DEPARTMENT OF THE AIR FORCE

PERFORMANCE WORK STATEMENT (PWS)

PROJECT:

COMMUNICATION SECURITY (COMSEC) SERVICES

FOR

Colombian Joint Force

(FMS CASE CO-D-GAK)

Solicitation number FA830726RB033

Date: May 28, 2026
No. of Pages: 22

TABLE OF CONTENTS

1.0 DESCRIPTION OF SERVICES

1.1 Introduction
1.2 Support
1.3 Overview of Services
1.4 Required Training
1.5 Functional Requirements
1.6 Work Situation
1.7 Travel Requirements
1.8 Operations Security (OPSEC)/Controlled Unclassified Information (CUI)
1.9 Mobilization/Demobilization

2.0 SERVICES SUMMARY (SS)

2.1 Full-time employee Equivalent Reporting
2.2 Service Delivery Summary

3.0 GENERAL INFORMATION

3.1 Management and Administration
3.2 Phase in/out Plan
3.3 Policy
3.4 COMSEC Account Manager Identification
3.5 Risk Mitigation Plan
3.6 Personnel Management and Training

4.0 EVACUATION/DECLARATION OF EMERGENCY

4.1 Evacuations
4.2 Declaration of Emergency

5.0 REGULATORY DOCUMENTS

6.0 COMSEC PUBLICATIONS

7.0 ACRONYMS

DESCRIPTION OF SERVICES

1.1 Introduction. Pursuant to the Communications and Information Security Memorandum of Agreement (CISMOA), between the United States Department of Defense and Colombian Joint Staff, the contractor "who is referred as the incumbent" shall provide support for Communications Security (COMSEC) material and equipment. This effort is done via Foreign Military Sales (FMS) to support various secure coalition interoperability programs between the United States and Colombia.

1.2 Support. The contractor shall provide one (1) primary and one (1) alternate COMSEC Account Manager who are (Bilingual in Spanish and English) in support of various FMS interoperability programs between the U.S. and Colombia. The COMSEC Account Manager will maintain COMSEC equipment facilities. The place of performance is located at Bogota, Colombia, but may travel to other locations/sites. COMSEC Account Managers must be proficient in Spanish (ILR 4) and English. https://www.govtilr.org/Skills/ILRscale2.htm

1.3 Overview of Services. This contract provides COMSEC and C5ISR Services support for Colombian Joint Staff through FMS case CO-D-GAK COMSEC Custodian services shall be in support of DoD provided COMSEC equipment and material released to the Colombian Joint Staff in support of the United States Southern Command (USSOUTHCOM). COMSEC Account Manager shall support secure interoperability programs that interface with multiple agencies to include, but not limited to, the U.S. Embassy – Bogota Colombia, Security Corporation Office (SCO), the National Security Agency (NSA), USSOUTHCOM, the Defense Security Cooperation Agency (DSCA), as well as other agencies/offices as deemed necessary. COMSEC Managers shall perform central receiving, temporary storage, and transfer services for U.S. DoD-provided COMSEC equipment and keying and other materials; perform support services for or related to U.S. DoD-provided COMSEC equipment and keying and other materials; and/or train Colombian Military personnel in the proper custodianship, safeguarding, and operation of U.S. DoD-provided COMSEC equipment and keying and other materials from U.S. COMSEC National Distribution Authorities (i.e. NSA, or where the material/equipment will be received from) to/from the Colombian Joint Staff to the appropriate U.S. National Distribution Authorities (NDA). COMSEC Account Manager shall report to USSOUTHCOM J6-C2IP and/or J6-C2IP for coordination and instructions on all issues concerning COMSEC equipment/keying material, and associated programs released to Colombia Joint Staff. Additionally, contractor personnel shall coordinate any cryptographic key material and equipment issues with USSOUTHCOM J6-C2IP and/or J6-OC. The contractor Program Manager shall consist of program oversight, such as employee liaison and supervision, administration, monthly status reporting, Operations Security (OPSEC), budget and expense monitoring, and quality control.

1.4 Required Training: COMSEC Account Manager shall have the following training. All future training requirements will be at the expense of the incumbent contractor.

1.4.1 Maintain CompTIA Security+ or higher certification as outlined on 1.5.3.4
1.4.2 Maintain at least one COMSEC Account Manager to be General Services Administration (GSA) lock/safe technician as outlined on 1.5.1.9

1.4.3 Maintain at least one COMSEC Account Manager needs to have ViaSat Network Management Software High Assurance Internet Protocol Encryptors (VINES/HAIPE) training as outlined in 1.5.3.17

