

Headquarters Air Combat Command (HQ ACC)

9th Reconnaissance Wing

Performance Work Statement (PWS) for

69 RG Information Technologist Support Services

Revision 2.0, Dated: 27 September 2017

1.0 INTRODUCTION/BACKGROUND: The 69th Reconnaissance Group (69RG) conducts Intelligence, Surveillance, and Reconnaissance (ISR) operations essential for Combatant Commanders, Congressional, and National Command Authority decisions critical to the national defense. Comprised of the 348th Reconnaissance Squadron (348 RS) at Grand Forks AFB, ND and the 12 Reconnaissance Squadron (12 RS) at Beale AFB, CA, the 69RG conducts RQ-4 high-altitude qualification training and intelligence, surveillance, and reconnaissance missions. The squadron prepares combat elements for global employment, peacetime collection and Emergency War Order support.

2.0 TASK ORDER OBJECTIVE: The objective of this task order is to provide support services for information technology maintenance and operations in support of mission planning infrastructure. The contractor shall provide all necessary personnel, expertise, and management on location at Beale AFB, CA for the 12 RS, and Grand Forks AFB, ND for the 348 RS to accomplish the task order objectives. These objectives will be accomplished by fulfilling the requirements of the Information Technologist role for the squadron.

3.0 INFORMATION TECHNOLOGIST TASK REQUIREMENTS: The contractor shall provide analytical, advisory, technical expertise and analysis to 12 RS and 348 RS activities including performing and managing a variety of communication and information technology tasks. Requires network administrative privileges to perform duties. Is required to maintain training and certification requirements in order to sustain elevated rights to the appropriate domain(s). Performs Communications-Computer Systems (C-CS) planning and implementation activities. Provides support to communications systems current and future planning activities. Supports implementation of C-CS projects and ensures C-CS architecture, configuration, and integration conformity. Provides analytical, advisory, technical, functional and management oversight to network upgrades and maintenance regarding critical communications systems for the MPC. The Information Technologist will fulfill all requirements in paragraph. The contractor shall:

3.1 Subtasks - Information Technologist

3.1.1 Manage, operate and update squadron inventory of C-CS equipment per AFI. Typically referred to as ADPE or ITAMs. Work with wing organizations to properly comply with all applicable guidance and checklists (MICT) to pass annual inspections as directed by the AFI. Provide current accurate inventory no less than annually or as required by AFI.

3.1.2 Provide standard customer service, verified by the Contracting Officer's Representative (COR), to support squadron operations. Standard customer service includes, but is not limited to: The delivery of products and services at the agreed upon time to all customers. Listen to, accept, and act upon customer feedback. Assist all customers in defining their needs and requests. Provide courteous and professional customer service. Deliver the highest quality products and service with the goal of exceeding customer expectations. Customers must be satisfied with each transaction.

3.1.3 Ensure all electronic technical data, regulations, and instructions required for safe flight is current on all required systems, including, but not limited to: SpecView, technical orders, SPINS, CONOPS, etc.

3.1.4 Provide analytical, advisory, and technical support to the 12 RS and 348 RS Squadron Commander.

3.1.5 Assist the 12 RS and 348 RS Squadron Commander to improve GHOC integration into USAF and National architectures.

3.1.6 Provide C-CS desktop/laptop computer administration and support for squadron.

3.1.7 Provide analytical and advisory support in the development and direction of strategic hardware, software, and infrastructure systems planning efforts for the 12 RS and 348 RS.

3.1.8 Analyze/evaluate mission support systems and networks to recommend changes and upgrades to 12 RS and 348 RS leadership to maximize weapon system efficiency and effectiveness.

3.1.9 Provide system administration of SharePoint, Intelink, and other mission essential software programs on multiple networks at classification levels up to and including TS/SCI.

