter. The Contractor's Security Representative shall not be replaced or removed without prior notice to the Contracting Officer and Command Security Manager.

1.8.2.8. Background Investigation Requirements and Security Approval Process for Contractors Assigned to National Security Positions or Performing Sensitive Duties: Navy security policy requires that all positions be given a sensitivity value based on level of risk factors to ensure appropriate protective measures are applied. The Dept. of the Navy recognizes contractor employees under this contract as Non-Critical Sensitive [ADP/IT-II] when the contract scope of work require physical access to a federally controlled base, facility or activity and/or requiring access to a DoD computer/network, to perform unclassified sensitive duties. This designation is also applied to contractor employees who access Privacy Act and Protected Health Information (PHI), provide support associated with fiduciary duties, or perform duties that have been identified by DON as National Security Positions. At a minimum, each contractor employee must be a U.S. citizen and have a favorably completed NACLC to obtain a favorable determination for assignment to a non-critical sensitive or IT-II position. The NACLC consists of a standard NAC and a FBI fingerprint check plus law enforcement checks and credit check. Each contractor employee filling a non-critical sensitive or IT-II position is required to complete:

- SF-86 Questionnaire for National Security Positions (or equivalent OPM investigative product)
- Two FD-258 Applicant Fingerprint Cards (or an electronic fingerprint submission)
- Original Signed Release Statements

Failure to provide the required documentation at least 30 days prior to the individual's start date shall result in delaying the individual's start date. Background investigations shall be reinitiated as required to ensure investigations remain current (not older than 10 years) throughout the contract performance period. The Contractor's Security Representative shall contact the Command Security Manager for guidance when reinvestigations are required.

Regardless of their duties or IT access requirements ALL contractor employees shall in-process with the Navy Command's Security Manager upon arrival to the Navy command and shall out-process prior to their departure at the completion of the individual's performance under the contract. Employees requiring IT access shall also check-in and check-out with the Navy Command's Information Assurance Manager. Completion and approval of a System Authorization Access Request Navy (SAAR-N) form is required for all individuals accessing Navy Information Technology resources. The SAAR-N shall be forwarded to the Navy Command's Security Manager at least 30 days prior to the individual's start date. Failure to provide the required documentation at least 30 days prior to the individual's start date shall result in delaying the individual's start date.

The contractor shall ensure that each contract employee requiring access to IT systems or networks complete annual Information Assurance (IA) training, and maintain a current requisite background investigation. Contractor employees shall accurately complete the required investigative forms prior to submission to the Navy Command Security Manager. The Navy Command's Security Manager will review the submitted documentation for completeness prior to submitting it to the Office of Personnel Management (OPM). Suitability/security issues identified by the Navy may render the contractor employee ineligible for the assignment. An unfavorable determination made by the Navy is final (subject to SF-86 appeal procedures) and such a determination does not relieve the contractor from meeting any contractual obligation under the contract. The Navy Command's Security Manager will forward the required forms to OPM for processing. Once the investigation is complete, the results will be forwarded by OPM to the DON Central Adjudication Facility (CAF) for a determination.

If the contractor employee already possesses a current favorably adjudicated investigation, the contractor shall submit a Visit Authorization Request (VAR) via the Joint Personnel Adjudication System (JPAS) or a hard copy VAR directly from the contractor's Security Representative. Although the contractor will take JPAS "Owning" role over the contractor employee, the Navy Command will take JPAS "Servicing" role over the contractor employee during the hiring process and for the duration of assignment under that contract. The contractor shall include the IT Position Category per SECNAV M-5510.30 for each employee designated on a VAR. The VAR requires annual renewal for the duration of the employee's performance under the contract.

1.8.2.9. Background Investigation Requirements and Security Approval Process for Contractors Assigned to or Performing Non-Sensitive Duties: Contractor employee whose work is unclassified and non-sensitive (e.g., performing certain duties such as lawn maintenance, vendor services, etc .) and who require physical access to publicly accessible areas to perform those duties shall meet the following minimum requirements:

- Must be either a US citizen or a US permanent resident with a minimum of 3 years legal residency in the United States (as required by The Deputy Secretary of Defense DTM 08-006 or its subsequent DoD instruction) and
- Must have a favorably completed National Agency Check with Written Inquiries (NACI) including a FBI fingerprint check prior to installation access.

To be considered for a favorable trustworthiness determination, the Contractor's Security Representative must submit for all employees each of the following:

- SF-85 Questionnaire for Non-Sensitive Positions
- Two FD-258 Applicant Fingerprint Cards (or an electronic fingerprint submission)
- Original Signed Release Statements

The contractor shall ensure each individual employee has a current favorably completed National Agency Check with Written Inquiries (NACI) or ensure successful FBI fingerprint results have been gained and investigation has been processed with OPM

Failure to provide the required documentation at least 30 days prior to the individual's start date may result in delaying the individual's start date.

* Consult with your Command Security Manager and Information Assurance Manager for local policy when IT-III (non-sensitive) access is required for non-US citizens outside the United States.

1.9. Ordering Procedures for Labor-Hour Contract Line Item Number (CLIN) for Additional Labor

1.9.1. This PWS provides the descriptions of services for performance based firm fixed price (FFP) contract line items ("minimum required services") and additional labor hours; this additional labor will be shown in the task order as a labor-hour contract line item (CLIN) with an attachment which will show the specific labor categories. See Table 2 below for a list of additional labor, labor categories and estimated level of effort. The estimated numbers level of effort is is based on historical data.

1.9.2. The labor hour contract line item number (CLIN) for additional labor will include an estimated ceiling price. *Those requirements noted "Additional Labor" may not be obligated at the time of award or exercise of options. These requirements may be executed via modification at a later date during the associated year*

contingent upon approval of the funding. Historically, when available, this funding has been provided in the third (April – June) or fourth (July – September) quarters of the respective fiscal year. If the government requires execution of the labor-hour CLIN, written notice will be provided to the contractor within 30 days before the period of performance. The labor-hour categories shall be pre-priced by the contractor and will be provided in the contract award document (SF 1449). If funding becomes available, the Contracting Officer will provide the labor category, suggested number of hours, and the associated task area to the Contractor for concurrence. A funding document will be sent to the contracting office and a modification will be issued for the additional services.

1.9.3. The additional labor is defined in Part 6, Table 2, "Additional Labor for Labor-Hour Contract Line Item Number". The estimated level of effort is not based on a full year term, and will be only for the respective period of performance in which it is executed.

PART 2 – DEFINITIONS & ACRONYMS

2. DEFINITIONS & ACRONYMS

2.1. Definitions

Contractor: A supplier or vendor having a contract to provide specific supplies or service to the government. The term used in this contract refers to the prime.

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.

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.

Technical Assistant (TA): The requiring activity representative who may be assigned to provide technical/administrative assistance to the COR. TAs may be assigned to assist and support the COR, but do not have the authority to provide any technical direction or clarification directly to the contractor.

Defective Service: A service output that does not meet the standard of performance associated with the Performance Work Statement.

Deliverable: Anything that can be physically delivered but may include non-physical things such as meeting minutes.

Develop(s/ment): The use of the term "develop" (or any derivative of it) in this PWS refers only to the production of services, materials, plans, etc. as described in the specific task areas (see Section 4. "Specific Tasks"). This term often indications research and development activities which is not the case in this PWS. This PWS contains only Operations & Maintenance-type activities.

Physical Security: Actions that prevent the loss or damage of Government property.

Quality Assurance: The government procedures to verify that services being performed by the Contractor are performed according to acceptable standards.

Quality Assurance Surveillance Plan (QASP): An organized written document specifying the surveillance methodology to be used for surveillance of contractor performance.

Quality Control: All necessary measures taken by the Contractor to assure that the quality of an end product or service shall meet contract requirements.

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

2.2. Acronyms

A/V	Audio / Visual
ACAS	Assured Compliance Assessment Solution
ACIS	Avaya Certified Implementation Specialist
ACL	Access Control List
ADP	Automated Data Processing
ANSI	American National Standards Institute
APDS	Avaya Professional Design Specialist
ASP	Active Server Pages
C&A	Certification and Authorization
C4	Command & Control, Communications, and Cyber
C4I	Command & Control, Communications, Cyber, and Intelligence
CCB	Configuration Control Board
CCIB	Control Interoperability Board

CCNA	Cisco Certified Network Associate
CCNP	Cisco Certified Network Professional
CCRI	Command Cyber Readiness Inspections
CEH	Certified Ethical Hacker
CEKMS	Coalition Electronic Key management System
CERT	Computer Emergency Response Teams
CFR	Code of Federal Regulations
CI	Configuration Items
CIO	Chief Information Officer
CIRP	Cyber Incident Response Plan
CISSP	Certified Information Systems Security Professional
CLIN	Contract Line Item Numbers
CM	Configuration Management
CMRS	Continuous Monitoring Risk Scoring
CMS	Configuration Management System
CND	Computer Network Defense
COMSEC	Computer Security
CONAUTH	Controlling Authority
CONUS	Continental United States (excludes Alaska and Hawaii)
COOP	Continuity of Operations
COP	Common Operating Picture
COR	Central Office of Record
COR	Contracting Officer Representative
COTR	Contracting Officer's Technical Representative
COTS	Commercial Off the Shelf
CS	Computer Security (previously Information Assurance)
CTR	Contract Technical Representative
CTS	Certified Technology Specialist
DADMS	Database Management System
DFARS	Defense Federal Acquisition Regulation Supplement
DISA	Defense Information Systems Agency
DMCC	DoD Mobility Classified Capability
DNS	Domain Name System
DoD	Department of Defense
DRSN	Defense RED Switch Network
EAEP	Enterprise Architecture and Engineering Panel
EASB	Enterprise Architecture and Service Board
ECMRA	Enterprise-wide Contractor Manpower Reporting Application
ECVVoIOP	Enterprise Classified Voice & Video Over Internet Protocol
EITSMS	Enterprise Information Technology Service Management System
EKMS	Electronic Keying Management Systems
FAR	Federal Acquisition Regulation
FFP	Firm Fixed Price
FY	Fiscal Year
GCCS	Global Command and Control System
GNSC	Global Network Operations Support Center
GSORTS	Global Status of Readiness and Training System
HBSS	Host Base System Security
HTML	Hyper Text Markup Language
IA	Information Assurance
IAF	Information Assurance Framework
IAM	Information Assurance Manager
IAT	Information Assurance Technician
IAVA	Information Assurance & Vulnerability Assessment
IDS	Intrusion Detection System
IIS	Internet Information Services

IMB	Interoperability Management Boards
IP	Internet Protocol
IPS	Intrusion Protection System
ISSM	Information Systems Security Manager
IT	Information Technology
ITIL	IT Infrastructure Library
JC2CUI	Joint Command and Control Common User Interface
JDK	Java Developers Kit
JHITS	Joint Hawaii Information Transfer System
JIE	Joint Information Environment
JOPES	Joint Operations Planning and Execution System
JUSMAG	Joint U.S. Military Advisory Group
KEYMAT	COMSEC Key Material
KM	Knowledge Management
KO	Contracting Officer
LE/CI	Law Enforcement Counter Intelligence
LOE	Level of Effort
MAC	Move, Add, and Change
MCSA	Microsoft Certified Solutions Associate
MCSE	Microsoft Certified Solutions Expert
MILSTAR	Military Strategic and Tactical Relay
MINDEF	Ministry of Defense
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MPE	Mission Partner Environment
MS	Microsoft
NIPRNet	Non-classified Internet Protocol Router Network
O&M	Operations and Maintenance
OCI	Organizational Conflict of Interest
OCONUS	Outside Continental United States (includes Alaska and Hawaii)
ODC	Office of Defense Cooperation
OEM	original equipment manufacturer
PBX	Private Branch Exchange
PMO	Program Management Office
PMP	Project Management Professional
PMR	Program Management Review
POC	Point of Contact
PSC	Product Service Code
PWC	Pacific Warfighting Center
PWS	Performance Work Statement
QASP	Quality Assurance Surveillance Plan
RFS	Request for Service
RHCSA	Red Hat Certified System Administrator
RMF	Risk Management Framework
SAV	Staff Assisted Visits
SCAP	Security Content Automation Protocol
SCC	SCAP Compliance Checker
SCIP	Secure Communications Internet Protocol
SCP	Solarwinds Certified Professional
SDLC	Systems Development Life Cycle
SIPRNet	Secret Internet Protocol Router Network (SIPRNet)
SME	Subject Matter Expert
SOP	standard operating procedure
SQL	Structured Query Language
SRG	Security Requirement Guides
SRM	Site Recovery Manager

ST&E	Security Tests & Evaluations
STE	Secure Telephone Equipment
STIG	Security Technical Implementation Guide
SWT	SECTERA Wireline Terminal
TASKORD	Task Order (type of official military order)
TA	Technical Assistant
TE	Technical Exhibit
TELCOM	Telecommunications
TO	Technical Order
USPACOM	United States Pacific Command
VI	Virtual Infrastructure
VM	Virtual Machine
VMS	Vulnerability Management System
VOE	Virtual Machine Operating Environment
VTC	Video Teleconferencing
XML	Extensible Markup Language

PART 3 - INCIDENTAL PROPERTY, EQUIPMENT, AND SERVICES

3. INCIDENTAL PROPERTY, EQUIPMENT, and SERVICES

3.1. Services

The Government will provide network access and services to unclassified and classified (as required) workstations.

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, computers, and other items necessary to maintain an office environment.

PART 4 – SPECIFIC TASKS

4. SPECIFIC TASKS

4.1. Software & Portal Support

The contractor shall provide technical support to the Government in the administration, management, development, operation, and maintenance of software, hardware, network, systems, systems security, collaborative tools, and informational resources.

The contractor shall conduct technical and functional analyses and develop recommendations for hardware and software procurements to improve and upgrade Government capabilities.

The contractor shall participate in technical exchange meetings, work groups, and workshops focused on furthering development of Government capabilities. The contractor shall produce required presentations, reports, point papers, and other related documents as required. The contractor shall produce customized software scripts using COTS available software systems and ensure delivery is tested and integrated into existing Government capabilities.