1.5 Functional Requirements. The Services shall provide the following duties:

1.5.1 COMSEC Account Manager. The contractor shall manage the U.S./Colombia FMS COMSEC account in accordance with U.S. Government (USG) policy as outlined in new CJCSI 6510.06D, Security Directive 1, High Assurance Cryptographic Integration Assessment (HACIA) and NSA CSS Policy Manual No. 3-16. (Contractor should check for updates to these guidelines to ensure compliance with most recent information.). The COMSEC Account Manager shall perform duties related to receipt, custody, issue/distribution, safeguarding, accounting, COMSEC equipment familiarization and destruction of classified and non-classified USG provided COMSEC material and equipment. The COMSEC Account Manager shall be responsible for the maintenance to include software upgrades (when applicable and available in support of emergency requirements), maintaining up-to-date records, the submission of all required accounting reports, and be thoroughly familiar with the procedures for handling COMSEC material. In fulfilling these responsibilities, the COMSEC Account Manager shall perform the following duties:

1.5.1.1 The COMSEC Account Manager shall protect COMSEC material and deny access to individuals without a valid security clearance and a valid need-to-know and verify the identification, clearance and need-to-know of any individual requesting access to the records and/or material associated with the COMSEC account.

1.5.1.2 The COMSEC Account Manager shall identify new COMSEC requirements or modifications to existing COMSEC material to be serviced by the COMSEC account. The contractor shall take prompt action to make updates to the COMSEC account, as necessary, to ensure the account accurately reflects all current COMSEC material.

1.5.1.3 The COMSEC Account Manager shall receive receipt for and ensure the safeguarding and accounting of all COMSEC material shipped. The shipping methods can include, but not limited to, U.S. Diplomatic Courier Service (DCS), Freight Forwarder (FF), Pilot Pickup.

1.5.1.4 The COMSEC Account Manager shall maintain COMSEC accounting and related records as outlined with applicable USG COMSEC Guidance, new CJCSI 6510.06D, Security Directive 1, High Assurance Cryptographic Integration Assessment (HACIA) and NSA CSS Policy Manual 3-16.

1.5.1.5 The COMSEC Account Manager shall conduct an inventory semi-annually and upon appointment of a new Primary COMSEC Account Manager, by physically sighting all COMSEC material issued to the COMSEC account and reconcile this inventory with the Central Office of Record (NSA COR) as mandated in NSA CSS Policy Manual 3-16. The Primary COMSEC Account Manager can also use the COMSEC Responsible Officer (CRO) to assist in the inventory who are outside a 25-mile radius of the Primary for the semi-annual inventory.

1.5.1.6 The COMSEC Account Manager shall perform routine destruction of COMSEC material when required, or effect other disposition of material as directed by the Central Records Office (NSA COR) or Controlling Authority.

1.5.1.7 To ensure the integrity of COMSEC material (e.g. key or equipment); the COMSEC Account Manager shall inspect the implemented protective technologies upon initial receipt, during each inventory and prior to issuing/return of material to authorized Colombian Joint Force personnel.

1.5.1.8 The COMSEC Account Manager shall ensure the prompt and accurate entry of all amendments to COMSEC publications held by the account.

1.5.1.9 Provide technical support to include troubleshooting, and replacement, of GSA locks when necessary for any/all GSA security containers used by the Partner Nation for the purposes of COMSEC material storage. COMSEC Account Manager shall be thoroughly familiar with the proper handling and safeguarding of COMSEC materials and equipment. A minimum of one (1) COMSEC Account Manager shall be a GSA Certified Safe & Lock technician. The Contractor shall provide and maintain no less than one (1) X-Series GSA locks on hand in-country for repair/replacement of any inoperable locks.

1.5.1.10 The COMSEC Account Manager shall ensure that required page checks are accomplished on all keying material as specified with applicable USG COMSEC Guidance, new CJCSI 6510.06D, Security Directive 1, High Assurance Cryptographic Integration Assessment (HACIA), and NSA CSS Policy Manual 3-16, and on all publications when they are received, returned from hand receipt, transferred, destroyed, when a change of Primary Account Manager occurs, and when posting amendments which include replacement pages to ensure completeness of each publication.

1.5.1.11 The COMSEC Account Manager shall verify all shipments of accountable COMSEC material shipped outside of the account's organization is packaged and shipped as specified with applicable USG COMSEC Guidance, CJCSI 6510.06D, Security Directive 1, High Assurance Cryptographic Integration Assessment (HACIA), and NSA CSS Policy Manual No. 3-16. The COMSEC Account Manager shall ensure that all material received is inspected for evidence of tampering and, if at an element where the size of the COMSEC account is so large as to prevent the COMSEC Account Manager from personally checking security packaging and markings, performing page checks and posting amendments. If suspected physical incident is found, submit an incident report immediately, in accordance with applicable USG COMSEC Guidance, new CJCSI 6510.06D, Security Directive 1, High Assurance Cryptographic Integration Assessment (HACIA), and NSA CSS Policy Manual 3-16.

1.5.1.12 The accountability of COMSEC material should be maintained in a manner to ensure the locations and people being held accountable for issued COMSEC material (e.g. via review of hand receipts) can be readily determined. The COMSEC team shall be fully knowledgeable of the current COMSEC material held within the COMSEC account and the general purpose for which it is being used.

1.5.1.13 The COMSEC Account Manager shall establish and follow procedures to ensure strict control of each item of keying material whenever operational requirements require that COMSEC material is turned over from one shift to another or from one individual to another.

