****

**Defense Systems Group**

**COMSEC Custodian Plan**

**OCONUS Projected COMSEC Custodian Opportunities**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Location** | **COCOM** | **Staffing**  **(Projected)** | **Incumbent** | **Est. Annual Value** | **POP**  **Years** | **COMMENT** |
| **Sweden** | **EUCOM** | **2** | **ManTech** | **280K currently.**  **Should we recompete $400-500K** | **3** | **All countries are in the NATO Partnership For Peace program, but are typically a militarily non-aligned nation** |
| **Switzerland** | **EUCOM** | **2** | **None** | **$500K** | **3** |
| **Ireland** | **EUCOM** | **2** | **None** | **$500K** | **3** |
| **Finland** | **EUCOM** | **2** | **None** | **$500K** | **3** |
| **Austria** | **EUCOM** | **2** | **None** | **$500K** | **3** |
| **Malta** | **EUCOM** | **2** | **None** | **$400K** | **3** |
| **Qatar** | **CENTCOM** | **2** | **None** | **$700K** | **5** |  |
| **Kuwait** | **CENTCOM** | **2** | **None** | **$700K** | **5** |  |
| **Jordan** | **CENTCOM** | **2** | **TBD** | **$700K** | **3** |  |
| **Israel** | **EUCOM** | **2** | **Exercet Comm** | **$700K** | **3** |  |
| **Saudi Arabia** | **CENTCOM** | **2** | **None** | **$700K** | **5** |  |
| **United Arab Emirates** | **CENTCOM** | **2** | **None** | **$600K** | **5** |  |
| **Oman** | **CENTCOM** | **2** | **None** | **$600K** | **5** |  |
| **Pakistan** | **CENTCOM** | **2** | **None** | **$700K** | **3** |  |
| **Various Africa Nations** | **AFRICOM** | **2 per Country** | **None** | **$500K** | **3** | **Nothing close to concrete, but did receive positive reaction when subject was brought up.** |
| **Estimated annual revenue**  \* Does not include Africa. | | | | **$8.2M\*** |  |  |

**Table 1**

**Description of Services**

* The contractor personnel shall serve as the primary and alternate U.S. COMSEC manager.
* The contractor personnel, identified as U.S. COMSEC custodians, must have a current final U.S. security clearance of SECRET.
* Contractor personnel shall perform central receiving, temporary storage, and transfer services for DOD-provided COMSEC equipment, COMSEC documents, keying and other materials from U.S. COMSEC National Distribution Authorities (i.e. National Security Agency (NSA) or where the material/equipment will be received from) to the Host Nation Armed Forces or upon return from the Host Nation Armed Forces to the appropriate U.S. National Distribution Authorities (NDA).
* Contractor personnel shall report to COCOM/CCJ3-CI for coordination and instructions on all issues concerning COMSEC equipment, keys/keymat, and associated programs released to the Host Nation Armed Forces.
* Contractor personnel shall provide the following U.S. COMSEC managerial duties:
  + Protect COMSEC material and limit access to individuals without a valid need-to-know and clearance.
  + Receive, receipt for, and ensure the safeguarding and accounting of all COMSEC material issued to the COMSEC account, and when applicable, produced within the element.
  + Maintain COMSEC accounting and related records as outlined in NSA/Central Security Service (CSS) Policy Manual 3-16, "Control of Communications Security (COMSEC) Material", dated August 2005.
  + Conduct an inventory semiannually by physically sighting all COMSEC material charged to the account and reconcile this inventory with the Central Office of Record (COR). The conduct of an inventory may also be directed by the COR. An inventory shall also be accomplished upon appointment of a new U.S. COMSEC Manager. All the above inventories shall be conducted as outlined in NSA/CSS Policy Manual 3-16, or the applicable service regulations.
  + Perform routine destruction of COMSEC material when required, or effect other disposition of material as directed by the COR or Controlling Authority. The COMSEC manager shall establish Emergency and Precautionary Destructions plans as part of the account's Emergency Action Plan.
  + Submit transfer, destruction, and possession reports, when required, to the NSA Central Office of Record.
  + To ensure the integrity of COMSEC material (i.e. key or equipment), inspection of protective technologies shall occur prior to issuing of material to authorized Host Nation Armed Forces personnel and after return from the Host Nation Armed Forces personnel.
  + Ensure the prompt and accurate entry of all amendments to COMSEC publications held by the account.
  + Ensure that required page checks (as specified in NSA/CSS Policy Manual 3-16 instructions) are accomplished on all keying material and publications when they are received, returned from hand receipt, transferred, destroyed, when a change of U.S. COMSEC Manager occurs, and when posting amendments which include replacement pages to ensure completeness of each publication.
  + Ensure that all accountable U.S. COMSEC material shipped outside of the account’s organization is packaged and shipped as specified in NSA/CSS Policy Manual 3-16 instructions. Ensure that all material received is inspected for evidence of tampering. If suspected physical incident is found, submit a report immediately, in accordance with NSA/CSS Policy Manual 3-16 instructions.
  + Shall be aware of the location of all accountable COMSEC material stored within the COMSEC account's facility and shall maintain continual accountability for all COMSEC materials issued by the COMSEC account to the Host Nation Armed Forces.
  + Establish procedures to ensure strict control of each item of keying material whenever operational requirements necessitate that material be turned over from one shift to another or from one individual to another. All the above procedures shall be in accordance with NSA/CSS Policy Manual 3-16 instructions, or the applicable service regulation.
  + Ensure that appropriate COMSEC material is readily available to properly cleared and authorized individuals whose duties require its use. If the material is classified, verify that the individuals are cleared to the level of the material. Issue material to users by means of a hand receipt, as provided for in NSA/CSS Policy Manual 3-16 instructions, or the applicable service regulation, and advise recipients of their responsibility for safeguarding the material until it is returned to the manager.
  + Report immediately, to the element commander or chief, any known or suspected incidents of a COMSEC incident, personnel incident, or physical incident, and submit a report in accordance with the procedures outlined in NSA/CSS Policy Manual 3-16 instructions. COCOM/CCJ3-CI will be informed on incidents and info copied on all reports.
  + Train Host Nation Defense Forces personnel in the proper custodianship, safeguarding and operation of DOD-provided COMSEC equipment, keying and other materials, to include installation of equipment, loading and zeroing equipment, trouble-shooting (when necessary), and emergency destruction procedures, in order to satisfy requirements for secure interoperability.
  + Ensure adequate quantities of key material are maintained and replacement material is ordered in a timely manner to avoid any breaks in support or service.
  + Immediately notify COCOM/CCJ3-CI if the possession of key material is not attained within one month of the designated re-key date, or if there are issues that arise during re-key.
  + Routinely check Secure Local Area Network (SLAN) emails for traffic and respond to and take appropriate action as required from the emails.
  + COMSEC Custodians shall submit a monthly report outlining any activity/findings/corrective actions within 5 calendar days after the completion of the month being reported. The purpose of these reports is to provide AFSAC an oversight of the custodial duties within country. Contractor format is acceptable.