The scope of this effort includes services necessary to provide a full range of design, development, testing, deployment, integration, and maintenance of software and scripts using existing hardware, network, and systems resident on the Government architecture. Software support activities will use the Systems Development Life Cycle (SDLC). The scope of services includes:

- Program and project management
- Complete project documentation
- Business application and process analysis
- Requirements definition, development, and validation
- Software/systems design, development, testing, deployment, integration, and maintenance of locally produced scripts
- User support and training
- Quality assurance

The contractor will provide the system engineer and administrative expertise to meet unique goals and objectives of the Portal Program for USPACOM. Contractor will perform Portal Program analysis and recommendations for the implementation of portal solutions. Contractor will provide a technical implementation plan that is coordinated with stakeholder leadership. Contractor will provide data analysis to support the implementation of portal software and metric analysis of the metadata being stored in both the classified and unclassified SharePoint data servers. Contractor will conduct an assessment of methods to improve the Portal Program while providing portal software implementation technical support to ensure program meets security and network connectivity standards established by the DoD.

The contractor will support the Command's information sharing and collaboration capability by conducting baseline assessments and evaluate existing information management platforms, applications, systems and processes. Also, contractor will provide recommendations for more efficient and effective alternatives. Contractor will provide recommendations to improve USPACOM processes and procedures needed to support the Command's information sharing and collaboration environment. Contractor will provide SharePoint business analyst capability to identify gaps in processes, find opportunities for improvements, capture requirements, create mockups, generate proof of concept solutions, assist in implementation and training, and document improvements leveraging the current Command's SharePoint platform's features and capabilities.

4.1.1. Special Qualifications:

- Experience with two or more of the following web based programming languages or equivalent:
  a. HyperText Markup Language (HTML)
  b. Active Server Pages (ASP)
  c. Java
  d. VB
  e. C#.net

    f. JavaScript
    g. Extensible Markup Language (XML)
    h. SQL
    i. VBScript
- experience with one or more of the following development software tools or equivalent:
    a. Java Developers Kit (JDK)
    b. JEdit, Subversion
    c. Turbine
    d. iReports
    e. MS Visual Studios
- experience with one or more of the following relational databases or equivalent:
    a. MS Access
    b. MS SQL
    c. Oracle
- experience with one or more of the following web servers or equivalent
    a. MS IIS 7.5 or higher
    b. Apache
- experience with MS Windows 2008 or higher
- experience with MS SharePoint 2010 portal or higher
- experience with WebLogic web server
- experience with Sun Solaris and Vi
- Troubleshooting software and server problems
- Advising and negotiating with customers on software issues.
- Microsoft Office tools such as Word, PowerPoint, Excel, Project, and Outlook
- Preparing documentation, providing user training, and program demonstrations
- Security + CE Certified at start of service

4.1.2. Contractor Travel: No off-island travel is required

4.1.3. Performance Requirements:

Contract programmers shall verbally report significant problems in delivering software. Formal activity reports are due IAW the deliverables schedule.

Contractor(s) shall maintain and troubleshoot operational and maintenance (O&M) applications. Incident calls must be documented and all software maintenance changes coordinated through the J6 change control process. The CIO's ITSF and Service Desk CONOPS will determine the types of incident calls and completion time. Project maintenance logs must be maintained by programmers. Log entries must be completed within one workday from end of the activity recorded, and will be entered electronically.

Contractor(s) shall manage the life cycle of an application, from initial customer request to delivery of the product and follow-on maintenance. All the project components will be handled from cradle to grave, including periodic In Process Reviews (IPRs) at particular phases of life cycle, depending on scope and complexity of work. Required IPRs will be documented and included in project documentation and checklist. Execution timeframe from initial customer request to delivery of the product shall be within +/- 5% of the base-lined project plan timeline.

Contractor(s) shall conduct feasibility studies of all major O&M work and new service requests and create timelines with level of effort and costs. Contract programmers must be agile and capable of documenting and implementing new requirements on very short timelines to meet command and control requirements. Contractor shall provide results of feasibility study within 30 days of being assigned.

Contractor(s) shall conduct meetings with customers, provide periodic project progress demonstrations for projects anticipated to last 30 or more days, conduct maintenance modifications on applications, and collect customer requirements and feedback as determined by the project timelines. Customer contact depends on activity and importance of project. Written progress reports with project timeline status will be noted in weekly activity reports and project reports. Demonstrations will be provided as specified by the base-lined

project work break structure task within +/- 5% of the timeline for projects having a life-cycle timeline of 30 days or more. Historically, HQ USPACOM J6 has had approximately 4 projects of this scale per year.

Contractor(s) shall determine appropriate programming language and database to use for the scope of work. Before starting maintenance work, written or verbal recommendations will be delivered with the software tools that will be used for the project. Unless specific authorization is received from government Section Chief, programmers will adhere to PACOM standard programming languages and databases at all times. Project documentation review by Section Chief will note authorized deviation from standards Analysis will begin upon date Contractor is given access to government files. Findings and recommendations shall be provided to the contractor NLT 30 days upon completion of analysis.

Contractor(s) shall conduct testing and evaluation of application and database as determined by the project timelines. No product will be turned over for production without testing against a test database unless specific authorization is received from Section Chief. Contractor will ensure application software and data files used for testing and production are on separate volumes or partitions, and development and production files are properly backed to disk as well as to tape. Testing shall begin as specified by the baseline project work break structure task within +/- 5% of the timeline. Evaluations and recommendations shall be provided to the government NLT 10 business days after testing concludes.

Contractor(s) will create the necessary tables, views, and fields in the database for the project. All tables, views and field names will be self-documenting, reflecting purpose of table or field as much as possible. Where possible, DoD standard naming and data element characterizations will be used. Tables, views and fields, as well as source code, will be documented in project documentation and subject to peer and Section Chief review at any time. Contractor shall complete database for government review & approval as specified by the base-lined project work break structure task within +/- 5% of the timeline.

Contractor(s) will coordinate delivery of final product and documentation. All projects must be completed and turned over with user sign off and acceptance based on the project exit criteria. Tracking will be measured in weekly activity reports, IPRs and audits/management reviews.

Contractor(s) will produce deliverables such as project management plans and risk management plans via a project management tool like MS Project or equivalent. Contractor will also respond to Directorate's periodic requests for updates to projects via Gantt and quad charts. Project management plans, including risk management plans, Gantt and quad charts, shall be provided NLT 30 days after initial identification and assignment of new projects.

4.1.4. See PART 6 – TABLES: Table 1, "Minimum requirements for Firm Fixed Priced CLIN"

4.1.5. See PART 6 – TABLES: Table 2, "Additional Labor for Labor-Hour CLIN"

4.1.6. See PART 6 – TABLES: Table 3, "Performance Objective Summary"

4.1.7. See PART 6 – TABLES: Table 4, "Deliverables Schedule"

4.2. Service Desk Support

Contractor will implement and operate an IT Infrastructure Library (ITIL)-based service desk to provide the HQ a single assured point of contact for all Automated Data Processing (ADP) hardware, software, and networking problems; for service requests, to include new systems, major modifications to existing systems and entry points for emerging technologies. Also maintains service catalogs, an approved product list, and a knowledge base for Service Desk operations.

Adheres to HQs policy of using Information Technology Requests for all maintenance requests. Documents all users' trouble calls and coordinates all software maintenance changes with government leads while ensuring project maintenance logs are maintained and reviewed.

4.2.1. Special Qualifications:

- experience using Microsoft Office tools (Word, PowerPoint, Excel, and Outlook)
- Security+ Certification

4.2.2. Contractor Travel: No off-island travel is required

4.2.3. Performance Requirements:

Application Software Certification: The Contractor shall provide the Application Test Managers, Program Management Office (PMO), and the Navy enterprise network contract vendor(s) with the software applications and data collection required to complete software testing, certification, and Request for Service (RFS).

Application Database Maintenance: The Contractor shall monitor the Navy Applications and Database Management System (DADMS) daily for approved application software to eliminate duplicative software submission. The Contractor shall provide accurate data processing into DADMS to ensure the timeliness, accuracy, and integrity of the database in support of HQ USPACOM Navy enterprise network operation.

Service Execution: The Contractor shall perform the USPACOM Navy enterprise network Contract Technical Representative (CTR) duties in transforming data automation requirement into orderable Contract Line Item Numbers (CLIN) and submit the seat data package(s) for procurement, staging of services, and equipment delivery using the Navy Marine Corps Intranet (NMCI) Enterprise Tool (NET) within two (2) business days.

Service Management: The Contractor shall analyze IT service requests for Move, Add, and Change (MAC) of existing Navy enterprise network services, translate the service requests into electronic forms (eForms) and submit for MAC processing via the Enterprise Information Technology Service Management System (EITSMS) within one (1) business day. The Contractor shall monitor MAC services submitted daily and take all appropriate actions to expedite the timely processing of requests with the EITSMS MAC queue manager.

4.2.4. See PART 6 – TABLES: Table 1, "Minimum requirements for Firm Fixed Priced CLIN"

4.2.5. See PART 6 – TABLES: Table 2, "Additional Labor for Labor-Hour CLIN"

4.2.6. See PART 6 – TABLES: Table 3, "Performance Objective Summary"

4.2.7. See PART 6 – TABLES: Table 4, "Deliverables Schedule"

4.3. Network Engineering & System Administration

Network Engineering:
The networking communications experts serve as the focal point for expertise in computer network and Video TeleConferencing (VTC) techniques. This work involves the planning, analysis, design, development, testing, information assurance, configuration, installation, implementation, integration, and management/maintenance of networked systems used for transmission of information in voice, data, and/or video formats. Note: This is not Research and Development; rather the design and development refers to the configuration of existing systems, both hardware and software. This includes, but not limited to, network engineering for Cisco-based and VTC-based systems.

System Administration:
The system administration experts serve as the Subject Matter Expert (SME) for the Virtual Operating Environment (VOE), Windows Active Directory Domain, Windows Servers and Workstations, Linux Servers, the Global Command and Control System (GCCS), the Automated Message Handling System (AMHS) and the Domain Naming System (DNS). This work involves the planning, analysis, design, development, testing, securing, information assurance, configuration, installation, implementation, integration, management/maintenance and monitoring of Windows and Linux/Unix based platforms and applications, as well as the Virtual Operating Environment (VMware, Cisco UCS, EMC DataDomain and Isilon). System administrators also assist the Network Engineers in making recommendations to the Government for system and infrastructure improvements.

The following paragraphs describe the tasks as associated with network engineering and system administration:

4.3.1. Special Qualifications:

Systems Engineer (Cisco Based):

- Must have experience managing Cisco-based network architectures in a DoD environment.
- Be "Cisco Certified Network Professional" (CCNP) (or equivalent) and "Security+CE" certified.

Network Administrator (Cisco Based):

- Must have experience managing Cisco-based network architectures in a DoD environment.
- Be "Cisco Certified Network Associate" (CCNA) (or equivalent) and "Security+CE" certified.

Network Administrator (Solarwinds):

- Must have experience managing Cisco-based network architectures.
- Be a "Solarwinds Certified Professional" (SCP) and "Security+CE" certified.

Systems Engineer (VTC):

- Must have experience managing Video TeleConferencing systems.
- Be "Certified Technology Specialist" (CTS) and "Security+CE" certified

System Administrator (Windows) Senior:

- Must have experience managing Windows operating systems in a DoD environment. Knowledge of PowerShell scripting, Active Directory Service Management, and automation is highly desirable.
- Preferred: Be a "Microsoft Certified Solutions Expert" (MCSE) (or equivalent) and "Security+ CE" certified.
- Minimum: Be a "Microsoft Certified Solutions Associate" (MCSA) (or equivalent) and "Security+ CE" certified.

System Administrator (Windows) Intermediate:

- Must have experience managing Windows operating systems in a DoD environment. Knowledge of PowerShell scripting, patching, security, troubleshooting and backups is highly desirable.
- Preferred: Be a "Microsoft Certified Solutions Associate" (MCSA) (or equivalent).
- Minimum: Be proficient with Windows 2008 Server (or newer), Windows 10 Workstation and "Security+ CE" certified.

System Administrator (Virtual Infrastructure (VI)) Senior:

- Must have experience managing VMware based solutions and experience managing enterprise grade storage solutions in a DoD environment.
- Must have experience managing Cisco UCS solutions in a DoD environment.
- Must have experience managing EMC DataDomain and Isilon solutions in a DoD environment.
- Be "VMware Certified Professional 6" (or equivalent) and "Security+ CE" certified.

System Administrator (Linux) Senior:

- Must have experience managing Linux Red Hat (or equivalent) operating systems and Bind DNS in a DoD environment. Must have knowledge and experience in managing audit logs and scripting.
- Be "Red Hat Certified System Administrator (RHCSA)" (or equivalent) and "Security+ CE" certified.

System Administrator (AMHS) Intermediate:

- Must have experience managing and supporting Automated Message Handling System (AMHS), Windows servers, Doubletake SMTO relay and PKI in a Virtual Operating Environment (VOE), within a DoD environment. Must have knowledge and experience in managing audit logs and scripting.
- Be proficent with AMHS and Windows Server 2008 or newer and "Security+ CE" certified.

System Administrator (GCCS) Intermediate:

- Must have experience managing and supporting Global Command and Control Systems in a DoD environment. Must have knowledge and experience with Solaris, Windows Server 2008 or newer and Window 10 workstation.
- Be proficent with GCCS and Windows Server 2008 or newer and "Security+ CE" certified.

4.3.2. Contractor Travel: No travel is required for this task

4.3.3. Performance Requirements: N/A
Network Engineering:

- Make recommendations to the Government for infrastructure improvements.
- In conjunction with the Project Manager, provide advice concerning the improvement of network equipment and system.
- Deploy network routers, switches, firewalls and VTC-specialized equipment on the operational networks with minimal downtime.
- Integrate equipment on server farms and selected switches in a physical or virtual operating environment.
- Complete Security Technical Implementation Guide (STIG) validation and account for vulnerabilities in the in the DISA STIG repository.
- Deploy various network monitoring and configuration tools.
- Validate network redundancy, conduct risk analysis for single points of failure with courses of action for mitigation or remediation.
- Create detailed network architecture and rack elevation diagrams.
- Develop a recommended lifecycle refresh plan of all network devices.
- Analyze USPACOM Internet Protocol (IP) management practices and implement improved processes.