1.5.1.14 The COMSEC Account Manager shall ensure that appropriate COMSEC material is readily available to properly cleared and authorized individuals (based on a list provided by host country) whose duties require its use. If the material is classified, verify that the individuals are cleared to the level of the material. The COMSEC Account Manager shall issue material to users by means of a hand receipt (SF-153), as provided in applicable USG COMSEC Guidance, new CJCSI 6510.06D, Security Directive 1, High Assurance Cryptographic Integration Assessment (HACIA), and NSA CSS Policy Manual 3-16, and advise recipients of their responsibility for safeguarding the material until it is returned to the COMSEC Account Manager.

1.5.1.15 The COMSEC Account Manager shall report immediately to USSOUTHCOM-J6 C2IP/COMSEC Branch, the U.S. Embassy in Bogota Colombia and the NSA Central Office Record (COR) of 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 applicable USG COMSEC Guidance, new CJCSI 6510.06D, Security Directive 1, High Assurance Cryptographic Integration Assessment (HACIA), and NSA CSS Policy Manual 3-16. USSOUTHCOM-J6 should be informed of all COMSEC incidents and receive copies of all official reports.

1.5.1.16 The COMSEC Account Manager shall perform COMSEC audits at COMSEC Responsible Officer (CRO) sub-accounts and COMSEC user sites and units that use and operate USG-provided COMSEC material and equipment at the direction of the MILGRP and USSOUTHCOM-J6. The COMSEC Account Manager shall routinely check SECRET Internet Protocol Router Network (SIPR Net) emails for traffic, and send notifications of any unofficial physical security violations, based on sound judgment, to those parties that are responsible and/or accountable of USG Physical Security violations.

1.5.1.17 The COMSEC Account Manager shall serve as the liaison regarding all COMSEC issues between the U.S./Colombia FMS COMSEC account, SCO, and USSOUTHCOM.

1.5.1.18 The COMSEC Account Manager shall provide COMSEC support to Partner Nation on the proper handling and use of USG-provided COMSEC material and equipment. The COMSEC Account Manager shall assist in COMSEC equipment familiarization with Colombia Joint Force personnel in addition to the proper custodianship, safeguarding and operation of DoD-provided COMSEC equipment, encryption key and other COMSEC-related materials, zeroing equipment, basic troubleshooting (when necessary), and emergency destruction procedures, to satisfy requirements for secure interoperability.

1.5.1.19 The COMSEC Account Manager must have a background in COMSEC Management principles.

1.5.1.20 The COMSEC Account Manager must have background in Electronic Keying Management Systems (EKMS). An EKMS COMSEC account certification will need to be accomplished.

1.5.1.21 The COMSEC Account Manager must have experience in downloading and transferring electronic keys using all current fill devices (e.g. SKLs).

1.5.1.22 The COMSEC Account Manager should have background in all cryptographic/COMSEC equipment used by Colombia.

1.5.1.23 The COMSEC Account Manager shall establish and maintain Emergency & Precautionary Destruction Plans as part of the account's Emergency Action Plan (EAP). COMSEC Account Manager shall conduct exercises of the COMSEC account EAP (per NSA CSS Policy Manual 3-16 on a semi-annual basis). This Emergency Plan must consider both natural disasters and hostile actions (such as enemy or terrorist attack, mob action, or civil uprising). Emergency Plans at OCONUS entities must include Emergency Destruction Procedures (EDPs). (CDRL A004)

1.5.1.23.1 COMSEC Account Manager EAP shall include planning for hostile actions to safely evacuate or securely destroy COMSEC material. By contrast, planning for epidemics, pandemics, hostile actions, and natural disasters shall be directed toward maintaining security control over the material until the situation stabilizes and shall address the contractor policies and procedures to identify an evacuation plan, if necessary.

1.5.1.23.2 COMSEC Account Manager shall review the EAP annually and update as necessary or whenever changes in the local environment dictate an update to the plan.

1.5.1.23.3 COMSEC Account Manager shall coordinate the EAP with USSOUTHCOM J63-OC personnel and all authorized personnel at the facility must be aware of the existence of the plan.

1.5.1.24 The COMSEC Account Manager shall ensure the FMS COMSEC Account is always kept in good standing with NSA. In the event the FMS COMSEC Account is not in good standing, the contractor shall notify the USSOUTHCOM J38-O, J6-C2IP, NSA, SCO, and USG Contracting Officer immediately for determination on emergency supersession, compromise, and to provide a follow-up no later than five (5) business days and explain the contractor's policies, procedures and actions to be taken to get the FMS COMSEC Account back in good standing.