**Job Descriptions/Experience**

The positions of COMSEC Custodian will be:

* Thoroughly familiar with the proper handling and safeguarding of Communications Security materials and equipment.
* Thoroughly familiar with Civil codes.
* Be able to research and understand National Security Agency (NSA) Information Assurance (IA)/COMSEC regulations and USCENTCOM operational directives.
* Thoroughly familiar with Operational Security strategies and methods.
* Familiar with the publications and directives that will be used to support daily and special operations.
* Able to develop, prepare, and deliver COMSEC training to the Host Nation hand receipt/COMSEC responsible officers.
* Able to articulate concerns, verbally and in writing, clearly to senior U.S. and Host Nation leadership.
* Possess the ability to work independently without technical guidance.
* experienced in theory of all aspects of the COMSEC Equipment/Systems.
* Possess a high degree of tact, diplomacy and the ability to work and cooperate harmoniously with Host Nation military and civilian personnel.
* Able to obtain an International drivers license, or driving privileges in the host country
* In possession of a final US SECRET level clearance

**Proposal Description**

General

This is an outline for an unsolicited proposal to support a consolidated COMSEC Custodian program under the Headquarters Air Force Security Assistance Center (AFSAC) at Wright-Patterson AFB, Ohio.

Background

In August 2007 AFSAC advertized through the Wright Patterson AFB contracting website PIXS, a Sources Sought for a consolidated program. However, we have had no indication that AFSAC continued the market research. ManTech believes that this consolidation approach for providing the service is more cost efficient for the Government and for the end user, as well as presenting operational benefits through cohesion, common standards and contract synchronization.

Technical Approach

Our approach will follow the stringent processes required in all the appropriate COMSEC manuals and publications, and bolstered through our Standard Operating Procedures (SOP) for new COMSEC account start-ups and our SOP for training Foreign Armed Forces in the use, management, and accountability of US COMSEC equipment and material.