System Administrator (Virtual Infrastructure (VI)):

- Plan and schedule installation of new or modified hardware, operating systems, and applications software in support of the Virtual Machine Operating Environment (VOE).
- Install, upgrade and manage the VOE to include but not limited VMware based products such as:
    - VMWare vSphere
    - VMWare vCenter
    - VMWare SRM
    - VMWare vCOPS
    - VMWare View
    - VMWare ESXi
    - Cisco UCS
    - EMC DataDomain
    - EMC VNX SAN
    - EMC Isilon
    - EMC RPA
    - Connection View Server
    - Virtual Desktop Infrastructure
- Design, deploy and manage HQ USPACOM's thin client architecture.
- Manage enterprise EMC based storage solutions in support of the VOE.
- Design, plan and manage Continuity of Operations (COOP) Services supporting VOE at the primary and backup locations to include assisting with the development and management SRM orchestration scripts and storage replication appliances.
- Complete STIG validations; ensuring vulnerabilities are accounted for in the DISA STIG repository.
- Develop appropriate build documents and standard operating procedures (SOPs) for VM and storage based operating systems.
- Implement security procedures and tools.
- Update configuration management documents.
- In coordination with the Host Based System Security (HBSS) team; ensure proper configuration & operational capability of systems.
- Apply information security/information assurance policies, principles and practices in the delivery of systems administration services.
- Analyze manual processes and make recommendations for process and automation improvements.

System Administrator (Linux):

- Plan and schedule installation of new or modified hardware and Linux based operating systems and applications software.
- Implement Domain Name System (DNS) Security (DNS SEC) on Bind DNS servers
- Review the DNS architecture and develop action plan(s) to implement required configurations.
- Complete STIG validations on 30-40 Linux based systems and applications; ensure all vulnerabilities are properly accounted for in VMS.
- Develop appropriate build documents and SOPs for newly deployed operating systems and applications.
- Implement security procedures and tools.
- Update configuration management documents.
- Maintain applications operating on Linux based systems to include (but not limited to) SMTP relay services, Bind DNS, VMware, Splunk SysLog Server, Assured Compliance Assessment Solution (ACAS), etc.
- Work with the HBSS team to ensure proper configuration & operational capability of systems.
- Apply information security/information assurance policies, principles and practices in the delivery of systems administration services.
- Analyze manual processes and make recommendations for process and automation improvements.
- Analyze Private Branch Exchange (PBX) systems and develop software update procedures.
- Design and Implement SysLog Server for collection of PBX system logs.
- Develop Splunk SysLog reports and alerts.

System Administrator (Windows):

- Plan and schedule installation of new or modified hardware, operating systems, and applications software.
- Install rack mounted servers and workstations, replace and/or patch operating systems to include but not limited to Windows 2008 and Windows 7.
- Deploy and migrate web applications to include Microsoft SharePoint 2010/2013 and Internet Information Services (IIS).
- Complete STIG validations; ensuring vulnerabilities are accounted for in the appropriate repository.
- Develop appropriate build documents and standard operating procedures (SOPs) for Windows based operating systems and applications.
- Implement security procedures and tools.
- Update configuration management documents.
- Work closely with the Host-Based Security System (HBSS) team to ensure proper configuration and operational capability of systems.
- Work with Microsoft Enterprise Premier Support as required.
- Deploy Non-classified Internet Protocol Router Network (NIPRNet) and Secret Internet Protocol Router Network (SIPRNet) Public Key Infrastructure services.
- In accordance with DFARS 239.7102-3, apply information security/information assurance policies, principles and practices in the delivery of systems administration services.
- Analyze manual processes and make recommendations for process and automation improvements.

System Administrator (Windows):

- Plan and schedule installation of new or modified hardware, operating systems, and applications software.
- Will maintain the security posture of all assigned Windows systems (servers and workstations) and ensure compliance with DoD requirements (STIG, IAVA, Task ORD).
- Will create and maintain custom scripts, as required (i.e., Windows, Active Directory, Group Policy, STIG, etc.).
- Will maintain and update Windows deployment files (classified/unclassified) for automated secure installations of mission critical Windows Systems.
- Responsible for monthly patching of assigned Windows systems and applications to include but not limited to:

    - Windows Active Directory
    - Windows Servers
    - Windows Workstations
- Responsible for Active Directory level file shares and printing services/servers.
- Develop appropriate build documents and standard operating procedures (SOPs) for Windows based operating systems and applications.
- Implement security procedures and tools.
- Update configuration management documents.
- Work closely with the Host-Based Security System (HBSS) team to ensure proper configuration and operational capability of systems.
- In accordance with DFARS 239.7102-3, apply information security/information assurance policies, principles and practices in the delivery of systems administration services.
- Analyze manual processes and make recommendations for process and automation improvements.

System Administrator (AMHS):

- Plan and schedule installation of new or modified hardware and Windows based operating systems and software applications.
- Will maintain and upgrade existing hardware, Windows based operating systems and software applications.
- Will maintain the security posture of all assigned systems and ensure compliance with DoD requirements (STIG, IAVA, Task ORD).
- Will create and maintain custom scripts, as required (i.e., Windows, Active Directory, Group Policy, STIG, etc.).
- Will maintain and update AMHS deployment files for automated secure installations of mission critical AMHS Systems.
- Responsible for monthly patching of assigned systems and applications to include but not limited to:
    - Automated Message Handling System (AMHS)
    - Doubletake
    - Microsoft Internet Information Service (IIS) 7.5 (or later)
    - Microsoft SQL 2008 (or later)
    - Windows Server 2008 R2 (or later)
    - SMTP Relay
- Develop appropriate build documents and standard operating procedures (SOPs) for Windows based operating systems and applications.
- Implement security procedures and tools.
- Update configuration management documents.
- Work closely with the Host-Based Security System (HBSS) team to ensure proper configuration and operational capability of systems.
- Work with AMHS support as required.
- In accordance with DFARS 239.7102-3, apply information security/information assurance policies, principles and practices in the delivery of systems administration services.
- Analyze manual processes and make recommendations for process and automation improvements.

System Administrator (GCCS):

- Plan and schedule installation of new or modified GCCS-J hardware and Windows based operating systems and software applications.
- Will maintain and upgrade existing GCCS-J hardware, Windows based operating systems and software applications.
- Will maintain the security posture of all GCCS-J Windows systems (servers and workstations) and ensure compliance with DoD requirements (STIG, IAVA, Task ORD).
- Will create and maintain custom scripts, as required (i.e., Windows, Active Directory, Group Policy, STIG, etc.).
- Will maintain and update GCCS-J Windows deployment files (classified/unclassified) for automated secure installations of mission critical Windows Systems.

- Responsible for monthly patching of GCCS-J Windows systems and applications to include but not limited to:
    - Global Command & Control System-Joint (GCCS-J)
    - GCCS-J COP
    - Agile Client
    - Active Directory
    - Windows Servers
    - Windows Workstations
    - File Share
    - Printing
- Responsible for Active Directory level file shares and printing services/servers.
- Develop appropriate build documents and standard operating procedures (SOPs) for Windows based operating systems and applications.
- Implement security procedures and tools.
- Update configuration management documents.
- Work closely with the Host-Based Security System (HBSS) team to ensure proper configuration and operational capability of systems.
- In accordance with DFARS 239.7102-3, apply information security/information assurance policies, principles and practices in the delivery of systems administration services.
- Analyze manual processes and make recommendations for process and automation improvements.

4.3.4. See PART 6 – TABLES: Table 1, "Minimum requirements for Firm Fixed Priced CLIN"

4.3.5. See PART 6 – TABLES: Table 2, "Additional Labor for Labor-Hour CLIN"

4.3.6. See PART 6 – TABLES: Table 3, "Performance Objective Summary"

4.3.7. See PART 6 – TABLES: Table 4, "Deliverables Schedule"

4.4. Telecommunications Support

Telecommunications Systems Support includes many sub-functions to include interfacing with the Joint Hawaii Information Transfer System (JHITS), supporting Defense RED Switch Network (DRSN) operations, providing support to the Military Strategic and Tactical Relay (MILSTAR) Satellite Communications System, Iridium mobile satellite phone support, as well as more traditional telecommunications operations support such as break-fix actions for desktop telephones and maintaining the Private Branch Exchange (PBX) switches. Telecommunications Services Support includes end-to-end system troubleshooting efforts on these and other major telecommunications systems. Troubleshooting requires a working knowledge of voice and data circuits, modems, data and voice multiplexer equipment, telecommunications interfaces and other auxiliary equipment. Support is required in traditional as well as emerging "Voice Over (Secure) IP" VOIP/VOSIP technologies.

Contractor provides support by coordinating, installing, testing, and evaluating DRSN projects, including new DRSN circuit installations, the upgrade of DRSN infrastructure, the upgrade of DRSN and cryptographic equipment, the relocation of DRSN circuits and equipment, and installation of new IT capabilities. With Government oversight, the contractor will also determine the steps required, specify the methods to be used, and engineer DRSN-related solutions, while independently applying established policies, procedures, processes, and techniques to produce cost estimates and ultimately, a completed product.

The contractor will administer multiple aspects of the MILSTAR Satellite Communications System to include maintaining and troubleshooting MILSTAR related equipment located in the High Altitude Electromagnetic Pulse hardened shelters on Camp Smith. They coordinate technical support to engineer enhancements, maintain facilities, and troubleshoot connectivity.

Also included under the this subtask are more traditional telecommunications functions such as maintaining, engineering, programming and troubleshooting the PBX, Secure Telephone Equipment (STE), secure and non-secure cellular telephones, the expansion of network ports, and various uninterruptible

power supplies and peripheral equipment. Occasional infrastructure related tasks may be needed such as installing and documenting fiber paths. Planning, coordinating and executing actions related to establishing, changing, testing, operating, troubleshooting, and maintaining communication circuits.

4.4.1. Special Qualifications:

The Contractor's employer must be an official Avaya® Gold (or higher) Business Partner in order to reach back to upper level Avaya engineering support and hold the following certifications/credentials:

- Avaya Professional Design Specialist (APDS) Unified Communications
- Avaya Certified Implementation Specialist (ACIS) Communication Manager
- ACIS Aura Communication Manager and Communication Manger Messaging

The dedicated, on-site technician must:

- Be Security+ certified and have root-level access on PACOM fielded systems.
- Must have experience in network administration.
- Must have experience with: Avaya® Private Branch Exchanges; Call Manager 2.0 & 4.0; EPN, ISDN, DSN, E&M, Multi-Function Digital, and STE devices.
- Must have experience using MS Office tools (Word, PowerPoint, Excel, and Outlook).
- Must have experience advising and negotiating with customers including senior level customers (military and civilian), analysts, other vendor personnel, and IT staff.

4.4.2. Contractor Travel: No off-island travel is required.

4.4.3. Performance Requirements:

Avaya® Private Branch Exchanges (PBX) HQ USPACOM Support:

- The contractor shall provide maintenance, engineering, programming, and troubleshooting support to the USPACOM Avaya® Private Branch Exchanges (PBX) in Camp Smith Building 700 (to include expansion port networks in Camp Smith Buildings 4 & 20), the Pacific Warfighting Center at Ford Island, and select Flag Officer quarters at Joint Base Pearl Harbor Hickam, Hawaii. System encompasses and interfaces with Communication Manager Messaging voicemail system, VeraSMART Call Accounting System, REDCOM® Secure Conferencing Bridge, DRSN CEU, Uninterruptible Power Supply units, and various peripheral equipment.
- Engineering, programming, and troubleshooting support covers critical areas throughout USPACOM to include (but not limited to) the Joint Operations Center, Emergency Actions Booth, Special Operations Command, Joint Interagency Task Force West, Naval Computer and Telecommunications Area Master Station Pacific, and the Pacific Warfighting Center.
- Official telecommunications service support is provided to Flag Officer/Executive quarters at various locations, island wide.
- All actions must be in-line with original equipment manufacturer (OEM) maintenance specifications.
- The Contractor shall be responsible for maintenance of the EAS system. Support may be required after hours, on weekends, and during holidays. Acceptable Service Response for this system is defined as responding within 2 hours of notification and the system fully operational again within 24 hours of receipt of any required parts. Reference paragraph 1.6.4.3 for information concerning the estimated frequency of this support.
- The Contractor is responsible for the programming, maintenance, and management of the EAS system administration Local Area Network (LAN).
- Maintenance of the EAS is to include applicable system patches required by Avaya®, the Defense Information Systems Agency (DISA), and the Joint Interoperability Test Center (JITC) to meet mandated baselines.
- The Contractor must update and maintain current PBX systems documentation and Standard Operating Procedures for the EAS System.
- The Contractor serves as the PBX Subject Matter Expert (SME) and provides recommendations and solutions for system enhancements and applications implementation to the government.
- The Contractor shall provide recommendations to the Infrastructure and Telecom Branch for various review boards (e.g. Information resource Management Board (IRMB)) and must develop a

working knowledge base of all critical communications circuits, equipment, and interfaces supporting the USPACOM mission.

- As requested by the government, the Contractor develops and implements the Government Disaster Recovery Procedures and Protocols.
- The Contractor is responsible for the programing, implementation and incorporation of the Government's Multi-Level Precedence and Preemption (MLPP) capabilities.

DRSN Operational and Maintenance HQ USPACOM Support:

- The contractor shall provide technical expertise to maintain the operational level and provide maintenance of DRSN switches as mandated by Defense Information System Agency (DISA) Operational and Maintenance (O&M) guidelines which mandates that all DRSN sites are monitored by Trunk Activity, Switch Activity and Circuit Activity. Trunks and circuits shall be maintained at the 99% operational levels.
- Contractor shall provide support by coordinating, installing, testing, and evaluating DRSN projects, including new DRSN circuit installations, the upgrade of DRSN infrastructure, the upgrade of DRSN and cryptographic equipment, the relocation of DRSN circuits and equipment, and installation of new IT capabilities.
- With Government oversight, the contractor will also determine the steps required, specify the methods to be used, and engineer DRSN-related solutions, while independently applying established policies, procedures, processes, and techniques to produce cost estimates and ultimately, a completed product.
- The contractor shall respond to Navy DRSN user system or operational trouble calls.
- The contractor shall provide technical expertise and assistance in trouble shooting DRSN equipment or system failures.
- The contractor shall support the end user with solutions or recommendations to restore the DRSN system to operational level as directed by DISA O&M mandates.
- The contractor shall respond to all trouble calls within time frames defined in DISA instructions of receipt and respond within 1 business day to all trouble calls that cannot be resolve with the 1st contact with end user and/or provide end user a recommend solution. The solutions or recommendations shall be documented in the DRSN Operational and Maintenance Monthly log in accordance with DISA O&M guidelines.
- The contractor will administer multiple aspects of the MILSTAR Satellite Communications System to include maintaining and troubleshooting MILSTAR related equipment located in the High Altitude Electromagnetic Pulse hardened shelters on Camp Smith.