1.5.2 C5ISR Support Services. The COMSEC Account Manager shall provide C5ISR support services to the Colombia Joint Force and interface with the United States Embassy, the U.S. DoD, as well as other agencies/offices as deemed necessary. The function of the alternate COMSEC Account Manager is to act as the Primary COMSEC Account Manager in the event of temporary absence of the FMS Primary COMSEC Account Manager. The alternate COMSEC Account Manager shall perform the duties outlined in Paragraph 1.5.1. In fulfilling these responsibilities, the contractor shall perform the following duties:

1.5.2.1 The COMSEC Account Managers shall serve as a liaison between U.S. Government and Colombia Joint Force on matters related to C5ISR Secure Interoperability to increase operational usage in current and future C5ISR operations.

1.5.2.2 The COMSEC Account Managers shall assist the Colombia Joint Force to identify, evaluate, and integrate emerging multi-discipline C4lSR technologies and non-material solutions into operational architectures and operating procedures.

1.5.2.3 The COMSEC Account Managers shall provide analytical assessments/evaluations related to both threat and intelligence mission requirements on current country authorized C5ISR programs. Contractor Program Manager shall report all analytical assessments/evaluations on C5ISR program within the Monthly Status Report (CDRL A001).

1.5.2.4 The COMSEC Account Manager can assist in integration strategies in conjunction with country authorized C41SR components to mitigate risks posed to operational C5ISR weapon system operations.

1.5.2.5 The COMSEC Account Manager shall provide subject matter expert input to empirical and qualitative assessments regarding technology and procedural impacts to current and programmed C5ISR systems, sub-components, tactics, techniques and procedures, and organizational structures and participate as observer in Bi-lateral (U.S./Partner Nation) Joint C5ISR experimentation, operational exercises and system development and integration activities.

1.5.2.6 The COMSEC Account Manager shall report all classified information that has been released to Colombia Joint Force and to USSOUTHCOM-J6, via SCO for coordination and instructions.

1.5.2.7 The COMSEC Account Manager must have a background in C5ISR Systems and Networks. Contractor personnel may be asked to provide DoD training certifications in meeting current or future DoD C5ISR requirements.

1.5.2.8 The COMSEC Account Manager can assist Combatant Command (CCMD) with physical security survey and/or assessment of Partner Nation facilities when required using USG provided guidance and report findings to USSOUTHCOM J6-C2IP/J6.

1.5.3 Contractor/Program Manager Responsibilities

1.5.3.1 The contractor shall provide United States Citizens who are NSA-certified COMSEC Account Managers for the Colombia COMSEC program located at the COMSEC facility in Bogota, Colombia. The contractor shall make all necessary arrangements to ensure the certification is obtained prior to COMSEC Account Manager arriving in country. Additionally, the contractor shall submit a monthly report that includes COMSEC Account Manager and C5ISR analytical duties performed outlined within paragraphs 1.5.1 and 1.5.2. The purpose of the monthly report is to provide Lackland Contracting Officer Representatives (COR) and Contracting Officer (CO) with an oversight of duties performed within country **(the report will not contain any classified information or operations).** All future anticipated in/out-of-country travel for the following month shall be submitted in the prior month's Monthly Status Report. (CDRL A001)

1.5.3.2 The COMSEC Account Manager shall report the destruction or loss of U.S. COMSEC material immediately and outline any activity/findings/corrective actions no later than five (5) calendar days and report to the COR (Primary and Alternate(s)), Contracting Officer, and SCO via email.

1.5.3.3 COMSEC Account Manager must hold a current 8570/8140 IAT Level II certification (at a minimum Security+). COMSEC Account Manager currently on contract will have 12 months to obtain certification, all new COMSEC Account Manager will be required to have certification prior to filling the position. This shall be at no cost to Partner Nation. Failure to maintain or achieve certification will result in removal from contract. The Government will review the resumes (redacted to remove only PII) of contractor personnel proposed to be assigned, and if personnel are not currently employed by the Contractor, a written agreement from the potential employee to work will be part of the technical proposal. (CDRL A005)

1.5.3.4 COMSEC Account Manager personnel shall be a graduate of formal COMSEC training prior to their assignment, along with being certified in the NSA COMSEC course (normally a three (3) day course) within six (6) months from their appointment date as a COMSEC Account Manager (IAW NSA CSS Policy Manual No. 3-16, paragraph 16).

1.5.3.5 COMSEC Account Manager shall get read access to WebRoR to assist in the tracking and status of equipment that is being Repaired and Returned (R&R). To get access, visit https://scip.dsca.mil/welcome/ and register. MILGRP-Colombia will be able to provide COMSEC R&R FMS Case and Line to track status for each Implanting Agency (IA).

1.5.3.6 COMSEC Account Manager shall attend USSOUTHCOM Foreign Disclosure (FD) or appropriate Regional COMSEC Account Familiarization and equipment training course.

1.5.3.7 COMSEC Account Manager shall be thoroughly familiar with the proper handling and safeguarding of COMSEC materials and equipment.

1.5.3.8 COMSEC Account Manager shall be thoroughly familiar with Colombia's civil codes.

1.5.3.9 COMSEC Account Manager shall be able to research and understand National Security Agency (NSA) Information Assurance (IA)/COMSEC regulations and USSOUTHCOM agency operational directives.