Upon contract award, ManTech will submit the Primary COMSEC Custodian (PCC) and Alternate COMSEC Custodian (ACC) for NSA approval IAW NSA/CSS Policy Manual 3-16. Upon NSA approval of the PCC and ACC, the PCC will initiate the process through NSA (and in coordination with the COCOM/J6) to establish a COMSEC account for the Host Nation Armed Forces. ManTech’s COMSEC Custodians will then immediately assume full responsibility for the administration and management of the COMSEC account by conducting receipt, custody, issue, safeguarding, accounting, and when necessary, destruction of COMSEC material for the Host Nation Forces. The custodians will maintain current and up-to-date electronic and paper records IAW applicable records management policies and regulations, and will submit all required accounting reports, and will be thoroughly familiar with the procedures for handling COMSEC material. The PCC will be designated as the principle and primary local ManTech representative and account supervisor. The PCC will be the local senior custodian responsible for the technical and administrative operation and maintenance of the COMSEC Account. The PCC will have a final U.S. SECRET clearance in order to be authorized access to COMSEC material IAW National Industrial Security Program Operating Manual (NISPOM) requirements, and will also be a senior level technician that has the skills equivalent to a USAF 3C071 (AFSC), Craftsman or Advanced Level Communications – Computer Systems Operations technician, or has held a similar position with similar technical training and experience within DOD.

The PCC will develop a formal local training program, based on our Training SOP, for customers/hand receipt holders that will constitute initial and recurring training. The training program will ensure that Host nation Forces personnel are aware of basic policy and procedures, remain current to policy and procedure changes, and are compliant with all applicable directives when handling COMSEC material. The training program will be part of the account’s External Standard Operating Procedures and will encompass the following:

* Receipt
* Handling
* Safeguarding (including personnel controls and physical barriers)
* Inventorying
* Incident Reporting
* Emergency Action Plan (EAP) Requirements
* Operational Activities
  + Installation
  + Loading and zeroizing
  + Troubleshooting
* Destruction

The Alternate COMSEC Custodian will be the Technical Advisor to the host country for C3I systems, and will coordinate with the host country COMSEC officials to provide technical assistance and training to the host country hand receipt holders and users, and will ensure that EAPs are developed and rehearsed.

The Alternate COMSEC Custodian will also administer and manage the formal training plan that includes at a minimum the following:

* Handling
* Accountability, and safeguarding of COMSEC material
* Security briefings
* What constitutes a COMSEC security incident; and incident reporting requirements.

Additionally, the Alternate COMSEC Custodian will be the point-of-contact for COMSEC inter-operability between U.S. Government and the host country Government, and will ensure a seamless interoperability by testing communications links. Another responsibility of this individual will be to monitor COMSEC links to ensure an unbroken secure communications service. The Alternate COMSEC Custodian will coordinate with U.S. and the host country security and military staffs to schedule and plan C3I exercises between the host country and U.S. Military units, and will also review/evaluate exercise results and make any recommendations for improvements to the U.S. and the host country systems.

Staffing

PRIMARY AND ALTERNATE CUSTODIANS:

Based on previous COMSEC Custodian solicitation, MANTECH offers a scalable and flexible management and account staffing solution based on the estimated or specified work loads for each task order. The baseline staffing for each task order is two (2ea) qualified COMSEC Custodians to perform the duties of Primary and Alternate custodians. Additional staffing may be implemented and executed for task orders when the identified workload supports more personnel. Surge requirements of 30 days or less will be supported with existing personnel “borrowed” from other TOs. Surge requirements for 31 days to 90 days will be supported from a contingency pool of qualified personnel in CONUS and Europe. Based on European labor and tax laws, surge/contingency/emergency staffing for 90+ days will be identified as early as possible and coordinated separately.

PROGRAM MANAGEMENT:

Our established Program Management Office in Mannheim, Germany will perform the required program management functions and duties to support the European, African and SWA task orders. This location affords the best operational support and interface with the local customers and the ManTech personnel by being geocentric to the areas of operation. Coordination with the local customers and the responsiveness of the ManTech Management will be almost real-time in contrast to the difficulty of coordination and interface from a CONUS based location. ManTech offers to support the COMSEC task orders with the current management staff on an hourly allocation of 250 hours per TO. When the task orders reach activation of four accounts, ManTech will support with a full-time, exclusive, project manager.

QUALITY CONTROL:

Quality Control (QC) will be performed by our fully qualified Facility Security Officer staff from our corporate headquarters in Chantilly, Va., and will be under the management and control of the Facility Security Officer. Quality Control will be accomplished by announced inspections and audits at the COMSEC Accounts to ensure compliance with all applicable NSA, COCOM, and NISPOM regulations and policies. ManTech will use ISO 9000 inspection procedures to bolster our performance with continuous improvement, and verification documentation. Resultant Quality Control reports and follow-ups will be forwarded the AFSAC Contract Officer.