DISA Enterprise Classified Voice & Video Over Internet Protocol (ECVVoIP) and the DoD Mobility Classified Capability (DMCC) HQ USPACOM Support:

- The contractor shall provision, engineer, install, maintain, and troubleshoot all aspects of the DISA Enterprise Classified Voice & Video Over Internet Protocol (ECVVoIP) and the DoD Mobility Classified Capability (DMCC) initiatives at HQ USPACOM.
- The contractor shall provide subject matter expertise in the technology refreshment planning of the DISA ECVVoIP and DMCC hardware, software, protocols and configurations.
- The contractor shall support the development of technology refreshment and other programmatic documentation related to the DISA ECVVoIP and DMCC networks and support network problem identification, analysis and resolution. This will require interfacing with Global Network Operations Support Center (GNSC) analyst, the customer, network operations, and installation maintenance personnel.
- The contractor shall provide technical assistance, engineering, and program support at strategic, operational and tactical levels for the DISA ECVVoIP and DMCC network and endpoints.
- The contractor shall ensure proper steps are taken to troubleshoot and resolve problems, raise the problem process to the appropriate resource level and be responsible for the problem until resolution.
- The contractor shall identify and track all software baseline and patches deployed on the DISA ECVVoIP and DMCC networks and endpoint equipment to include assisting with the tracking, assessment, testing and implementation updates, patches and upgrades in accordance with the

Information Assurance & Vulnerability Assessment (IAVA) directives issued by the USCYBERCOM and DISA CIO.

- The contractor shall provide support in the detection, diagnosis and resolution of incidents or events on the DISA ECVVoIP and DMCC network elements, associated circuits, and endpoints.
- The contractor shall support the planning, analysis, engineering and subsequent deployment of approved hardware and software affecting the DISA ECVVoIP and DMCC networks and endpoints.
- The contractor shall support all logistics efforts associated with the pre-configuration and shipment coordination of the DISA ECVVoIP and DMCC equipment.
- The contractor shall provide official written recommendation on engineering solutions and complex trouble resolutions.
- The contractor shall support the design and engineering of new site installations, site implementation plans, IA assessments and develop and implement Disaster Recovery Procedures and Protocols.
- Support may be required after hours, on weekends, and during holidays. Acceptable Service Response for this system is defined as responding within 2 hours of notification and the system being fully operational again within 24 hours of receipt of required parts. This is an emergent capability; therefore, there is no historical data to estimate the required level of effort.

4.4.4. Removed

4.4.5. See PART 6 – TABLES: Table 2, "Additional Labor for Labor-Hour CLIN"

4.4.6. See PART 6 – TABLES: Table 3, "Performance Objective Summary"

4.4.7. See PART 6 – TABLES: Table 4, "Deliverables Schedule"

4.5. Electronic Key Management Support

Contractor shall provide support to administer the Coalition Electronic Key management System (CEKMS) and the PACOM Regional COMSEC Account. Contractor shall perform central receiving, temporary storage, and transfer services for DoD-provided COMSEC equipment, documents, keying and other materials; train Ministry of Defense (MINDEF) personnel in the proper custodianship, safeguarding and operation of DoD-provided COMSEC equipment and materials, including keying materials; and conduct periodic inventories and inspections of DoD-provided COMSEC equipment, documents and materials, including keying materials.

4.5.1. Special Qualifications:

- Contractors will register and arrange to attend the COMSEC Managers Course training within three months of contract start. See 4.5.2.
- The Contractor shall be thoroughly familiar with the proper handling and safeguarding of Communications Security materials and equipment.
- The Contractor shall be able to clearly articulate COMSEC concerns, including recommended Courses of Actions both verbally in writing, to U.S. and Host Nations senior leadership.
- Must have a strong background in C4I Systems and Networks and shall be experienced in theory of all aspects of COMSEC Equipment and Systems to include Secure Communications Internet Protocol (SCIP) devices, Secure Analog and Data Service devices, SECTERA Wireline Terminal (SWT) and Secure Telephone Equipment (STE)).
- The Contractor must have a background in Electronic Keying Management Systems (EKMS).

4.5.2. Contractor Travel:
Contractor will be required to travel to CONUS, and within the PACOM AOR to attend meetings, conferences, training and in direct support of their duties as Regional Account Managers. Estimated number of trips is one (1) per quarter with up to two (2) travelers for an estimated maximum of four (4) two-person trips.

4.5.3. Performance Requirements:

- Contractor shall receive, store, and transfer United States DoD COMSEC material (including equipment, documents, and KEYMAT). Contractor shall perform and document quarterly inventories and inspections (NLT 1st business day of the 2nd month of the quarter) of all stored COMSEC equipment, KEYMAT, documents, and materials.
- Contractor will use the NSA Central Office of Record (COR) website to receive COMSEC inventories, manage transaction files, and receive and publish COMSEC policies.
- Contractor will develop in-country distribution plans in conjunction with Office of Defense Cooperation (ODC), Joint U.S. Military Advisory Groups (JUSMAG), Ministry of Defense (MINDEF), and host nations as required. Government will approve all plans.
- Contractor will provide COMSEC Custodian services as referenced in NSA CSS Policy Manual No. 3-16 and IAD DOC 125-10 Local Management Device Manual
- Contractor will provide on-site/on-equipment informal unit training to coalition personnel on installation, and operating techniques pertaining to the adjustment, calibration, trouble-shooting, bench check, and inspection of all COMSEC equipment and systems. This specification is contingent upon the presence of a functioning test bench and releasability of installation and operating techniques.
- Contractor will develop local informal training programs and demonstrations for personnel utilizing COMSEC material and equipment.
- Contractor will support United States Government committees and/or staffs by providing minutes of meetings to include status of COMSEC devices and key, inventory reports, after action reports, travel and trip reports maintenance and repair reports where secure coalition interoperability, and COMSEC issues and/or plans are discussed.
- Contractor will report on the current status of COMSEC-related issues during the United States Command and Control Interoperability Board (CCIB) and Interoperability Management Boards (IMB) meetings. These meetings are held twice a year per country.
- Contractor will provide status reports to the USPACOM Theater COMSEC Manager concerning new requirements or modifications to existing requirements to be serviced by the COMSEC Regional Account.
- Contractor will provide keying material during emergency and/or contingency situations.
- Contractor will coordinate with the USPACOM Theater COMSEC Manager for instructions and interpretation of SOPs and instructions and all issues concerning COMSEC equipment, KEYMAT, and associated information that has been provided to our coalition countries.
- Contractor will develop Standard Operating Procedures (SOPs) in coordination with the USPACOM Theater COMSEC Manager.
- Contractor will produce required accounting records and reports and submit to the USPACOM Theater COMSEC Manager.
- Contractor will perform routine destruction of COMSEC material when required, or effect other disposition of material as directed by the NSA COR keying material Controlling Authority (CONAUTH).
- Contractor will submit transfer, destruction, and possession reports when required to the appropriate US Government and/or DOD office.
- Contractor will conduct an inventory semiannually and upon appointment of a new COMSEC Custodian, by physically sighting all COMSEC material charged to the account, and reconcile this inventory with the COR. The conduct of an inventory may also be directed by the COR or other competent authority, to include USPACOM Theater COMSEC Manager.
- Contractor will update COMSEC publications held by the account with all published amendments.
- Contractor will accomplish required page checks on all keying material (as specified in U.S. policy manuals and U.S. COMSEC authorities) and on all publications when they are received, returned from hand receipt, transferred, destroyed, when a change of COMSEC Custodian occurs, and when posting amendments which include replacement pages to ensure completeness of each publication.
- Contractor will notify the NSA COR's COMSEC Registration office pending account re-location.

Applicable Publications (Current Editions): The Contractor must abide by all applicable regulations, publications, manuals, and local policies and procedures to include the following:

- NSA CSS Policy Manual No. 3-16
- IAD DOC 125-10 Local Management Device Manual Dated June 2010

4.5.4. See PART 6 – TABLES: Table 1, "Minimum requirements for Firm Fixed Priced CLIN"

4.5.5. See PART 6 – TABLES: Table 3, "Performance Objective Summary"

4.5.6. See PART 6 – TABLES: Table 4, "Deliverables Schedule"

4.6. System Integration

Implements the business rules and processes, which underpin the tools acquired, and oversees the successful migration from manual or legacy processes to ones automated by software for effectiveness and efficiency.

This requirement is closely related to the Project Management. The most significant distinction pertains to "scope." The contractor will closely manage up to three projects at a time. The Project Manager has many more projects to track, but with much less daily involvement, whereas, the System Integrator is the direct lead for their assigned project(s).

4.6.1. Special Qualifications:

- Must have experience with IT project management experience; preferably in a DoD environment.
- Must be Project Management Professional (PMP) certified.
- Security+ certification
- Experience using Microsoft Office tools (Word, PowerPoint, Excel, and Outlook).

4.6.2. Contractor Travel: No off-island travel is required

4.6.3. Performance Requirements:

- Perform scope and stakeholders management for installation of the various systems/software projects, e.g. server tech refresh, Archer, FootPrints.
- Make recommendations to the Government regarding scope changes for projects under his prevue.
- Identify risks and perform risk management, e.g. dependencies within existing Operations and Maintenance (O&M) environment, procurement time lines.
- Integrate the multiple projects into an overarching timeline that ensures a delivery coinciding with end of the period of performance and handle project interdependencies
- Balance SPAWAR-supplied resources for projects under their control.
- Ensure rigorous application of information security/information assurance policies, principles, and practices in the delivery of all services.

4.6.4. See PART 6 – TABLES: Table 1, "Minimum requirements for Firm Fixed Priced CLIN"

4.6.5. See PART 6 – TABLES: Table 3, "Performance Objective Summary"

4.6.6. See PART 6 – TABLES: Table 4, "Deliverables Schedule"

4.7. Project Management

Contractor will work with the Network Engineers to plan and coordinate the acquisition of assets purchased by the Government. Plans for the integration and deployment of acquired assets/software using established Project Management principles. Develop schedules in coordination with USPACOM J64 representative. Perform risk assessment planning throughout the lifecycle of the projects. Complete and/or review all documentation generated by implementation teams.

This requirement is closely related to System Integration. The most significant distinction pertains to "scope." This position will provide general project management oversight for many projects at one time whereas the System Integrator oversees all aspects of only his/her assigned project(s).

4.7.1. Special Qualifications:

- Must have experience with IT project management experience; preferably in a DoD environment.

- Must be Project Management Professional (PMP) certified.
- Security+ certification is desired, but not required.
- Experience using Microsoft Office tools (Word, PowerPoint, Excel, and Outlook).

4.7.2. Contractor Travel: No off-island travel is required

4.7.3. Performance Requirements:

- Oversee overall project integration and report directly to USPACOM J6 designated government program/project lead(s).
- Complete/review all documentation generated by implementation teams. (Reports shall be in desired government formats. See the Deliverables section of this document.)
- Based on Government priorities and project timelines, make recommendations to the USPACOM J6 lead regarding manpower allocations for the projects they are managing.
- Ensure best practices and all relevant security standards are followed.
- As needed and in-conjunction with USPACOM Information Assurance personnel, ensure accreditation packages are updated properly.
- Develop implementation schedules in coordination with the J6 lead and Contractor teammates.
- Develop project timelines and ensure schedules are observed.
- Resolve issues with the USPACOM Program/Project Manager.
- Ensure the USPACOM Project Manager and Contractor team are aware of project status and issues.
- Perform risk assessment planning throughout the lifecycle of each project.
- Conduct meetings as necessary, gathering information needed to ensure the configuration designs and implementations meet USPACOM IT infrastructure and business requirements.

4.7.4. See PART 6 – TABLES: Table 1, "Minimum requirements for Firm Fixed Priced CLIN"

4.7.5. See PART 6 – TABLES: Table 3, "Performance Objective Summary"

4.7.6. See PART 6 – TABLES: Table 4, "Deliverables Schedule"

4.8. Computer Network Defense Support

Contractor will perform day-to-day Computer Network Defense (CND) services and is responsible for supporting information security technology disciplines and practices to ensure the confidentiality, integrity and availability of information assets in accordance with established standards and procedures. The contractor will work closely with Information Assurance staff to ensure system security and compliance is achieved, maintained and reported accurately for HQ USPACOM networks.

Tasks include performing wireless assessments; updating detection signatures and/or access control lists based on vendor releases and/or intelligence reporting; maintaining cyber situational awareness by participating in working groups and attending meetings when a CND representation is required (participation is limited to non-decision making activities); operating, repairing, updating, installing/removing of DoD and commercial vulnerability scanning and security patching tools such as the Host Based Security System (HBSS); analyzing multiple sources of data to gain situational awareness of cyber activity; performing log analysis and event correlation to identify anomalous traffic. The contractor analyzes, interprets and recommends solutions for system shortfalls, discrepancies or improvements in technologies and security requirement, and provides official written recommendation on engineering solutions and complex trouble resolutions.

When needed, they may perform computer forensics to assistance with internal investigations in accordance with DoD standards and industry best practices and assist law enforcement counter intelligence.

4.8.1. Special Qualifications:

- Must have experience related to IA, IT, CND, or defensive cyberspace operations.
- Must have experience in a Regional Cyber Center/Network Control Center or National Cyber Center/Network Control Center.
- Must have experience managing HBSS on a distributed network.

- Experience using Microsoft Office tools (Word, Excel, PowerPoint, Outlook, and Visio) in preparing analytical reports, information papers, and briefings for executive level recipients.
- In accordance with DoD 8570.01-O and DFARS 239.7102-3, the technician must possess at least one current Information Assurance Technical (IAT) Level II certification (i.e., Security+, GSEC, SSCP, etc). In the event the on-site technician(s) are not IAT Level II certified, the Contractor shall ensure the technician(s) obtain certification within 90 days from the date of hire. Additionally, "Certified Ethical Hacker (CEH)" certification is highly desired, but not required. The Government representative will determine the suitability of any certification equivalencies.