1.5.3.10 COMSEC Account Manager shall be thoroughly familiar with Operational Security strategies and methods. Conduct physical security inspection of facilities where there is an operational need to install and operate COMSEC equipment.

1.5.3.11 COMSEC Account Manager shall be able to develop, prepare, and deliver hand receipt to COMSEC responsible officers. While transferring COMSEC items to host country, the COMSEC Account Manager shall assist host nation in COMSEC equipment familiarization as

long as host country can provide COMSEC Account Manager with technical manual(s) of the COMSEC item.

1.5.3.12 COMSEC Account Manager shall be able to clearly articulate concerns, including recommended Courses of Actions (COAs) both verbally and in writing, to senior U.S. and Host Nation leadership.

1.5.3.13 COMSEC Account Manager shall possess the ability to work independently without technical guidance.

1.5.3.14 COMSEC Account Manager shall be experienced in theory of all aspects of the COMSEC Equipment/Systems.

1.5.3.15 Must be able to lift at least 60 pounds without assistance.

1.5.3.16 Must have working knowledge and be able to perform basic troubleshooting of secure telephone systems (i.e. Secure Communications Internet Protocol (SCIP) devices, Secure Analog and Data Service devices, and Viper Phone. Must have understanding with ViaSat/L3 VINES as well as provide technical support to assist with Inline Network Encryption (INE) family of devices (i.e. KG-175 & KG/SG/IPS-250/255X). This includes devices management and timely updates to device firmware/software as directed by the NSA COR, key allocation, and configuration of the INE Devices used by Colombia Joint Force. In addition, COMSEC Account Manager will develop and provide Cryptographic Ignition Key (CIK) handling procedure, encapsulation methods, standard operating procedures (SOPs) and coordinate with platforms/program managers to ensure circuit availability during down-time (patching, updates, ext..).

1.5.3.17 Must be able to perform Over-The-Air-Rekey (OTAR), Over-The-Air-Transfer (OTAT), and Over-The-Air-File-Distribution (OTADS).

1.5.3.18 Must maintain accountability to properly execute emergency supersession quickly when OMC guidance is provided.

1.5.3.19 Must have computer skills in Microsoft Office products to include Outlook, Word and Excel.

1.5.3.20 Must have background in tactical and strategic communications systems and networks.

1.5.3.21 Must be able to maintain highest accountability and pass all COMSEC inspections/audits whether scheduled or unscheduled.

1.5.3.22 COMSEC Account Manager may be required to work occasional overtime to support the Host Nation.

1.5.3.23 Knowledge of the learning process and how to transfer knowledge to less qualified personnel, including the ability to express thought in both oral and written

communications. (Instructor Training Ability). COMSEC Account Managers must be proficient in Spanish (ILR 4) and English. https://www.govtilr.org/Skills/ILRscale2.htm

1.5.3.24 COMSEC Account Manager shall possess a high degree of tact, diplomacy and the ability to work and cooperate harmoniously with the Colombian military and civilian personnel.

1.5.3.25 Contractor/PM shall provide in-country COMSEC Account Manager all required communication equipment items to conduct day-to-day COMSEC operations in Colombia which will be priced into the contract as an Other Direct Cost CLIN on the contract, (e.g. laptops, Wi-Fi routers, printer/scanner and any other items deemed necessary). All perishable items such as office and cleaning supplies along with paper, toner, printer ink cartridges, pens/pencils and general office supplies will be provided by the contractor. Office equipment shall be a part of the Colombian COMSEC Account Manager inventory. The internet service is required to support the daily operations of the COMSEC account in their coordination and correspondence with USG agencies and Vendor/Manufacturers, research of equipment usage and operations instructions and the requirement to submit monthly and quarterly reports and inventories to the above agencies.

1.5.3.26 The contractor shall provide health insurance for all personnel while working in country.

1.6 Work Situation. The COMSEC Account Manager shall provide coverage in Bogota, Colombia, between the hours of 0730 and 1600, or as agreed to by the using activity, but one (1) COMSEC Account Manager must be available on-call 24 hours a day / 7 days a week. Normal duty days will be Monday through Friday, excluding American Embassy selected holidays. Work is normally conducted in an office environment on a 40-hour per week basis. COMSEC Account Manager are designated Mission Essential/Critical (not through the U.S. Embassy). The COMSEC Account Manager may be required to travel within the country to alternate duty locations to perform COMSEC Account Manager services. One (1) COMSEC Account Manager must remain at Bogota, Colombia, during normal duty hours unless partner nation authorizes all COMSEC Account Managers to be away from Primary duty location.

1.6.1 Recognized Holidays: COMSEC Account Manager shall follow American Embassy and Partner Nation selected holidays.

1.6.2 In performing the tasks contained above, the COMSEC Account Manager will interface with a variety of other Department of Defense (DoD) and USG organizations and offices, and other U.S. contractors. COMSEC Account Manager will not provide direction or otherwise interject themselves into relationships between the U.S. and other government agencies. COMSEC Account Manager are expected to make recommendations and offer solutions that adhere to USG policies. Services provided under this requirement are considered non-personal services.