- 3.1.10** Monitor, maintain, and troubleshoot required equipment for a dedicated SIPR server to host SharePoint in support of GHOC operations. This site must be certified for, and maintain on-call, up to 24/7/365 continuous operation.
- 3.1.11** Provide technical and functional support ensuring RQ-4 Mission Control Element (MCE) and Launch Recovery Elements (LRE) are mission capable. Specifically support for SIPR workstations located in these enclosures.
- 3.1.12** Monitor, troubleshoot, and maintain Voice over Internet Protocol technology and switching equipment
- 3.1.13** Design, implement, monitor, maintain, and troubleshoot equipment, protocols, and/or frequencies associated with voice and data line-of-site and beyond-line-of-site radio frequency transmission systems as well as other technologies, methods, and systems relevant to MPC operations.
- 3.1.14** Ensure regulatory compliance for all 12 RS and 348 RS hardware, software, and network infrastructure
- 3.1.15** Maintain video teleconference and associated audio visual equipment in multiple conference and briefing rooms located in the 12 RS and 348 RS by keeping the equipment and network connections serviceable.
- 3.1.16** Observe/evaluate the GHOC Concept of Operations and provide recommendations to 12 RS and 348 RS senior leadership regarding improvements to increase the efficiency and effectiveness of system integration, operations, and maintenance.
- 3.1.17** Perform basic configuration management and initial system diagnostics on desktop computers, laptops, operating systems, and productivity software.
- 3.1.18** Conduct research of new and existing technologies to suggest and/or recommend technical solutions for new modifications or resolve system deficiencies.
- 3.1.19** Evaluate and recommend changes to current and future network requirements to meet the organization's needs.
- 3.1.20** Provide analytical, technical, functional and management support by coordinating and troubleshooting logistical issues and plans sustaining GHOC continued mission support activities.
- 3.1.21** Draft plans for integration of GHOC Communications systems. Perform mission review with communications systems customers for architectural integration and impact on C-CS infrastructure.
- 3.1.22** Maintain Communications systems planning and implementation source documents consisting of architectures, configuration management plans, and correspondence.
- 3.1.23** Control and manage network IP address space, Domain Name System, Network Directory, and messaging services per base and Higher Headquarters direction.
- 3.1.24** C-CS advisor at meetings for facility design, military construction programs and minor construction planning.
- 3.1.25** Implement C-CS projects. Monitor project completion actions. Ensure availability of logistic support. Monitor project exceptions.
- 3.1.26** Attend meetings on base occurring approximately monthly where various aspects of MPC C-CS are discussed.
- 3.1.27** Configuration Management: Support installation and management of hardware and software at the operating system level.

3.1.28 Control and manage network IP address space, Domain Name System, Network Directory, and messaging services per base and Higher Headquarters direction.

3.1.29 Security Management: Follow and enforce national, Department of Defense (DoD), and Air Force security policies and directives both verbal and written reports for non-compliance issues.

3.1.30 Perform proactive security functions to deter, detect, isolate, contain, and recover from information system and network security intrusions.

3.1.31 Identify and characterize incidents, generate incident reports, and investigate suspicious network activity.

3.1.32 Problem Management: Categorize, isolate, and resolve network problems on NIPR, SIPR and JWICS.

3.1.33 Perform fault isolation by validating, isolating, and correcting faults and verifying service restoration with customers.

3.1.34 Process and advocate scheduled and authorized network outages occur around mission needs. Implement service restoration plans, coordinate corrective actions, and submit outage reports in response to unscheduled outages. Develop and implement mitigation strategies to ensure continued service of required C-CS equipment and network resources.

3.1.35 Maintain C-CS equipment inventories, to include tracking locations for accountability purposes.

3.1.36 Process, document, and coordinate resolution of trouble calls from MPC personnel.

3.1.37 Manage remote dial-in communications capabilities and remote distributed print services.

3.1.38 Manage program for cryptology systems and comply with all regulatory requirements

3.1.39 Support the design, maintenance, and update of locally developed, GHOC-Approved, MS (Word/Access/Excel/Project, or other programs as required) based computer database programs and local forms.

3.1.40 SIPR and NIPR account creations and management, updates and deletions. Interface with 548 ISR Group to create JWICS accounts. Including Token management for access to these accounts.

3.1.41 Create and manage MPC personnel rosters related to email distribution lists and other communications systems.

3.1.42 Provide monthly refresher training to MPC personnel on the function and use of necessary mission planning software applications and hardware systems.