4.8.2. Contractor Travel: No off-island travel is required

4.8.3. Performance Requirements:

- The contractor will analyze and evaluate HBSS systems and recommend enhancements to their configurations, capabilities, IA aspects of major HBSS outages, and recommend remedial measures and Computer Network Defense (CND) trends in HBSS operations and infrastructure.
- The contractor will ensure that all assets located within the USPACOM non-NMCI network enclaves are appropriately included in the USPACOM HBSS architecture, and configured per USPACOM and USCYBERCOM acceptable standards.
- The contractor will analyze the HBSS policy and management server, deploy HBSS clients, perform asset baseline management, configure and monitor rogue system sensors, support and manage Antivirus and Antispyware policies, and configure firewall and host intrusion prevention policies and rule sets.
- The contractor will coordinate with local system owners and administrators for initial deployment of HBSS components, as well as for any significant HBSS changes.
- The contractor will assist in resolving any conflicts or issues arising from HBSS implementation with the system owner, system administrator, program office representative, or data owner.
- The contractor will assist remote administrators with troubleshooting the installation of HBSS components and issues that arise with deployment of custom signatures and firewall rules.
- The contractor will create and implement firewall rule sets for each system type including web servers, domain controllers, Structured Query Language (SQL) servers, workstations, kiosks and mobile platforms.
- The contractor will create custom Host Intrusion Detection/Prevention signatures and filter out false positive events as they are reported.
- The contractor will assist USPACOM CND staff with IDS, IPS, Firewall, HBSS, and packet capture log analysis in order to fully integrate the capabilities of HBSS into the operational construct of USPACOM CND.
- The contractor will provide recommendations for network level defensive configurations for Intrusion Detection System (IDS), Intrusion Protection System (IPS), Firewall, and packet capture devices based on the policies implemented at the HBSS program level.
- The contractor will provide support to external USPACOM systems per approved Memorandum of Agreements (MOA) or Memorandum of Understandings (MOU). This can include site visit HBSS support and inspection capabilities as required or requested by USPACOM CND or supporting activities.
- The contractor will conduct analysis of malicious data-sets and publicly known exploits or vulnerabilities for the creation of custom detection and prevention methods.
- The contractor will maintain heightened awareness of current threats and trends in the CND arena.
- The contractor will provide HBSS guidance to USPACOM theater entities on current network threats and trends not only occurring within the Department of Defense (DoD), but also the commercial sector.
- The contractor will monitor other service, DOD, and industry Computer Emergency Response Teams (CERT) Alerts, Warnings and Advisories, and use information gathered to protect USPACOM systems.
- The contractor will track and report on enterprise deployment of HBSS tool.
- The contractor will review/respond to alerts for every HBSS client (workstation and server) in the environment continuously on a daily basis. The contractor will deconflict false positive alerts and incorporate into existing firewall IDS/IPS policies throughout the architecture.

- The contractor will provide weekly HBSS baseline reports to local system owners, system administrators, and requesting organizations as necessary for proper reporting and trend analysis.
- The contractor will provide detailed reports on system status, module deployments, and event trends IAW with the Deliverables section of this document.
- The contractor will maintain and validate changes to each system baseline on a weekly basis.
- The contractor will generate actionable reporting and notifications upon discovery of anomalous activity, and forward initial analysis of intrusions or anomalous activity to incident responders.
- The contractor will perform analysis and preparation of network level data correlation in support of anomalous activity identified through the HBSS report structure.
- The contractor shall analyze and recommend courses of action for USPACOM to address IA and CND issues for the USPACOM HBSS architecture and analyze emerging HBSS configurations, capabilities, and systems as new technologies and capabilities become available and provide recommendations to aid USPACOM's HBSS processes.
- Perform wireless assessments for HQ USPACOM in Building 700 on Camp H.M. Smith, Hawaii in accordance with the USPACOM wireless security policy.
- Update detection signatures and/or Access Control Lists (ACL) based on vendor release and/or intelligence reporting.
- Maintain cyber situational awareness by participating in working groups and attending meetings when a CND representation is required.
- Leverage the latest DoD and commercial vulnerability scanning and security patching tools to accurately characterize risk to HQ USPACOM networks.
- Regularly analyze multiple sources of data from CND tools to gain situational awareness of cyber activity within the HQ USPACOM networks. Perform log analysis and event correlation to identify anomalous traffic.
- Upon discovery of anomalous traffic, initiate incident response in accordance with the HQ USPACOM Cyber Incident Response Plan (CIRP).
- The contractor will provide weekly cyber threat summary, to include all incident response activities directly affecting USPACOM CND or supporting activities.
- When needed, perform computer forensics to assistance with internal investigations in accordance with DoD standards and industry best practices and assist Law Enforcement Counter Intelligence (LE/CI) investigations when needed.
- Analyze, interpret and recommend solutions for system shortfalls, discrepancies or improvements in technologies and security requirements.
- Provide recommendations on engineering solutions and complex trouble resolutions.

4.8.4. See PART 6 – TABLES: Table 1, “Minimum requirements for Firm Fixed Priced CLIN”

4.8.5. See PART 6 – TABLES: Table 2, “Additional Labor for Labor-Hour CLIN”

4.8.6. See PART 6 – TABLES: Table 3, “Performance Objective Summary”

4.8.7. See PART 6 – TABLES: Table 4, “Deliverables Schedule”

4.9. Enterprise Architecture Support

The contractor shall provide Joint Information Environment and Mission Partner Environment (JIE/MPE) information technology support to the Director, USPACOM Command, Control, Communications, and Cyber Directorate (J6).

4.9.1. Special Qualifications:

Must have experience with geographical combatant command or similar theater-wide architectures and extensive program management experience.

4.9.2. Contractor Travel: No off-island travel is required

4.9.3. Performance Requirements:

- JIE/MPE Project Management: Provide the project management expertise required to plan and coordinate the JIE/MPE capabilities required to enable information sharing, collaboration, and

interoperability provided as Enterprise Services that can be provided in federated, franchised, or centralized business models. Planning in support of JIE/MPE is currently ongoing within the USPACOM area of responsibility. Develop USPACOM JIE/MPE Implementation Plans in support of technical, operations, and governance requirements. USPACOM JIE/MPE high-level progress reporting and management, integrated schedule updates, and program/project milestones for JIE/MPE implementation. Contractor will review and comment all JIE and MPE Reference Architectures and supporting Technical Architecture products.

- JIE/MPE Analysis: Provide IT research and analysis in support of JIE/MPE technical, operational, and governance tasks, architectures, and requirements. The analysis shall include identifying, defining, refining, and documenting JIE/MPE capabilities in support of planning and execution. Analysis use cases and determine the best set of architecture artifacts for each phase of USPACOM JIE/MPE development. Provide assistance to the staff with regard to JIE/MPE capability planning, execution, and requirements including Department of Defense and Joint Staff requirements for USPACOM coordination.
- Contractor shall attend architecture meetings in support of JIE and MPE (mostly by telephony and desktop video). Contractor shall provide analysis and recommendations for the production of architecture artifacts based on the analytical findings of the DOD Enterprise Architecture and Engineering Panel (EAEP) and the Enterprise Architecture and Service Board (EASB) that contribute to the USPACOM. Contractor will provide recommendations in the development of a USPACOM strategy for implementing JIE and MPE objectives and solutions.
- Contractor shall conduct cyberspace/cyber security research and analysis of critical architectures within the USPACOM AOR. Contractor shall provide analysis and recommendations for the production of DoDAF products that create enterprise architecture models and reports in the area of IA/Cyber security.

4.9.4. See PART 6 – TABLES: Table 1, “Minimum requirements for Firm Fixed Priced CLIN”

4.9.5. See PART 6 – TABLES: Table 3, “Performance Objective Summary”

4.9.6. See PART 6 – TABLES: Table 4, “Deliverables Schedule”

4.10. Assessment, Certification, and Authorization

Contractor shall execute all phases of the US Department of Defense’s (DoD) Risk Management Framework (RMF) and Defense Information Assurance Certification and Accreditation Program (DIACAP), develop RMF and DIACAP based certification packages, and provides system risk mitigation recommendations to appointed USPACOM Information Systems Authorizing Official Representatives and USPACOM Information Systems Security Manager (ISSM). Contractor shall provide support to existing PACOM Certification & Accreditation Processes and workflows in alignment with the USPACOM Chief Information Officer’s (CIO) Information Assurance Framework (IAF).

Contractor shall provide technical subject matter expertise in the implementation of RMF and DIACAP, as well as,support all aspects of their security life cycle. Contractor will categorize information systems and define criticality/sensitivity of systems according to worst-case, adverse impact to missions. Contractor shall facilitate the selection of baseline security controls; apply tailoring guidance and supplemental controls as needed based on a risk assessment. Contractor should be able to make recommendations for implementation of security controls using sound systems engineering practices and be able to assess security controls by determining security control effectiveness (i.e., controls implemented correctly, operating as intended, and meeting security requirements for information system). Contractor shall support processes that facilitate the monitoring of the security state of information systems and continually track changes to the information systems that may affect security controls and reassess control effectiveness via annual RMF and DIACAP control set validations and audits. Contractor shall provide annual auditing services.

Contractor shall provide risk-based analysis on current, developing, and future cybersecurity systems to determine impacts on USPACOM’s systems portfolio, including HQUSPACOM and its subordinate organizations. The contractor shall provide subject matter expertise to advise USPACOM Action Officer

(AO) Representatives and Information Systems Security Manager (ASSM) while evaluating cybersecurity programs, providing draft correspondence memos IAW DOD 5110.4-M, Manual for Written Material, as required.

Contractor shall provide USPACOM AO Representatives and ISSM level-of-effort (LOE) assessments and estimated completion dates on assigned system security package reviews. Contractor shall provide adjusted completion dates, based on deliverables prioritized by USPACOM AO Representatives and ISSM.

Under DoDD 8570.1 requirements for Cyber Security Work Force this position will require, at least, an Information Assurance Manager (IAM) Level 2 Certified Information Systems Security Professional (CISSP), or equivalent certification.

4.10.1. Special Qualifications:

- Must have subject matter experience related to information assurance, information technology, computer network defense (IA, IT, CND), or defensive cyberspace operations.
- Must have experience in a Regional Cyber Center/Network Control Center or National Cyber Center/Network Control Center.
- Must have experience managing HBSS on a distributed network.
- Experience using Microsoft Office tools (Word, Excel, PowerPoint, Outlook, and Visio) in preparing analytical reports, information papers, and briefings for executive level recipients.
- IAW DoDD 8570.1 requirements for Cyber Security Work Force this position will require, at least, an Information Assurance Manager (IAM) Level 2 Certified Information Systems Security Professional (CISSP), or equivalent certification.

4.10.2. Contractor Travel: No off-island travel is required

4.10.3. Performance Requirements:

- With guidance from the USPACOM Information Assurance team, and in accordance with USPACOM policies, evaluate, recommend, and prepare the appropriate IA/Network Operations risk management reviews and C&A documentation for projects/areas under the control of the IT Services Division; e.g., voice, data, and video.
- Transform J6 DIACAP formatted C&A documentation packages to NIST based or USPACOM specified formats.

4.10.4. See PART 6 – TABLES: Table 1, “Minimum requirements for Firm Fixed Priced CLIN”

4.10.5. See PART 6 – TABLES: Table 2, “Additional Labor for Labor-Hour CLIN”

4.10.6. See PART 6 – TABLES: Table 3, “Performance Objective Summary”

4.10.7. See PART 6 – TABLES: Table 4, “Deliverables Schedule”

4.11. Compliance

4.11.1. Special Qualifications:

- Must have experience related to IA, IT, CND, or defensive cyberspace operations.
- Must have experience in a Regional Cyber Center/Network Control Center or National Cyber Center/Network Control Center.
- Must have experience managing HBSS on a distributed network.
- Experience using Microsoft Office tools (Word, Excel, PowerPoint, Outlook, and Visio) in preparing analytical reports, information papers, and briefings for executive level recipients.
- IAW DoDD 8570.1 requirements for Cyber Security Work Force this position will require, at least, an Information Assurance Manager (IAM) Level 2 Certified Information Systems Security Professional (CISSP), or equivalent certification.

4.11.2. Contractor Travel: No off-island travel is required

4.11.3. Performance Requirements:

- Contractor shall provide Cybersecurity research, analysis and reporting for all Cybersecurity compliance issues. Scope of work includes, but is not limited to, tracking, validating, and reporting USCYBERCOM TASKORD and IAVA compliance status for HQ USPACOM, subordinate and Direct Reporting Units.
- Contractor shall oversee the USPACOM Assured Compliancy Assessment Solution (ACAS) and Continuous Monitoring Risk Scoring (CMRS) systems. Contractor shall ensure detailed compliancy processes are properly implemented and followed. Contractor shall review current policies and provide recommendations for updates as required.
- Contractor shall identify, document, and effectively coordinate the preparation for all Command Cyber Readiness Inspections (CCRI), Staff Assisted Visits (SAV), and Security Tests & Evaluations (ST&E). Contract shall perform network and physical security risk assessments in support of the USPACOM Information System AO and ISSM.
- Contractor shall conduct technical and procedural audits of systems using evaluation tools and configuration standards such Security Requirement Guides (SRG), Security Technical Implementation Guides (STIG), Security Content Automation Protocol (SCAP) automated tools, STIG Viewer, SCAP Compliance Checker (SCC), HBSS Policy Auditor, and DISA STIG Viewer, and Vulnerability Management System (VMS). Contractor shall notify USPACOM ISSM within 1 business day upon discovery of any Category 1 (CAT 1), very high or high severity vulnerabilities.
- Contractor shall provide overall USPACOM information systems compliancy status, vulnerability trends, and briefs to USPACOM leaders and ISSM.

4.11.4. See PART 6 – TABLES: Table 1, "Minimum requirements for Firm Fixed Priced CLIN"

4.11.5. See PART 6 – TABLES: Table 2, "Additional Labor for Labor-Hour CLIN"

4.11.6. See PART 6 – TABLES: Table 3, "Performance Objective Summary"

4.11.7. See PART 6 – TABLES: Table 4, "Deliverables Schedule"

4.12. Portfolio Program Support

Contractor shall provide the system expertise administration and solution implantations that meets unique goals and objectives of the Portfolio Program for USPACOM. Perform efforts necessary to perform Portfolio Program responsibilities

4.12.1. Special Qualifications: Must have IT project or program management experience

4.12.2. Contractor Travel: No off-island travel is required

4.12.3. Performance Requirements:

- Contractor will provide technical, analytical, and system expertise for operations for the USPACOM Portfolio Program. These efforts are to support the readiness and operations of USPACOM.
- Contractor will provide system program validation, analysis of portfolios to meet program gaps, and analysis of capability gaps for survivability of the systems supporting USPACOM operations.