1.6.3 Security Clearance. The COMSEC Account Manager shall be able to obtain and maintain a final SECRET security clearance. Contractor is responsible and shall ensure employees performing duties under this contract are submitted for Periodic Reinvestigations (PRs) as required by the DoD and AF Personnel Security Program requirements.

1.6.4 Report to Instructions: COMSEC Account Manager will report to the MILGRP-Colombia for accountability. The MILGRP-Colombia is located at the American Embassy, Bogota, Colombia. Checking in with the MILGRP-Colombia is required according on a weekly basis, more often if required by the MILGRP-Colombia. This is for accountability reasons only.

1.6.5 Certifying Official or Designee: The Certifying Official or designee will ensure the requirements are met to store and maintain COMSEC material at the COMSEC Facility located at Bogota, Colombia, and other designated COMSEC locations. Site surveys will be performed by SOUHCOM J6 inspectors. The certifying official will be the:

Director, National Security Agency
15131 Account Registration
Central Office of Record
9800 Savage Rd, Suite 6574
Fort George G. Mead MD, 20755
Voice: (410) 854-8526
Unclassified Fax: (410) 854-6631

1.6.6 Alternate Certifying Official or Designee: The Director, National Security Agency's Deputy or designated Officer in charge in the absence of the Director.

1.6.7 The country of Colombia will levy no taxes or fees (including taxes on individual or corporate income or property, customs and import duties, or other taxes on employee personal household goods, supplies and personal effects imported into Colombia for personal use) on the contract or its employees. COMSEC Account Managers are subject to import duties on new items/equipment, but no export duties are assessed. Colombia will assess no personal income taxes.

1.6.8 Limited U.S. Logistics Support will be provided by the U.S. Government, to include:

- Government ID cards (DoD CAC)
- Access to classified/unclassified U.S. Government networks (for performance of duties mentioned in section 1.3)
- **No APO/FPO privileges for Colombia**
- The contractor shall provide a Company letter listing along with MP ICAM Forms 1 and 2 for all new employees. The Company letter listing shall be provided once an employee departs, or a new employee arrives.
- This is an unaccompanied assignment, if contractor decides to bring dependents, all costs will be at the expense of the employee.

This is dependent on Host Nation and US Embassy guidance.

1.6.9 Colombia Joint Forces will be responsible for the following in-country logistics:

a. Access to any/all locations and/or Colombian Military installations/bases/units utilizing COMSEC Equipment using U.S. provided COMSEC equipment.
b. Provide adequate office space for all COMSEC Account Manager. Office space should have standard office furniture and equipment.

1.6.10 United States Government, to include Military and DoD Civilians in country will be responsible for the following in-country logistics.

a. To help facilitate all access control to Host Nations
b. Facilitate COMSEC Account Manager attendance at MILGRP-Colombia COMSEC meetings when required.
c. Facilitate obtaining approvals for documentation by host nation.

1.6.11 Driving conditions. COMSEC Account Manager must be able to drive a vehicle and obtain an International Driver's License. Upon getting a work permit/business Visa, obtain a local driver's license if authorized. Lease or long-term rental vehicles are authorized. Some locations may require the use of 4WD vehicles. Vehicles shall be of adequate size and ground clearance to enable access to allow for COMSEC equipment delivery and site visits to all Colombian Joint Forces locations that utilize U.S.-provided COMSEC equipment and material. The Government of Colombia will NOT provide a driver for the vehicle.

1.6.12 Housing: Government quarters are not available. The contractor shall supply housing. The contractor shall use the U.S. Department of State Group 3 without family rates, IAW U.S. Department of State Standardized Regulations (DSSR) 130 for Bogota, Colombia, location. If housing costs are outside of the DSSR regulations, provide response on the costs and location of proposed housing.

1.7 Travel Requirements. Temporary Duty (TDY) travel is anticipated for this requirement. All external country travel shall be submitted within 14 calendar days before a TDY. The TDY request is coordinated through the CORs and pre-approved by the Contracting Officer. With the exception of last-minute emergency TDYs, provide justification and receipts within five business days or as soon as possible to the Contracting Officer and COR for review.

1.7.1 All travel associated with this PWS will be cost reimbursable. Travel locations will be dictated by mission requirements. The COMSEC Account Manager shall travel, both CONUS and OCONUS, in support of contractual work requirements.

1.7.2 Routine travel will be required to ensure up-to-date knowledge of any/all interoperability requirements as well as emerging secure interoperability technologies. Command and Control Interoperability Board (CCIB) meetings and working groups, as well as Colombian Joint Force directed travel that is in line with the duties and responsibilities as outlined in the PWS, may be required. The following official travel guidelines are provided:

1.7.2.1 COMSEC Account Manager/ (Primary or Alternate) are required to travel for the following events:

a. The COMSEC Account Manager or Alternate shall attend all CCIBs and Working Groups related to COMSEC Account Manager duties.
b. Attendance at any other Colombian Joint Force or U.S. DoD directed travel that involves COMSEC Account Manager duties (i.e., CCIBs, Program Management Review (PMRs), Mode 5 Identification Friend or Foe (IFF) conferences, etc).