4.0 KNOWLEDGE, SKILLS, AND ABILITIES (KSAs): The contractor shall ensure that all employees hired have the required background to perform the duties as defined in the contract, maintain the appropriate security clearance and access to the required installations. The contractor shall ensure that all personnel hired meet the following requirements:

4.1 General Qualifications for all positions

4.1.1 Be a U.S. citizen.

4.1.2 Pass a standard physical examination that includes, at a minimum: medical history, height, weight, and blood

pressure.

4.1.3 All positions required to be able to complete light office lifting defined by moving 20lbs box up a flight of stairs.

4.1.4 Possess a Top Secret/Sensitive Compartmented Information (TS/SCI) and NATO Secret security clearances

4.2 Information Technologist Specific Qualifications: Knowledge of Air Force C-CS technologies with a minimum of five (5) years of experience working with a variety of the C-CS field's concepts, practices and procedures, ground based telecommunications systems, avionics and information system technology, management of program and project implementation actions, and Air Force planning documents and application of these documents to the C-CS systems. This also includes a minimum of four years of experience with:

4.2.1 Asynchronous Transfer Mode (ATM)

4.2.2 Ethernet, local, and wide area networks

4.2.3 UNIX and non-UNIX operating systems

4.2.4 Voice over Internet Protocol technology

4.2.5 Cryptology systems and regulatory requirements

4.2.6 Access to DoD information systems will be required to perform contract duties. The Contractor, at the time of contract award, must ensure contractor personnel possess a valid, current, Security+ CE baseline certification IAW DoD 8570.01-M. Refer to **Section 14.0 - SECURITY INSTRUCTIONS** for further instructions.

5.0 DELIVERABLES: The Contractor shall provide task order deliverable(s) in a format mutually agreed upon by the Government and the Contractor. All deliverables will be reviewed for timeliness, accuracy and format. If a deliverable due date falls on a weekend or holiday, the Contractor shall submit the deliverable on the last work day prior to the due date.

| Schedule | | | |
|------------------------------------|---------------|----------------|--|
| Deliverables | PWS Reference | Deliver To | Due Date |
| ITAMS Computer equipment inventory | 3.1.1 | Admin/Tech Flt | June 1 st or as required by Wing Inspection |

6.1 Monthly Status Report: The contractor will submit by the 5th calendar day of each month (if the 5th falls on a weekend/holiday, it will be due the last workday before the weekend/holiday) a report specifying the manning at each location, indicating any leave and vacancies. Also, the contractor will submit the breakdown of each location including the number of hours worked, and status update on all equipment, operations, and personnel. Financial reports include expenditures for that previous month as billed in Wide Area Workflow, to include monthly charges and travel expenditures.

6.2 Travel Requests and Trip Reports: Prior to official travel, the contractor will submit a travel request to the COR no later than 10 duty days prior to travel. Following official travel, the contractor shall prepare a trip report detailing the purpose of the trip, the locations visited, and any other significant issues that were identified during the travel. The contractor shall provide this trip report to the COR within five (5) days after the completion of travel. Travel reports will also be attached in WAWF during invoicing.

6.3 Key Positions/Personnel: All positions within this requirement designated as 'key' for the overall success

of the task order.

6.4 Quality Control Plan: Develop and maintain a quality control plan in accordance with application DoD and USAF regulations and instructions.

6.5 Service Delivery Summary:

TABLE 2 – SERVICE DELIVERY SUMMARY

| Performance Objective | PWS Paragraph | Performance Threshold |
|---|------------------------|---|
| Provide qualified people at TO start | 3 - 9 | Performance is acceptable when a) qualified personnel are on the job at TO Start unless previously negotiated by the CO and; b) the mission is not impacted due to position vacancies or personnel qualifications |
| Develop and submit all required deliverables | Table 1 - Deliverables | Performance is acceptable when a) 100% of deliverable requirements are met and received on time; and b) Critical information is accurate. |
| Quality of Service (applicable for all TO services provided) | 3 | Not more than 1 validated customer service complaints within each fiscal quarter. |
| Replacement/substitute personnel | 11.7 | Performance is acceptable when: a) Vacancies are filled with qualified personnel within 30 calendar days of vacancy, unless approved in writing or otherwise directed in advance by the CO; and b) There is no mission impact due to position vacancies or unqualified personnel. |
| The COR shall inspect, on a random basis, ten to twenty percent of all PWS items not identified in the Service Summary Table at least monthly for compliance. | | a) No more than one noncompliance is allowed per month with re-performance to be conducted within one day of notification of the discrepancy. b) A mutually acceptable timeframe between the COR, customer, and contractor may be established instead. |