4.12.4. See PART 6 – TABLES: Table 2, "Additional Labor for Labor-Hour CLIN"

4.12.5. See PART 6 – TABLES: Table 3, "Performance Objective Summary"

4.12.6. See PART 6 – TABLES: Table 4, "Deliverables Schedule"

4.13. Knowledge & Information Management Support

Contract will support the Command's knowledge management capability by conducting specialized knowledge management assessments to baseline existing processes and determine more efficient and effective alternatives; develop process improvement recommendations; provide knowledge management staff and user training; consultative support to USPACOM Directors, Branch Chiefs, project leads, and/or

staff members on an ad-hoc basis; conduct coordination with external knowledge management related agencies and activities to complete project milestones and deliverables; perform knowledge management duties as directed to support USPACOM staff during contingency operations and exercises.

Contractor will support the Command's information sharing and collaboration capability by conducting baseline assessments and evaluate existing information management platforms, applications, systems and processes. Also, contractor will provide recommendations for more efficient and effective alternatives. Contractor will assist in the development and documentation of processes and procedures needed to support the Command's information sharing and collaboration environment. Contractor will provide SharePoint business analyst capability to identify gaps in processes, find opportunities for improvements, capture requirements, create mockups, generate proof of concept solutions, assist in implementation and training, and document improvements leveraging the current Command's SharePoint platform's features and capabilities.

4.13.1. Special Qualifications:

Knowledge Management Specialist:

- Must have experience in Program/Project Management.
- Must have experience in Knowledge Management disciplines and practices.
- Must have experience using Microsoft Office tools (Word, Excel, PowerPoint, Outlook, Project and Visio) in preparing analytical reports, information papers, and briefings for executive level recipients.

Information Management Analyst:

- Must have experience in Program/Project Management.
- Must have experience in SharePoint Content and Site Administration.
- Must have experience in SharePoint Information Architecture.
- Must have experience using Microsoft Office tools (Word, Excel, PowerPoint, Outlook, Project and Visio) in preparing analytical reports, information papers, and briefings for executive level recipients.

4.13.2. Contractor Travel: No off-island travel is required

4.13.3. Performance Requirements:

Information Architecture: Contractor will review, evaluate and propose information architectures and recommend appropriate technical approaches for the PACOM Portals. Work will focus on PACOM's Strategic, Operational and Administrative plans and facilitate user navigation and search access to relevant information to more efficiently and effectively achieve mission objectives.

Taxonomy: Contractor will develop2, implement and maintain taxonomy (or taxonomies) which are currently implemented in the SharePoint Managed Metadata Store and Concept Searching. Contractor's assistance will help ensure that the taxonomies are implemented properly to support effective user search, faceted search and the search-based content strategy.

Search: Contractor will develop, implement and maintain Search functions; critical for users trying to find information. Contractor's assistance will help ensure our search functionality is configured for optimal performance.

Identity Management: Contractor will implement and maintain portal identity management (permissions structure, administration, auditing, etc.) critical to support the information architecture that underlies all operation and exercise collaboration sites. Contractor's assistance in providing us with an actionable identity management strategy which is consistent with the planned information architecture will ensure our critical operation and exercise collaboration portal is accessible as required by internal staff and external agencies.

Governance: Using the existing SharePoint Governance Framework, contractor will develop, refine, and implement Portal Governance. Contractor's assistance will help ensure that the portals are properly managed and content is current, relevant, consistent, and secure.

Portal Migration: Contractor will review current implementation and develop recommendations for migrating to the current version of the then-current portal solution. Contractor's assistance will help ensure that PACOM deliberately manages and plans lifecycle management of the portal.

Automating Business Processes: Contractor will work with users to analyze business processes and develop and implement solutions that will automate the processes.

KM Maturity: Contractor will help mature Knowledge Management at HQPACOM. Using the PACOM KM maturity model as a foundation, recommend and implement changes in the HQ to improve KM capabilities and maturity. Areas include (but are not limited to):

- Communities of Practice
- Lessons Learned
- Developing a knowledge sharing culture
- Knowledge sharing framework
- Collaboration
- Strategy design
- Process improvement
- Succession planning
- Integrating KM practice

4.13.4. See PART 6 – TABLES: Table 2, "Additional Labor for Labor-Hour CLIN"

4.13.5. See PART 6 – TABLES: Table 3, "Performance Objective Summary"

4.13.6. See PART 6 – TABLES: Table 4, "Deliverables Schedule"

4.14. Video Teleconferencing Support

Video Teleconferencing (VTC) System Services include the personnel and equipment needed to support all aspects of VTC operation within USPACOM. VTC System personnel require an understanding of VTC equipment/system standards, components, configurations, scheduling, and setup procedures. They operate as the first-line troubleshooter for all the hardware and software configurations of the VTC control systems and end devices. They assist users by setting up necessary conference room VTC systems for briefings, presentations, and conferences and work closely with A/V personnel to establish VTC connectivity and to verify all VTC and A/V equipment is functional.

VTC System Services also include evaluating the effectiveness of existing VTC systems, and recommending the development of innovative policies, procedures, solutions, and management tools for Information Operations. The contractor will develop, plan, and implement short and long term goals, objectives and strategies in support of Information Operations and determine the associated resource requirements. In addition, they contractor will evaluate new technology products for use in cutting edge systems.

4.14.1. Special Qualifications:

- experience using Microsoft Office tools (Word, PowerPoint, Excel, and Outlook) in preparing reports, information papers, and briefings for the PACOM Staff as required.
- experience with the operation of VTC equipment (Cisco, Tandberg, Polycom, etc). Service Desk experience is desired.
- VTC hardware and software troubleshooting skills.
- ability to effectively communicate with customers (including professional telephone etiquette). The ability to effectively work with all levels of technology users and leadership.
- ability to work in a highly visible, constantly changing, fast-paced, high-level government environment supporting military, government and contractor personnel is required.
- Security + certification is desired, but not required.

4.14.2. Contractor Travel: No off-island travel is required

4.14.3. Performance Requirements:

- Manage and sustain all aspects of the HQ USPACOM VTC Request System at HQ USPACOM. The Contractor may be tasked to support real world contingencies/operations and exercises in support of the HQ USPACOM mission.
- Schedule and coordinate VTCs for HQ USPACOM Commander, Deputy Commander and Staff.
- Provide a VTC Scheduler experienced with the operation of VTC equipment (Cisco, Tandberg, Polycom, etc). Experience on a Service Desk is preferred.
- Provide technical and operational VTC troubleshooting solutions to internal and external organizations.
- Ensure proper steps are taken to troubleshoot and resolve problems, raise the problem process to the appropriate resource level and be responsible for the problem until resolution.
- Identify and brief J642 leadership with regards to manpower support for HQ USPACOM Commander, Deputy Commander and Staff VTCs.
- Provide and oversee VTC scheduling training to HQ USPACOM Staff and newly assigned J642 VTC Operators as required.
- Provide official written recommendation on solutions and complex trouble resolutions as required and develop and maintain VTC Scheduling Standard Operating Procedures (SOPs)
- Provide a monthly status report to summarize the work accomplished and describe the work planned for the following month. The report also shall highlight problems, issues and/or concerns requiring USPACOM assistance to resolve.

4.14.4. See PART 6 – TABLES: Table 2, "Additional Labor for Labor-Hour CLIN"

4.14.5. See PART 6 – TABLES: Table 3, "Performance Objective Summary"

4.14.6. See PART 6 – TABLES: Table 4, "Deliverables Schedule"

4.15. Audio Visual Support

Audio Visual (A/V) System Services include the personnel and equipment needed to support all aspects of A/V operation within USPACOM. A/V System personnel require an understanding of A/V equipment/system standards, components, configurations, and setup procedures. They operate as the first-line troubleshooter for all the hardware and software configurations of the A/V control systems and end devices such as DVDs, VCRs, audio systems, video display units, projectors, room A/V control systems, etc. They assist users by setting up necessary conference room A/V systems for briefings, presentations, and conferences and work closely with VTC personnel to establish VTC connectivity and to verify all A/V equipment is functional.

4.15.1. Special Qualifications:

- experience using Microsoft Office tools (Word, PowerPoint, Excel, and Outlook) in preparing reports, information papers, and briefings for the PACOM Staff as required.
- Be "Certified Technology Specialist" (CTS) and "Security+" certified.
- Microsoft Office Visio or AutoCAD experience is preferred.
- experience in A/V and VTC systems and operations.

4.15.2. Contractor Travel: No off-island travel is required

4.15.3. Performance Requirements:

- Manage and sustain HQ USPACOM A/V and VTC systems for full operational capability per mission requirements. The Contractor may be tasked to support real world contingencies/operations and exercises in support of the HQ USPACOM mission.
- Provide first-line (Tier 1) troubleshooting and maintenance for all the hardware and software configurations of USPACOM A/V and VTC systems, A/V infrastructures and components, and AMX brand A/V control systems to internal and external organizations as directed and required.
- Provide recommendations for new A/V system hardware and software and recommend improvements to existing A/V systems as directed and required. Provide official written recommendation on A/V and VTC solutions and complex trouble resolutions.

- Ensure proper steps are taken to troubleshoot and resolve problems, raise the problem to the appropriate resource level and be responsible for the problem until resolution.
- Provide accurate A/V and VTC documents, diagrams, and programming codes as directed and required. Documents, diagrams, and programming codes will be safeguarded, filed, and stored appropriately and furnished to the Government upon completion of task or contract, whichever occurs first.
- Ensure A/V and VTC systems meet USPACOM Information Assurance (IA) and USPACOM Security Office Federal, DoD, local, and industry policies/standards for security compliance.
- Account for and provide an accurate equipment (hardware and software) inventory list quarterly.
- Provide A/V and VTC systems and equipment training to newly assigned J6421 personnel as required and develop and maintain A/V and VTC Standard Operating Procedures (SOPs) as directed.
- Provide a monthly status report to summarize the work accomplished and describe the work planned for the following month. The report also shall highlight problems, issues and/or concerns requiring USPACOM assistance to resolve.

4.15.4. See PART 6 – TABLES: Table 2, "Additional Labor for Labor-Hour CLIN"

4.15.5. See PART 6 – TABLES: Table 3, "Performance Objective Summary"

4.15.6. See PART 6 – TABLES: Table 4, "Deliverables Schedule"

4.16. Asset Management

Contractor shall identify, control, record, track, report, audit and verify the value and ownership of assets (also known as, Configuration Items (CI)) throughout their lifecycles, and for maintaining information about CIs required to deliver an IT Service and the relationships between CIs.

4.16.1. Special Qualifications:

- Must have experience in IT management (additional experience in Logistics is desired).
- No certification requirements exist.

4.16.2. Contractor Travel: No off-island travel is required

4.16.3. Performance Requirements:

- Identify, control, record, track, report, audit and verify the value and ownership of accountable assets (also known as CIs) throughout their lifecycle.
- Maintain information about CIs required to deliver an IT Service.
- Document the relationships between CIs.
- Produce status accounting reports.

4.16.4. See PART 6 – TABLES: Table 2, "Additional Labor for Labor-Hour CLIN"

4.16.5. See PART 6 – TABLES: Table 3, "Performance Objective Summary"

4.16.6. See PART 6 – TABLES: Table 4, "Deliverables Schedule"

4.17. Configuration Management

Contractor shall provide Subject Matter Expertise (SME) and oversight on Configuration Management (CM) disciplines and processes in support of the USPACOM missions and capabilities. The Configuration Management Engineer develops and promotes policies, processes, procedures and resources which will enable; management and control CM processes.

4.17.1. Special Qualifications:

- Must have experience in IT management and/or systems/network operations experience; preferably in a DoD environment.
- "Security+" certification is desired, but not required.

4.17.2. Contractor Travel: No off-island travel is required

4.17.3. Performance Requirements:

- Perform configuration management using ITIL based Configuration and Change processes and a Configuration Management System (CMS) and record the receipt of new or revised configuration changes into the appropriate CMS library and archives records.
- Review CM data; drawings and documents and ensures they meet policies and procedures and preparation of the Configuration Management Plan and CM process and procedures documentation.
- Identification service assets and CIs and develop and maintain HQ USPACOM Service Catalog.
- Collection, documentation and validation of CM audits and development and maintaining CM numbering and naming schema.
- Provide consultative support to HQ USPACOM Directors, Branch Chiefs, and project leads and/or staff members on an ad hoc basis by providing research and/or other well-informed options. Provide responses to requests for CM support within one day of receiving a request.
- Conduct coordination with external CM related agencies and activities to identify CM methodologies and approaches for use by HQ USPACOM. This includes coordination support for efforts by academia, corporations, vendors, and other Government agencies and organizations.
- Ensure configuration changes are recorded, assessed, authorized, prioritized, planned, tested, implemented, documented and reviewed in a standardized and controlled manner.
- Manage and lead the Configuration Control Board (CCB):
- Prepare CCB agenda and meeting minutes.
- Review Request for Change inputs for completeness and compliance with policies and procedures, allocate priority, and schedule CCB meetings.
- Track and monitor approved change requests through the release process to ensure change is properly implemented and documented in CMS system.
- Track and follow up on CCB action items, reporting status to CCB and ensure actions are validated, completed and entered into the CMS system.
- Manually or through automatic processes ensure Configuration Control data is recorded in the CMS system and remains up-to-date.

4.17.4. See PART 6 – TABLES: Table 2, “Additional Labor for Labor-Hour CLIN”

4.17.5. See PART 6 – TABLES: Table 3, “Performance Objective Summary”

4.17.6. See PART 6 – TABLES: Table 4, “Deliverables Schedule”

5. PART 5 - APPLICABLE POLICIES

The Contractor shall furnish sufficient personnel to perform all work specified within this contract.

The Contractor must abide by all applicable regulations, publications, manuals, and local policies and procedures.

The Contractor is required to comply with Public Law 105-270, Section 5 (2)(A). This law states that Contractors will not perform inherently governmental functions. Section 5 (2)(A) of this Public Law defines the term "inherently governmental function" as "a function that is so intimately related to the public interest as to require performance by Federal Government employees." Per Section 5(2)(B), inherently governmental functions include management of Government programs requiring value judgments, conduct of foreign relations, selection of program priorities, and the direction of intelligence and counter-intelligence operations. Per Section 5(2)(C), inherent governmental functions DO NOT include, (i) gathering information for or providing advice, opinions, recommendations, or ideas to Federal Government officials; or (ii) any function that is primarily ministerial and internal in nature."

Contractors shall not establish an employee-employer relationship with USPACOM under this PWS. Contractors shall not provide personal services to USPACOM under this PWS. Contractor personnel may not manage, supervise or task DOD civilian employees or military personnel while performing the tasks within this PWS. Contractor personnel may not make any commitment to non-DOD personnel, including a foreign official, which commits the expenditure of US Government resources, unless specifically authorized. The training of foreign personnel is prohibited under this PWS.