1.7.2.2 Program Manager is not required to travel and therefore travel will not be reimbursed except under the following circumstances:

a. All travel for program managers to perform COMSEC Account Manager duties in which the primary or alternate cannot attend.
b. Any other Colombian Joint Force or U.S. DoD directed travel that involves COMSEC Management duties in which the Primary COMSEC Account Manager cannot attend.

1.7.3 Travel justification and costs must be approved in advance by the COR to ensure the maximum benefit per trip is achieved as well as continuity of services. Travel shall be in accordance with the terms and conditions of the Joint Travel Regulation (JTR) guidance and IAW FAR Part 31. All travel arrangements shall be the responsibility of the Contractor including, but not limited to, airline, hotel and rental car reservations. The Contractor shall make every effort to schedule travel far enough in advance to take advantage of reduced airfares.

1.7.4 If travel is required to support this effort, all air travel should be Coach/Economy. Travel must be documented and justified in accordance with FAR 31/205-46 and the JTR and must be preapproved by the Contracting Officer.

1.7.5 Upon completion of out of country TDY, a TDY report is due to the CORs. (CDRL A002)

1.7.6 Leaving the Country. The COMSEC Account Manager shall provide an anticipated date of arrival back into the country. The contractor shall notify the PCO, COR and MILGRP via formal correspondence, at least 14 calendar days prior to COMSEC Custodian being unavailable and/or replaced. During COMSEC Custodian absences, to include all leave, the contractor is responsible for providing coverage to meet all requirements of the contract.

1.7.7 Passports, Visa's, Customs. The COMSEC Account Manager shall obtain and maintain passports, visas, country clearance, or other documents necessary to enter or exit any theater area of operation.

1.8 Operations Security (OPSEC). COMSEC Account Manager should be thoroughly familiar with OPSEC strategies and methods. OPSEC requirements are stipulated to reduce program vulnerability from successful adversary collection and exploitation of critical information.

COMSEC Account Manager shall employ sound OPSEC principles and procedures in the performance of their duties and responsibilities IAW DoD and AF OPSEC publications.

1.9 Mobilization/Demobilization. Mobilization/Demobilization will not be considered as work in fulfilling the contract requirements for commencement of work.

1.9.1 Mobilization/Demobilization shall include all activities and one-time associated costs for transportation of the COMSEC Account Manager personnel, equipment, and operating supplies to the work site. The Contractor will be responsible for all mobilization/demobilization expenses in the event of personnel release or voluntary reassignment.

1.9.2 Demobilization shall include all activities and costs for transportation of personnel, equipment, and supplies not required or included in the contract from the work site. Demobilization will only be authorized in the event of the completion of the contract with no anticipation of a follow-on contract, no continuing funds, or the unforeseen removal of contractor personnel from the worksite for their own safety through no fault of their own (based on the official direction of the U. S. Government). All demobilization travel must be pre-approved by the Contracting Officer unless it occurs under an emergency situation.

1.10 Payment by DFAS through Wide Area Workflow (WAWF) will be made as demobilization or mobilization occurs, after presentation of a proper invoice showing specific costs and supporting evidence of the charges.

2.0 SERVICE REQUIREMENTS

2.1 Contractor Full Time Equivalent Reporting

2.1.1 The contractor shall report ALL COMSEC Account Manager labor hours (including subcontractor labor hours) required for performance of services, regardless of contract type, provided under this contract for the Air Force via a secure data collection site. The Contractor is required to complete all required data fields at www.sam.gov. Reporting inputs shall be for the labor executed during the period of performance for each Government fiscal year (FY), which runs from 1 October through 30 September. While inputs may be reported any time during the FY, all data shall be reported no later than 31 October of each calendar year.

2.2 Service Delivery Summary

2.2.1 The Contractor service requirements are summarized in the Services Summary below. This summary outlines the performance objectives linked to the standards needed to meet the essential mission functions. The performance threshold describes the minimum acceptable service levels for each objective. These thresholds are essential to mission success.