7.0 GOVERNMENT FURNISHED PROPERTY:

7.1 Government Provided Equipment/Office: Host units will provide the following equipment and workspace to contractors at the host unit:

- 7.1.1** All Air Force Mission Support System (AFMSS) and all peripheral system hardware and software
- 7.1.2** Non-secure Internet Protocol (IP) Router Network (NIPRNET) workstations and printers.
- 7.1.3** Secure Internet Protocol (IP) Router Network (SIPRNET) workstations and printers
- 7.1.4** Joint Worldwide Intelligence Communications System (JWICS) workstations and printer
- 7.1.5** Secure workspaces for all required hardware and workstations.

8.0 DATA: The Government has unlimited rights to all deliverables of this task order to include intellectual

property rights. In the performance of this contract, the contractor may have access to data and information proprietary to a government agency or to another government contractor, or of such nature that its dissemination or use, other than as specified in this contract, would be illegal or otherwise adverse to the interests of the government or others. Neither the contractor nor contractor personnel shall divulge or release data or information developed or obtained under performance of this contract, except to authorized government personnel or upon written approval of the Contracting Officer or designated representative. Neither the contractor nor contractor personnel shall use, disclose, or reproduce proprietary information bearing a restrictive legend, other than as specified in the contract.

8.1 Disclosure: Disclosure of information regarding operations and services of the activity to persons not entitled to receive it, or failure to safeguard any classified information that may come to the contractor (or any persons under the contractor's control) in connection with work under this contract, may subject the contractor, contractor's agent, or employees to criminal liability under Title 18, Sections 793 and 798 of the United States Code. Neither the contractor nor the contractor's employees shall disclose or cause to be disseminated, nor information concerning the operations of the activity that could result in, or increase the likelihood of, the possibility of a breach of the activities' security or interrupt the continuity of operations.

8.2 Disputes: The contractor shall direct to the Contracting Officer or designated government representative, all inquiries, comments, or complaints arising from matters observed, experienced, or learned as a result of, or in connection with the performance of this contract, the resolution of which may require the dissemination of official information.

8.3 FOIA Requests: Inquiries received by the contractor for work performed under this contract shall be referred to the Contracting Officer for evaluation under the Freedom of Information Act (FOIA) of 1975, Public Law 93-502, 5 U.S.C.; Section 552. The government FOIA officer shall be responsible for determining whether such requests will be honored.

8.4 Privacy Act: The contractor shall not release any information (including contact lists, photographs, files, public announcements, statements, denials, or confirmations) on any part of the subject matter of this contract, or any phase of any program hereunder, without prior written approval of the Contracting Officer or designated government representative. Any documentation showing individuals' names or other personal information will be controlled and protected. The provisions of the Privacy Act of 1974, Public Law 93-579, 5 U.S.C., Section 552a, shall apply. The Government has unlimited rights to all deliverables of this task order to include intellectual property rights.

9.0 SECURITY

9.1 Compliance: The Contractor and all Contractor personnel shall abide by all AF and local rules, procedures and standards of conduct. A Department of Defense Contract Security Classification Specification (DD Form 254) is required for access to classified material. The Contractor shall also perform in accordance with the Compliance with National Industrial Security Program Operating Manual (NISPOM--DoD 5220.22M).

9.2 Visitor Group Security Agreement (VGSA): The contractor shall enter into a long term visitor group security agreement with the host base Information Protection Office if contract performance is on base. This agreement shall outline how the contractor integrates security requirements for contract operations with the Air Force to ensure effective and economical operation on the installation. The agreement should address:

9.3 Security support provided by the Air Force to the contractor to include storage containers for classified information/material, use of base destruction facilities, classified reproduction facilities, use of base classified mail services, security badging, base visitor control, investigation of security incidents, base traffic regulations, the use of security forms, and conducting inspections required by DOD 5220.22- R, Industrial Security Regulation, and Air Force Instruction 16-1406, Industrial Security Program Management.