When performing work associated with this PWS, Contractor personnel will make clear to all individuals they deal with that they are Contractor employees and not DOD employees. When participating and introducing themselves during official events wherein DOD, non-DOD or foreign officials are present, Contractor personnel will identify themselves as employees of the Contractor. Contractor personnel must be clearly identified (i.e., company shirt, pin, visible company ID, etc.).

Contractor employees performing services shall be required to comply with all HQ USPACOM and installation rules and regulations applicable to conduct, safety, security, and procedures governing site entry and exit.

Contractor personnel shall be required to safeguard data files and output products, regardless of format or medium, in accordance with appropriate security measures for classification of data being handled within Headquarters USPACOM (see DOD Regulation 5200.1, OPNAVINST 5500.2). Contractor personnel shall also safeguard Privacy Act Information in accordance with existing regulations.

Contractor personnel shall be required to read this PWS and understand, in particular, the provisions of this paragraph. All personnel shall comply with the U.S. Army Corps of Engineers EM 385-1-1 (2003) "Safety and Health Requirements Manual" (EM 385-1-1 is used as the DON's safety manual) and trained in the requirements of 29 CFR 1910, 29 CFR 1925, 29 CFR 1926, HRS Chapter 396 (HIOSH) and other applicable safety requirements.

6. PART 6 – TABLES

Table 1: Minimum requirements for Firm Fixed Priced Contract Line Item (CLIN)

PWS Task	Estimated Labor Category	Estimated # FTEs	Clearance
4.1. Software & Portal Support	Application Engineer (Level I)	1	TS/SCI
	Application Engineer (Level II)	1	TS/SCI
4.2. Service Desk Support	Communications Specialist	1	Secret
	Help Desk Specialist	2	Secret
4.3. Network Engineering	Systems Engineer – Senior	2	TS/SCI
	Network Administrator - Intermediate	1	TS/SCI
4.3 System Administration	Systems Administrator (Windows) – Senior	1	TS/SCI
	Systems Administrator (VI) - Senior	1	TS/SCI
	Systems Administrator (Linux) – Senior	1	TS/SCI
4.4. Removed			
4.5. Electronic Key Management Support	Computer Security Sys Specialist (Level I)	2	Secret
4.6. System Integration	Project Leader	1	TS/SCI
4.7. Project Management	Project Manager (Level II)	1	TS/SCI
4.8. Computer Network Defense Support	Data Security Specialist	1	TS/SCI
	"CND" Subject Matter Expert (Level I)	1	TS/SCI
4.9. Enterprise Architecture Framework	System Architect (Level II)	1	Secret
4.10. Assessment, Certification and Authorization	Data Security Consultant	1	Secret
4.11. Compliance	Computer Security Sys Specialist (Level II)	1	TS/SCI

Table 2: Additional Labor for Labor-Hour Contract Line Item Number (CLIN)

PWS Task	Estimated Labor Category	Estimated Level of Effort (HOURS)	Clearance
4.1. Software & Portal Support	Applications Systems Analyst/Programmer - Intermediate	1440	TS/SCI
	Web Software Developer	1440	TS/SCI
4.2. Service Desk Support	Help Desk Specialist	1440	Secret
4.3. Network Engineering	Network Administrator - Intermediate	1440	TS/SCI
4.3 System Administration	Systems Administrator (Windows) – Intermediate	1440	TS/SCI
	Systems Administrator (AMHS) – Intermediate	1440	TS/SCI
	Systems Administrator (GCCS) – Intermediate	1400	TS/SCI
4.4. Telecommunications Support	Telecommunications Engineer/Analyst – Intermediate	2880	TS/SCI
	Telecommunications Engineer/Analyst – Senior	1440	TS/SCI
4.8. Computer Network Defense Support	Data Security Administration Manager	1440	TS/SCI
	Data Security Analyst – Senior	1440	TS/SCI
4.10. Assessment, Certification and Authorization	Data Security Analyst - Intermediate	2880	Secret
4.11. Compliance	Data Security Analyst - Intermediate	1440	TS/SCI
4.12. Portfolio Program Support	Data Architect	2880	Secret
4.13. Knowledge & Information Management Support	Business Systems Analyst - Intermediate	4320	TS/SCI
	Data/Configuration Management Specialist	2880	TS/SCI
4.14. Video Teleconferencing Support	Help Desk Specialist	1440	TS/SCI
4.15. Audio Visual Support	Telecommunications Analyst/Technician	1440	TS/SCI
4.16. Asset Management	Help Desk Specialist	1440	Secret
4.17. Configuration Management	Business Systems Specialist	1440	Secret

Table 3: Performance Objectives

PWS Task	Performance Objective	Performance Threshold
4.1. Software & Portal Support	Respond to trouble calls for O&M applications.	95% delivery and compliance. Deviations from response times must be approved by government supervisors and coordinated with users.
	Manage lifecycles of applications. Execution timeframe from initial customer request to delivery of the product shall be within +/- 5% within the base-lined project plan timeline intervals.	95% delivery and compliance. Deviations from project milestone dates must be approved by government supervisors and coordinated with users
	Conduct feasibility studies with level of effort, timelines, and costs. Contractor shall provide results of feasibility study within 30 days of being assigned.	95% delivery and compliance. Deviations from scheduled delivery dates must be approved by government supervisors and coordinated with users.
	Provide demonstrations of applications maintenance modifications as needed. Demonstrations will be provided as specified by the base-lined project work break structure task within +/- 5% of the timeline	95% delivery and compliance. Deviations from response times must be approved by government supervisors and coordinated with users
	Analyze and determine appropriate programming language and database for PWS requirements. Findings and recommendations to be provided NLT 30 days upon completion of analysis.	95% delivery and compliance. Deviations from response times must be approved by government supervisors and coordinated with users
	Conduct testing and evaluation of applications and database. Testing shall begin as specified by the baseline project work break structure task within +/- 5% of the timeline. Evaluations and recommendations shall be provided to the government NLT 10 business days after testing concludes.	95% delivery and compliance. Deviations from scheduled delivery dates must be approved by government supervisors and coordinated with users
	Create project database and all necessary tables, views & fields. Contractor shall complete database for government review & approval as specified by the base-lined project work break structure task within +/- 5% of the timeline.	95% delivery and compliance. Deviations from scheduled delivery dates must be approved by government supervisors and coordinated with users
	Deliver final product, and documentation.	95% delivery and compliance. Deviations from scheduled delivery dates must be approved by government supervisors and coordinated with users

	Project management plans, including risk management plans, Gantt and quad charts, NLT 30 days after initial identification and assignment of new projects.	95% delivery and compliance. Deviations from scheduled delivery dates must be approved by government supervisors and coordinated with users.
4.2. Service Desk Support	The contractor shall provide service execution to CLIN conversion within two (2) business days.	95% delivery and compliance.
	The contractor shall provide service management to EITSMS processing within one (1) business day.	95% delivery and compliance.
4.3. Network Engineering and System Administration	Provide engineering and system administration for assigned systems.	Performance occurs with no required rework at least 80% of the time. Problems that occur are minor and are resolved in a satisfactory manner.
	Ensure administered/assigned services/systems remain available.	Available at least 99% of the time (outside of approved Authorized Service Interruptions (ASIs)).
	Deploy network routers, switches, firewalls and VTC-specialized equipment on the operational networks with minimal downtime.	Performance occurs with no required rework at least 80% of the time. Problems that occur are minor and are resolved in a satisfactory manner.
	Complete Security Technical Implementation Guide (STIG) validation and account for vulnerabilities in the Vulnerability Management System (VMS).	100% compliance
4.4. Telecommunications Support *Only Applicable to Additional Labor for Labor-Hour CLIN*	The Contractor shall provide "Acceptable Service Response" (within 2 hours), 24 x 7; includes after hours, weekends, holidays. Fully operational within 24 hours after receipt of applicable parts.	98% delivery and compliance.
	The Contractor shall develop and implement (at the direction of the Government) Disaster Recovery Procedures and Protocols.	98% delivery and compliance.
	Update and maintain current PBX systems documentation and Standard Operating Procedures for the EAS System.	100% compliance
	The Contractor shall provide "Acceptable Service Response" (within 2 hours), 24 x 7; includes after hours, weekends, holidays. Fully operational within 24 hours after receipt of applicable parts.	99% delivery and compliance.

	The Contractor shall provide "Acceptable Service Response" (within 2 hours), 24 x 7; includes after hours, weekends, holidays. Fully operational within 24 hours after receipt of applicable parts.	98% delivery and compliance.
4.5. Electronic Key Management Support	EKMS Contractor shall receive, store, and transfer United States DoD COMSEC material.	100% compliance
	Contractor shall perform periodic inventories and inspections of all stored COMSEC material.	100% compliance
	Develop in-country distribution plans	95% compliance
	Receive COMSEC inventories, manage transaction files, and receive and publish COMSEC policies.	100% compliance
	Provide on-site/on-equipment informal unit training to coalition personnel.	95% compliance
	Develop local informal training programs.	95% compliance
	Report on the current status of COMSEC-related issues to the CCIB and IMB.	95% compliance
	Provide keying material in contingency/emergency situations.	100% compliance
	Produce and submit required accounting records and reports to the USPACOM Theater COMSEC Manager.	100% compliance
	Perform destruction of COMSEC material when required as directed by the NSA COR keying material CONAUTH.	100% compliance
	Conduct an inventory semiannually and upon appointment of a new COMSEC Custodian.	100% compliance
4.6. System Integration	Oversee assigned project, ensure best practices and security standards are followed and integrate it into the PACOM portfolio.	Performance occurs with no required rework at least 80% of the time. Problems that occur are minor and are resolved in a satisfactory manner.
4.7. Project Management	Oversee assigned projects and ensure best practices and security standards are followed.	Performance occurs with no required rework at least 80% of the time. Problems that occur are minor and are resolved in a satisfactory manner.
4.8. Computer Network Defense Support	Manage the lifecycle of HBSS.	98% delivery and compliance
	Provide weekly HBSS Baseline	95% delivery and compliance

	Report	
	Update detection signatures and ACLs.	100% delivery and compliance
	Provide weekly cyber threat summaries, to include all incident response activities directly affecting USPACOM CND or supporting activities.	95% delivery and compliance
4.9. Enterprise Architecture Support	JIE/MPE Project Management	95% delivery and compliance
	JIE/MPE Analysis	95% delivery and compliance
	Enterprise Architecture Analysis	95% delivery and compliance
	Cyberspace/ Cyber Security research	95% delivery and compliance
4.10. Assessment, Certification and Authorization	As the SME, provide analysis of IA systems and operations, as requested. Analysis shall include at a minimum current, developing, and future cyberspace systems to determine their impact on PACOM's portfolio at headquarters and subordinate organization.	95% delivery and compliance
	Produce detailed weekly status reports on the completion of assigned deliverables, open issues/problems, new task assignments and ATO packages expiring within the next 30 days.	94% delivery and compliance
	Provide monthly report(s) that details monthly accomplishments, the systems' risk register, systems' ATO compliance status, and any outstanding issues and concerns.	92% delivery and compliance
	Produce RMF and DIACAP Assessment and Authorization artifacts; publish to Enterprise Mission Assurance Service (eMASS)	95% delivery and compliance
	Process accounts for Vulnerability Management System (VMS), eMASS and any other C&A related automation tool.	95% delivery and compliance
	Notify PACOM ISSM within one business day of discovery of new category 1, very high or high severity vulnerabilities.	99% delivery and compliance
4.11. Compliance	Produce detailed weekly status reports on the completion of assigned deliverables	94% delivery and compliance
	Provide weekly systems' vulnerability and CYBERCOM task order compliance status report.	94% delivery and compliance
	Provide monthly report(s) that details monthly	92% delivery and compliance

	accomplishments/activities, automated risk scores generated from ACAS or CMRS, and any outstanding issues and concerns.	
	Conduct technical vulnerability assessments using and provide results to PACOM ISSM and Cybersecurity Compliance Team Lead.	95% delivery and compliance
	Notify PACOM ISSM within one business day of discovery of new category 1, very high or high severity vulnerabilities.	99% delivery and compliance
4.12. Portfolio Program Support	Implement the Archer application (MISSL) for portfolio valuation and management.	95% delivery and compliance. Deviations from scheduled delivery dates must be approved by government supervisors and coordinated with users.
	Implement and operationalize the Archer applications for Budget, Five year (5YR) plan, and ledger (current year execution).	95% delivery and compliance. Deviations from scheduled delivery dates must be approved by government supervisors and coordinated with users.
	Develop and implement the Enterprise Management module to include the asset management module.	95% delivery and compliance. Deviations from scheduled delivery dates must be approved by government supervisors and coordinated with users.
	Develop Standard Operating Procedures (SOPs) for the administration and use of Archer. Provide written administrative and user's manuals.	95% delivery and compliance. Deviations from scheduled delivery dates must be approved by government supervisors and coordinated with users.
4.13. Knowledge and Information Management Support	Weekly and monthly status reports	Reports contain required information and are delivered on time at least 90% of the time. Revisions that occur are minor and are resolved in a satisfactory manner.
	Documentation Deliverables	Documents contain required information and are delivered within 5 working days of the due date. Revisions that occur are minor and are resolved in a satisfactory manner.
4.14. Video Teleconferencing Support	VTC Manage and sustain VTC scheduling system	98% delivery and compliance
	Schedule and coordinate VTCs for HQ USPACOM Commander, Deputy Commander and Staff	98% delivery and compliance
	Provide technical and operational VTC troubleshooting solutions	98% delivery and compliance
	Identify and brief J642 leadership with regards to manpower support	98% delivery and compliance

	for HQ USPACOM Commander, Deputy Commander and Staff VTCs.	
	Provide and oversee VTC scheduling training to HQ USPACOM Staff and newly assigned J642 VTC Operators as required.	98% delivery and compliance
	Develop and maintain VTC Scheduling Standard Operating Procedures (SOPs)	98% delivery and compliance
4.15. Audio Visual Support	Provide Acceptable Service Response (within 2 hours) and become fully operational within 24 hours after receipt of applicable parts.	98% delivery and compliance
	Maintain and Sustain A/V and VTC Systems.	98% delivery and compliance
	Provide accurate documentation, diagrams, programming codes, and SOPs	100% delivery and compliance
4.16. Asset Management	Provide accounting reports	95% delivery and compliance
4.17. Configuration Management	Oversee configuration changes and additions while ensuring best practices and security standards are followed. Integrate changes into the appropriate CMS library.	Performance occurs with no required rework at least 80% of the time. Problems that occur are minor and are resolved in a satisfactory manner
	Conduct the Configuration Control Board	99% delivery and compliance