Our Organization Chart is presented below.

**Program Manager**

Part-time for up to 3 accounts

Full-time at 4 accounts

**Quality Control**

Part-time with under 20 accounts

**COMSEC**

**Account**

**1**

**COMSEC**

**Account**

**2**

**COMSEC**

**Account**

**1**

**COMSEC**

**Account**

**3**

**COMSEC**

**Account**

**4**

**COMSEC**

**Account**

**XX**

Phase-In

ManTech proposes a well-planned and common sense Phase-In concept and approach based on best industry practices that reduce risks to performance, and capitalizes on our presence and experience in both Europe and South West Asia. We will utilize our SOP that we have developed for starting a COMSEC account in a foreign nation. This SOP contains procedures based on lessons learned from our experiences in Europe and SWA. To that end we place the following assumptions:

* In Europe, the COMSEC Custodians will require work and/or residency permits before entering the country to work. This documentation can take up to 90 days to be processed and approved.
* In SWA, our employees must be sponsored for work and/or residency permits and that will be accomplished by our area sponsorship partner. This normally takes just a few days.

After Task Order award and before the employees arrive at the work site, ManTech will deploy an advance team to the area to coordinate the primary employees’ logistical support, and initial customer interface. This coordination will focus on the coordination with in-country customers for office space, set-up of office area, and oriented to the operational area. The intent is to have the workcenter established and functional when the custodians arrive to mitigate the transition period and have a functional operation as soon as possible.

Phase-In Timetable

One of the strengths of our COMSEC Custodian program is our understanding of a realistic timetable to perform the series of activities necessary for a successful transition/start-up of the COMSEC Custodians account in a foreign country. This is based on our experience gained in phasing-in other contracts over the past 20 years; extensive experience in Outside the Continental United States (OCONUS) contract support; and our Phase-In Team’s knowledge of COMSEC duties, locations, and requirements. Our Phase-In timetable below provides the event milestones and personnel Phase-In schedules. We will coordinate with the customer to identify mission-essential systems and establish key milestones on an integrated Phase-In schedule. We will communicate, collaborate and keep the Government fully informed of the Phase-In status and progress, including activities where interaction is not required.

| **Item** | **Start** | **Duration**  **(Days)** | **Complete** | **Notes** |
| --- | --- | --- | --- | --- |
| Pre-Award Activities |  | 20 |  |  |
| Corporate Preparation  * Ops Support/Logistics Plans * NSA Packages (Draft) * Initial Deliverables (Draft) |  | 20 |  | Readiness established prior to award; to be activated at contract award. |
| **Post Contract Award (CA)** | **CA** | **30** | **30 days after award** | Phase-In |
| Start-up coordination, contact, and integration with POCs at COCOM J6 and US Embassy | 5 days after award | 5 | 10 DAYS AFTER AWARD | ManTech establishes formal interfacing contacts with contractual, performance, and participating POCs. |
| Submit COMSEC Custodian Appointment letters to NSA for approval. | 5 DAYS AFTER AWARD | 5 | 6 DAYS AFTER AWARD | Final approval packages forwarded to NSA. Government has minimum of 30 days for reply |
| ManTech advanced project team deployed to location | 7 DAYS AFTER AWARD | 15 | 22 DAYS AFTER AWARD | Coordinate in-country customer requirements; set-up office space; operational area orientation; and employee processing and orientation |
| COMSEC Custodians travel to location | 29 DAYS AFTER AWARD | 1 | 30 DAYS AFTER AWARD | Deployment contingent upon receipt of approved appointment from NSA. |
| ManTech Program Manager – Customer IPR/Phase-In Status updates | 5 DAYS AFTER AWARD | Every 10 Days | N/A | Weekly progress status review and coordination. |
| Start of Performance | 30 DAYS AFTER AWARD |  |  | Contingent on receipt of NSA approval of custodian appointment letters. |
| Initiate inventory custody transfers including COMSEC hand receipts | 30 DAYS AFTER AWARD |  |  | Inventory COMSEC material and equipment. Establish COMSEC data base for COMSEC hand receipts and issue as appropriate. |
| Custodians initiate direct contact and coordination with customers | 31 DAYS AFTER AWARD | 5 | 36 DAYS AFTER AWARD | Contact initiated during Phase to be continued throughout contract performance period |
| Conduct site visits as appropriate | 31 DAYS AFTER AWARD | TBD | TBD | Develop and Initiate planning, coordination and master schedule during Phase-In |
| Develop, coordinate and deliver initial contract deliverables | 35 DAYS AFTER AWARD | 10 | 45 DAYS AFTER AWARD |  |