9.4 Security support requiring joint Air Force and contractor coordination includes packaging classified information, mailing and receiving classified materials, implementing emergency procedures for protection of classified information, security checks, and internal security controls for protection of classified material and high value pilfer-able property.

9.5 On base, the long term visitor group security agreement may take the place of a Standard Practice Procedure.

9.6 Security Clearance: The contractor must possess or obtain a facility security clearance at the level of Top Secret prior to performing contract work. In addition to a Top Secret security clearance, some positions under this PWS will require access to classified NATO information. The Defense Industrial Security Clearance Office (DISCO) assumes costs and conducts security investigations for Top Secret, Secret, and Confidential facility security clearances. The contractor shall request security clearances (Submit Clearance Paperwork through DISCO to the Office of Personnel Management) for personnel requiring access to classified information within 15 days after receiving a facility clearance or, if the contractor is already cleared, within 15 days after contract award. Due to costs involved with security investigations, requests for contractor security clearances shall be kept to an absolute minimum necessary to perform contract requirements. Contractor personnel shall have appropriate clearances prior to commencing work on any T/O unless otherwise approved in writing by the CO. The Contractor shall also complete visit requests for each individual that will be performing work on a T/O in the Defense Security Service (DSS) Joint Personnel Adjudication System (JPAS) prior to performance start unless otherwise approved in writing by the CO. The Prime Contractor shall ensure that any teaming partners or subcontractors have the appropriate clearances prior to beginning performance. The Prime Contractor is required to accomplish a separate DD Form 254 for 9 RW/IP for each subcontractor or teaming partner.

| TABLE 4 – REQUIRED SECURITY CLEARANCES | | |
|---|------------------------------------|-----------------------------|
| Task | Clearance Required | Place of Performance |
| 3 – 9 | Top Secret // SCI, and NATO Secret | Beale AFB, CA |
| 3 – 9 | Top Secret//SCI, and NATO Secret | Grand Forks AFB, ND |

9.7 Clearance Documentation: Within 10 calendar days of contract award, the Contractor shall provide the Primary COR a list with the names, location of performance and clearance requirements of all company employees assigned to this effort.

9.8.1 Name, address, and telephone number of company representatives.

9.8.2 The contract number and contracting agency.

9.8.3 The highest level of classified information which contractor employees require access to.

9.8.4 The location(s) of contract performance.

9.8.5 The date contract performance begins.

9.9 Listing of Employees. The contractor shall maintain a current listing of employees. The list shall include the employee's name, social security number and level of security clearance. The list shall be validated and signed by the company Facility Security Officer (FSO) and provided to the Sponsoring Agencies Security Manager. An updated listing shall be provided when an employee's status or information changes, and upon request by CO/COR.

9.10 Security Program Training. The contractor will coordinate with the unit security manager on initial and all annual security training requirements for all contractors who work in controlled/restricted areas.

9.11 Pass-and-Identification Items. The contractor shall ensure the pass and identification items required for contract performance are obtained for employees and non-government owned vehicles.

9.12 Retrieving Identification Media. The contractor shall retrieve all identification media, including vehicle passes from employees who depart for any reason before the contract expires; e.g. terminated for cause, retirement, etc.

9.13 Traffic Laws. The contractor and its employees shall comply with base traffic regulations.

9.14 Weapons, Firearms, and Ammunition. Contractor employees are prohibited from possessing weapons,

firearms, or ammunition, on themselves or within their contractor-owned vehicle or privately- owned vehicle while on all CONUS government installations. Firearm policies while OCONUS will be IAW local installation authorities.

9.15 For Official Use Only (FOUO). The contractor shall comply with DoD 5400.7-R, Chapter 4, DoD Freedom of Information Act (FOIA) Program, requirements. This regulation sets policy and procedures for the disclosure of records to the public and for marking, handling, transmitting, and safeguarding FOUO material.