Table 4: Deliverables Schedule

PWS Task	Deliverable	Frequency	# of Copies	Medium/Format	Submit To
4.1. Software & Portal Support	Monthly Status Report	Monthly	2	MS Word or PDF submitted via email	COR/TA
	Project Checklists (if assigned as Project Lead)	Within 10 business days of new development project assignment	1	As appropriate: MS Word, MS Excel, MS Project or PDF submitted via email	COR/TA
	Formal Activities Report	Included in the Monthly Status Report	N/A	N/A	N/A
	Incident Call Log	Within 1 day from the end of the recorded activity	1	Electronically via USPACOM's trouble-ticketing system.	COR/TA
	In-Progress Reviews (IPR)	As required by Project timeline (produced by the Project Lead)	1	As appropriate: MS Word, MS Excel, MS Project or PDF submitted via email	COR/TA
	Feasibility Report	Within 30 days of new development project assignment	1	MS Word or PDF submitted via email	COR/TA
	Weekly Activity Report	Weekly, by close of business each work week.	1	As directed by the Section Chief, either verbally or via email	COR/TA
	Findings and Recommendation Report	Within 30 days of analyzing new requirements and included in weekly and monthly status reports.	1	MS Word or PDF submitted via email	COR/TA
	Evaluation and Recommendation Report	Within 10 business days after application module testing	1	MS Word or PDF submitted via email	COR/TA
	Creation of new relational databases (to include DB tables, views and fields)	As required by Project timeline (produced by the Project Lead)	1	MS SQL	COR/TA
	Completed Projects (if assigned as Project Lead)	Within 3 days of project completion	1	As appropriate: MS Word, MS Excel, MS Project and/or PDF submitted via	COR/TA

				email. MS SQL database if produced	
	Project Plan (if assigned as Project Lead)	Within 30 days of assigned projects	1	As appropriate: MS Word and/or MS Project submitted via email	COR/TA
4.2. Service Desk Support	Monthly Status Report	Monthly; due 5 business days from the last day of the preceding month	2	MS Word or Adobe PDF submitted via email	COR/ TA
	Software Applications and supporting data	Within 3 business days of the initial request	1	via DADMS and/or via email or disk	COR/TA
	Process Seat Ordering Requests	Within 2 business days of the initial request	1	via NET	COR/TA
	eForms Service Requests	Within 1 business day of the initial request	1	via eForms	COR/TA
	Monthly Status Report	Monthly; due 5 business days from the last day of the preceding month	2	MS Word or Adobe PDF submitted via email	COR/ TA
	Recommendations and suggestions	Within 10 business days of task assignment	1	MS Word, MS Visio and/or Adobe PDF submitted via email	COR/TA
	STIG validation report	Quarterly; due 5 business days from the last day of the preceding quarter	1	MS Word or Adobe PDF submitted via email	COR/TA
	Architecture and rack diagrams	Within 10 business days of task assignment	1	MS Word, MS Visio and/or Adobe PDF submitted via email	COR/TA
	Lifecycle Refresh Plan	Within 30 days of task assignment	1	MS Word, MS Visio and/or Adobe PDF submitted via email	COR/TA
	Build documents and SOPs	Within 30 days of task	1	MS Word, MS Visio and/or	COR/TA

		assignment		Adobe PDF submitted via email	
	Updated configuration management documents	Within 30 days of task assignment	1	In the same form as the document being updated	COR/TA
	Develop Software Update Procedures	Within 30 days of task assignment	1	MS Word, MS Visio and/or Adobe PDF submitted via email	COR/TA
	Splunk system log and alerts reports	Weekly, by close of business each work week.	1	MS Word, MS Excel and/or Adobe PDF submitted via email	COR/TA
4.4. Telecommunications Support *Only Applicable to Additional Labor for Labor-Hour CLIN*	Monthly Status Report	Monthly; due 5 business days from the last day of the preceding month	2	MS Word or Adobe PDF submitted via email	COR/ TA
	Recommendations and suggestions	Within 10 business days of task assignment	1	MS Word, MS Visio and/or Adobe PDF submitted via email	COR/TA
	Updated PBX systems documentation and Standard Operating Procedures for the EAS System.	As required; 5 business days from the date the updates were documented	1	MS Word or Adobe PDF submitted via email	COR/TA
	Government Disaster Recovery Procedures and Protocols.	As required; NLT 60 calendar days from task assignment	1	MS Word or Adobe PDF submitted via email	COR/TA
	Engineer DRSN-related solutions	Within 10 business days of task assignment	1	MS Word, MS Visio and/or Adobe PDF submitted via email	COR/TA
	Document DRSN Operational and Maintenance issues	IAW the current DISA O&M guidelines	1	via DISA's current logging tool	COR/TA
	Software baseline and patch tracker	As required; 5 business days from the date the baseline/update was released	1	MS Word, MS Visio and/or Adobe PDF submitted via email	COR/TA
4.5. Electronic Key Management	Monthly Status Report	Monthly; due 5 business days	2	MS Word or Adobe PDF	COR/TA

Support		from the last day of the preceding month		submitted via email	
	Inventories	Quarterly; NLT 1st business day of the 2nd month of the quarter	1	In the format dictated by NSA (re: para 4.5.3.2)	COR/TA
	In-country Distribution Plans	Within 30 days of task assignment	1	MS Word, MS Excel, Adobe PDF or other applicable products such as MS Project; submitted via email	COR/TA
	Local Informal Training Materials	Within 30 days of task assignment	1	MS Word, MS PowerPoint, Adobe PDF or other applicable products submitted via email	COR/TA
	Meeting Minutes and Status Reports	As required; within 3 business days after the meeting	1	MS Word or Adobe PDF submitted via email	COR/TA
	Standard Operating Procedures	As required; NLT 60 calendar days from task assignment	1	MS Word or Adobe PDF submitted via email	COR/TA
	Accounting Operating Procedures	As required; NLT 60 calendar days from task assignment	1	MS Word or Adobe PDF submitted via email	COR/TA
	Transfer, Destruction, and Possession Reports	As required; NLT 3 business days from transfer, destruction, or possession	1	MS Word or Adobe PDF submitted via email	COR/TA
	Updated COMSEC Publications	As required; NLT 10 business from task assignment	1	In the same format as the publication updated	COR/TA
4.6. System Integration	Monthly Status Report	Monthly; due 5 business days from the last day of the preceding month	2	MS Word or Adobe PDF submitted via email	COR/ TA
	Recommendations and suggestions	Within 10 business days of	2	MS Word, MS Visio and/or	COR/TA

	report	task assignment		Adobe PDF submitted via email	
	Product Plan Updates	Monthly; every 30 days from project initiation until completion (if contractor is assigned as project lead)	1	MS Word, Adobe PDF or other applicable products such as MS Project; submitted via email	COR/TA
	Risk and Risk Management Report	As required by Project timeline (produced by the Project Lead)	2	MS Word or PDF submitted via email	COR/TA
	Overarching Project Timeline	Within 30 days of new project assignment	2	MS Word, Adobe PDF or other applicable products such as MS Project; submitted via email	COR/TA
4.7. Project Management	Monthly Status Report	Monthly; due 5 business days from the last day of the preceding month	2	MS Word or Adobe PDF submitted via email	COR/ TA
	Recommendations and suggestions	Within 10 business days of task assignment	2	MS Word, MS Visio and/or Adobe PDF submitted via email	COR/TA
	Updated accreditation packages	Within 10 business days of task assignment	3	MS Word, MS Visio and/or Adobe PDF submitted via email	COR/TA
	Product Plan Updates	Monthly; every 30 days from project initiation until completion (if contractor is assigned as project lead)	1	MS Word, Adobe PDF or other applicable products such as MS Project; submitted via email	COR/TA
	Risk and Risk Management Report	As required by Project timeline (produced by the Project Lead)	2	MS Word or PDF submitted via email	COR/TA
4.8. Computer Network Defense Support	Monthly Status Report	Monthly; due 5 business days from the last	2	MS Word or Adobe PDF submitted via	COR/TA

		day of the preceding month		email	
	Recommendations and suggestions	Within 10 business days of task assignment	1	MS Word, MS Visio and/or Adobe PDF submitted via email	COR/TA
	Firewall Rule Sets and Host Intrusion Detection/Prevention Signatures	Weekly; by the 2nd business day of the following week	1	On associated systems	COR/TA
	Provide weekly HBSS Baseline Report	Weekly; by the 2nd business day of the following week	1	MS Word or Adobe PDF submitted via email	COR/TA
	Provide cyber threat summaries, to include all incident response activities directly affecting USPACOM CND or supporting activities.	Weekly; by the 2nd business day of the following week	1	MS Word or Adobe PDF submitted via email	COR/TA
4.9. Enterprise Architecture Support	Monthly Status Report	Monthly; due 5 business days from the last day of the preceding month	2	MS Word or Adobe PDF submitted via email	COR/ TA
	Findings and Recommendation Report	Within 30 days of analyzing new DOD Architecture products	1	MS Word, MS Visio and/or Adobe PDF submitted via email	COR/TA
	Project Plan (if assigned as Project Lead)	Within 30 days of assigned projects	2	As appropriate: MS Word and/or MS Project submitted via email	COR/TA
	Project Plan Updates (if assigned as Project Lead)	Within 5 business days of the update	2	As appropriate: MS Word and/or MS Project submitted via email	COR/TA
	Create schedule and coordinate coverage for upcoming Architecture meetings	At the beginning of each month	1	MS Word or Adobe PDF submitted via email	COR/TA
4.10. Assessment, Certification and Authorization	Monthly Status Report	Monthly; due 5 business days from the last day of the preceding month	3	MS Word, PowerPoint, Excel or PDF submitted via email	COR/TA

	Detailed weekly status reports on the completion of assigned deliverables, open issues/problems, new task assignments and ATO packages expiring within the next 30 days.	Weekly; by the 2nd business day of the following week	As appropriate	MS Word, PowerPoint, Excel or PDF submitted via email	COR/TA
	IA reports, briefings, recommendations, and presentations resulting from analysis of current, developing, and future cybersecurity systems	As required	As appropriate	IAW DOD 5110.4-M, Manual for Written Material or as required by the Government	COR/TA
4.11. Compliance	Monthly Status Report (include accomplishments, activities, automated risk scores generated from ACAS or CMRS, and any outstanding issues and concerns)	Monthly; due 5 business days from the last day of the preceding month	3	MS Word, PowerPoint, Excel or PDF submitted via email	COR/TA
	Detailed Weekly Status Reports (include systems' vulnerability and CYBERCOM task order compliance status)	Weekly; by the 2nd business day of the following week	As appropriate	MS Word, PowerPoint, Excel or PDF submitted via email	COR/TA
4.12. Portfolio Program Support	Monthly Status Report	Monthly; due 5 business days from the last day of the preceding month	2	MS Word, PowerPoint, Excel and/or PDF submitted via email	COR/ TA
4.13. Knowledge and Information Management Support	Monthly Status Report	Monthly; due 5 business days from the last day of the preceding month	2	MS Word, PowerPoint, Excel and/or PDF submitted via email	COR/ TA
4.14. Video Teleconferencing Support	Monthly Status Report	Monthly; due 5 business days from the last day of the preceding month	2	MS Word or Adobe PDF submitted via email	COR/TA
	Recommendations and suggestion	Within 10 business days of	1	MS Word, MS Visio and/or	COR/TA

	report	task assignment		Adobe PDF submitted via email	
	VTC Scheduling Standard Operating Procedures (SOPs)	As required; NLT 60 calendar days from task assignment	1	MS Word or Adobe PDF submitted via email	COR/TA
	VTC Scheduling SOP updates	As required; NLT 5 business days from the update date	1	MS Word or Adobe PDF submitted via email	COR/TA
4.15. Audio Visual Support	Monthly Status Report	Monthly; due 5 business days from the last day of the preceding month	2	MS Word or Adobe PDF submitted via email	COR/ TA
	Recommendations and suggestion report	Within 10 business days of task assignment	1	MS Word, MS Visio and/or Adobe PDF submitted via email	COR/TA
	A/V system documentation, diagrams, programming codes, and SOPs	As required; NLT 60 calendar days from task assignment	1	MS Word, MS Visio and/or Adobe PDF submitted via email	COR/TA
	Inventory List	Quarterly; NLT 5 business days after the end of the quarter	1	MS Word, MS Excel and/or Adobe PDF submitted via email	COR/TA
4.16. Asset Management	Monthly Status Report	Monthly; due 5 business days from the last day of the preceding month	2	MS Word or Adobe PDF submitted via email	COR/ TA
	CI Value and Ownership Reports	Within 10 business days of task assignment	1	MS Word, MS Excel and/or Adobe PDF submitted via email	COR/TA
	CI Relationship Report	As required; NLT 60 calendar days from task assignment	1	MS Word, MS Visio and/or Adobe PDF submitted via email	COR/TA
	Accounting Reports	Quarterly; NLT 5 business days after the end of the quarter	1	MS Word, MS Excel and/or Adobe PDF submitted via email	COR/TA
4.17. Configuration	Monthly Status	Monthly; due 5	2	MS Word or	COR/TA

Management	Report	business days from the last day of the preceding month		Adobe PDF submitted via email	
	Documented new or revised configuration changes	As required; NLT 5 business from the change	1	Updates to the CMS and a recap via MS Word, MS Visio and/or Adobe PDF submitted via email	COR/TA
	Develop the HQ USPACOM Service Catalog	As required; NLT 60 calendar days from task assignment	1	MS Word or Adobe PDF submitted via email	COR/TA
	Maintain the HQ USPACOM Service Catalog	As required; NLT 5 business days from the update date	1	MS Word or Adobe PDF submitted via email	COR/TA
	Develop the HQ USPACOM CM numbering and naming schema	As required; NLT 60 calendar days from task assignment	1	MS Word or Adobe PDF submitted via email	COR/TA
	Maintain the HQ USPACOM CM numbering and naming schema	As required; NLT 5 business days from the update date	1	MS Word or Adobe PDF submitted via email	COR/TA
	Respond to CM Support Requests	As required; NLT 1 business days from the update date	2	Email	COR/TA
	Provide the Configuration Control Board agenda	NLT 2 business days prior to a scheduled CCB.	As appropriate	Email	COR/TA
	Provide the Configuration Control Board minutes	NLT 2 business days after a scheduled CCB.	As appropriate	Email	COR/TA