9.16 Reporting Requirements. Contractor personnel shall report to an appropriate authority any information or circumstances of which they are aware may pose a threat to the security of DOD personnel, contractor personnel, resources, and classified or unclassified defense information. Contractor employees shall be briefed by their immediate supervisor upon initial on-base assignment.

9.17 Physical Security. The contractor shall be responsible for safeguarding all government property and controlled forms provided for contractor use. At the end of each work period, all government facilities, equipment, and materials shall be secured.

9.18 Controlled/Restricted Areas. The contractor shall implement local base procedures for entry to Air Force controlled/restricted areas where contractor personnel will work. An AF Form 2586, Unescorted Entry Authorization Certificate, must be completed and signed by the sponsoring agencies Security Manager before a Restricted Area Badge will be issued. Contractor employees must have a favorably completed National Agency Check plus written Inquiries (NACI) investigation before receiving a Restricted Area Badge. Interim access can be granted IAW AFI 31-501, Personnel Security Program Management

9.19 Key Control/Access Badge Control. The contractor shall establish and implement methods of making sure all keys/badges issued to the contractor by the Government are not lost or misplaced and are not used by unauthorized persons. The contractor shall not duplicate any keys issued by the government.

9.20 Lost Keys. The contractor shall immediately report to the Quality Assurance Evaluator (QAE) or Program Manager any occurrences of lost or duplicated keys. In the event keys, other than master keys, are lost or duplicated, the contractor may be required, upon written direction of the contracting officer, to re-key or replace the affected lock or locks without cost to the government. The government may, however, at its option, replace the affected lock or locks or perform re-keying and deduct the cost of such from the monthly payment due the contractor. In the event a master key is lost or duplicated, all locks and keys for that system shall be replaced by the government and the total cost deducted from the monthly payment due the contractor.

9.21 Prohibited Use. The contractor shall prohibit the use of keys, issued by the government, by any persons other than the contractor's employees and the opening of locked areas by contractor employees to permit entrance of persons other than contractor employees engaged in performance of contract work requirements in those areas.

9.22 Lock Combinations. The contractor shall control access to all government provided lock combinations to preclude unauthorized entry. The contractor is not authorized to record lock combinations without written approval by the government Program Manager. Records with written combinations to authorized secure storage containers, secure storage rooms, or certified vaults, shall be marked and safeguarded at the highest classification level as the classified material maintained inside the approved containers.

9.23 Automatic Data Processing Equipment (ADPE). The Contractor shall establish and implement procedures to ensure all ADPE (also known as ITAMS), to include laptops and other data processing devices, issued to the Contractor by the Government are not lost or misplaced, are not used by unauthorized persons or are not subject to unauthorized external devices. The Contractor shall immediately report to the CO or PM any occurrences of lost ADPE within two (2) hours of discovery of occurrence. In the event that ADPE is lost, the Contractor may be required, upon written direction of the CO, to replace the equipment at no additional cost to the Government. The Government may replace the equipment and deduct the cost of such from the monthly payment due the Contractor.

9.24 Communications Security (COMSEC). Contractors may require access to COMSEC information. The DD FM 254 will give further instructions on safeguarding and managing COMSEC material.

10.0 TRANSITION PLAN:

10.1 Transition In. The transition period will be fifteen (15) calendar days for contractor personnel. This allows 15 days for Contractor key personnel to process and obtain required ID/CAC cards, computer system access requests, travel and receive workplace and task orientation to ensure the entire team is in-place for period of performance start, in order to fulfill this TO. Any remaining days of the transition period can be spent receiving briefings on specific duties and responsibilities Contractor personnel will be expected to accomplish to fulfill this TO.

10.2 Transition Out. Prior to the end of the TO period of performance, the incumbent Contractor shall support a fifteen (15) business day (120 hours) transition period with in-coming personnel supporting the installations in accordance with **Table 2 – SERVICE DELIVERY SUMMARY**. During this period, all programs, information, data, etc. will be passed from the incumbent Contractor to the incoming Contractor so that there is no break in Customer or mission support.

11.0 ADMINISTRATION CONSIDERATIONS:

11.1 Performance Schedule: The Contractor shall perform this task from **01 April 2018 through 31 March 2021** ('base year') in accordance with **Table 5 – PERFORMANCE SCHEDULE**.

TABLE 5 – PERFORMANCE SCHEDULE

| Period Type | Period Dates |
|-------------|------------------------------|
| Base Year | 1 April 2018 – 31 March 2019 |
| Option 1 | 1 April 2019 – 31 March 2020 |
| Option 2 | 1 April 2020 – 31 March 2021 |
| Option 3 | 1 April 2022 – 31 March 2022 |

11.2 Place of Performance: The Contractor shall be located in accordance with **Table 6 – PHYSICAL LOCATIONS** to perform and accomplish tasks identified in this task order.

TABLE 6 – PHYSICAL LOCATIONS

| Task | Number of FTEs | Location |
|--------------------------|----------------|--|
| Information Technologist | 3 | Physical Location: Beale AFB, CA |
| Information Technologist | 3 | Grand Forks AFB, ND |

11.3 Off-site work: Off-site work shall not be permitted for this task order.

11.4 Duty Hours: All tasks are scheduled for 8 hour shifts during normal business hours as defined by squadron leadership. Federal Holidays will be observed by all positions.

11.5 Base Shutdown/Inclement Weather: The Contractor will follow guidance of the installation containing their place of performance to determine reporting schedules whether due to a base closure or inclement weather. Status of base shutdown/inclement weather shall be provided by the installation Command Post or alternative agency per installation guidance.

11.6 Kickoff Meeting: Contractor shall attend a kick off meeting specific to the TO requirement with the COR and the Administrative CO within fifteen(15) days of contract award The Contractor shall provide concurrence with the date, time and location for the meeting via email notification to the COR at least three (3) business days prior to the scheduled meeting.

11.7 Vacancies: In the event of an illness, death or any circumstance that creates a vacancy towards contract performance, the position will be filled with qualified personnel within 30 calendar days of the vacancy, unless approved

in writing or otherwise directed in advance by the CO. The Contractor is responsible for maintaining a stable workforce and providing qualified personnel to fulfill mission requirements.

11.8 Contractor Inventory: In accordance with Section 8108 of Public Law 112-10 of the Department of Defense and Full-Year Continuing Appropriations Action, 2011.

11.9 Contractor Manpower Reporting: The Contractor shall report ALL labor hours required for performance of services provided under this task order via the secure Contractor Manpower Reporting Application (CMRA) data collection site. The Contractor is required to completely fill in all required data fields at: <http://www.ecmra.mil>. Reporting inputs shall be for the labor executed during the period of performance for each Government fiscal year (FY), which runs 1 October through 30 September. While inputs may be reported anytime during the FY, all data shall be reported not later than 31 October of each calendar year. The Contractor may direct questions to the CMRA help desk. The prime Contractor is responsible to ensure all subcontractor data is reported.

11.10 Uses and Safeguarding of Information: Information from the secure web site is considered to be proprietary in nature when the contractor number and the Contractor identity are associated with the direct labor hours and direct labor dollars. At no time will any data be released to the public with the Contractor name and contract number associated with the data.

11.11 User Manual: Data for the AF services requirements must be input at the AF CMRA link. However, user manuals for Government personnel and Contractors are available at the U.S. Army CMRA link at <http://www.ecmra.mil>.

11.12 Subcontractor Input in CMRA: Prime Contractors are responsible to ensure all subcontractor data is reported. Subcontractors will not be able to enter any data into CMRA, but will enter their information into a Bulk Loader spread sheet available from the AF CMRA helpdesk. Subcontractor shall fill in columns A-C then return it to the AF CMRA helpdesk after it's completed and a technician team will enter the information into CMRA.

11.13 On-Call/Overtime Support: In times of increased operations or if additional work is required of the contractor to complete a task, on-call support or overtime may be requested. On-call support/overtime may be conducted through phone or by having additional contractor support at the cognizant government site. If support is required at the cognizant government site, the contractor will arrive within two hours of the request or at the time agreed upon by the COR and contractor). All support requests will be placed by the COR orally or in writing and will be assigned a call number. For all work within On-Call Support/overtime will paid at a rate of 1.5 times the requested position's base rate.