Performance Element/Objective	PWS Para.	Performance Standard/ Threshold	Method of Surveillance
SS-1 Protect U.S. NSA approved COMSEC material and limit access to individuals with a valid need-to-know and clearance	1.5.1.1	Performance is acceptable when there are no COR-validated complaints or corrective action reports per month of failure to correctly protect U.S. NSA approved COMSEC material and limit access to individuals with a valid need-to-know and clearance. A validated complaint or corrective action report will result in a security violation investigation. Results from the security violation investigation will determine future actions and outcomes.	Customer Complaints & Periodic Surveillance; MILGRP-Colombia Reported Complaints; USSOUHTCOM COMSEC Inspection; NSA COMSEC Inspection; USG COR Site Visits
SS-2 Receive, receipt for, and ensure the safeguarding and accounting of all U.S. NSA approved COMSEC material	1.5.1.3	Performance is acceptable when there are no COR-validated complaints or corrective action reports per month of failure to correctly receive, receipt for, and ensure the safeguarding and accounting of all U.S. NSA approved COMSEC material. A validated complaint or corrective action report will result in a security violation investigation. Results from the security violation investigation will determine future actions and outcomes. Re-performance shall occur within three (3) business days of notification.	Customer Complaints & Periodic Surveillance. MILGRP-Colombia Reported Complaints. USSOUHTCOM COMSEC Inspection. NSA COMSEC Inspection; USG COR Site Visits
SS-3 Maintain U.S. NSA approved COMSEC material accounting and related U.S. records	1.5.1.4	Performance is acceptable when there are no COR-validated complaints or corrective action reports per month of failure to correctly receive, receipt for, and ensure the safeguarding and accounting of all U.S. NSA approved COMSEC material. A validated complaint or corrective action report will result in a security violation investigation. Results from the security violation investigation will determine future actions and outcomes. Re-performance shall occur within three (3) business days of notification.	Customer Complaints & Periodic Surveillance; MILGRP-Colombia Reported Complaints; USSOUHTCOM COMSEC Inspection; NSA COMSEC Inspection; USG COR Site Visits
SS-4 Conduct, document, and submit an inventory semiannually and/or when sub-hand receipt holders change	1.5.1.5	Performance is acceptable when there is no COR - validated complaints of failure to correctly conduct, document and inventory semiannually and/or when sub hand receipt holders change. Performance is unacceptable when there is one or more COR-validated complaints of failure to correctly conduct an inventory semiannually. A validated complaint will result in a security violation investigation. Results from the security violation investigation will determine future actions and outcomes. Re-performance must occur within three (3) business days of notification.	Customer Complaints & Periodic Surveillance; MILGRP-Colombia Reported Complaints; USSOUHTCOM COMSEC Inspection; NSA COMSEC Inspection; USG COR Site Visits

Performance Element/Objective	PWS Para.	Performance Standard/ Threshold	Method of Surveillance
SS-5 Perform routine destruction of COMSEC material	1.5.1.6	Performance is acceptable when there is no COR-validated complaint per month of failure to correctly perform destruction of COMSEC material in the designated time-period and prescribed method as annotated in the regulations, instructions and messages. Performance is unacceptable when there is one or more COR -validated complaints per month of failure to correctly perform routine destruction of COMSEC material. A validated complaint will result in a security violation investigation. Results from the security violation investigation will determine future actions and outcomes. Re-performance must occur within three (3) business days of notification.	Customer Complaints & Periodic Surveillance; MILGRP-Colombia Reported Complaints; USSOUHTCOM COMSEC Inspection; NSA COMSEC Inspection; USG COR Site Visits
SS-6 Ensure that required page checks are accomplished on all keying material and publications	1.5.1.10	Performance is acceptable when there is no COR-validated complaint per month of failure to correctly ensure that required page checks are accomplished on all keying material and publications. Performance is unacceptable when there is one or more COR - validated complaints per month of failure to correctly ensure that required page checks are accomplished on all keying material and publications. A validated complaint will result in a security violation investigation. Results from the security violation investigation will determine future actions and outcomes. Re-performance must occur within three (3) business days of notification.	Customer Complaints & Periodic Surveillance; MILGRP-Colombia Reported Complaints; USSOUHTCOM COMSEC Inspection; NSA COMSEC Inspection; USG COR Site Visits
SS-7 COMSEC Emergency Action Procedures IAW NSA CSS MAN 3-16	1.5.1.23	Performance is acceptable when there is a current, written and rehearsed emergency plan for the protection of COMSEC material appropriate for manmade disasters, epidemics, pandemics, natural catastrophes, hostile actions, and natural disasters. Performance is unacceptable when the written emergency plan is not on file, current and rehearsed. A validated complaint will result in a security violation investigation. Results from the security violation investigation will determine future actions and outcomes. Re-performance must occur within three (3) business days of notification.	Customer Complaints & Periodic Surveillance; MILGRP-Colombia Reported Complaints; USSOUHTCOM COMSEC Inspection; NSA COMSEC Inspection; USG COR Site Visits
SS-8 NSA Account Suspended	1.5.1.24	Performance is acceptable when compliant with NSA policies. Performance is unacceptable when the NSA account is suspended by NSA for not meeting the NSA policies. Once notified, Contractor must ensure reinstatement of the NSA account within five (5) business days of notification.	Customer Complaints & Periodic Surveillance; MILGRP-Colombia Reported Complaints; USSOUHTCOM COMSEC Inspection; NSA COMSEC

Performance Element/Objective	PWS Para.	Performance Standard/ Threshold	Method of Surveillance
			Inspection; USG COR Site Visits

3.0 GENERAL INFORMATION

3.1 Management and Administration. The contractor shall provide the necessary resources and infrastructure to manage and administer the services required in the contract.

3.1.1 Contractor Performance Assessment Reporting System (CPARS) Applicability. FAR Part 42.1502 directs all Federal Agencies to collect and report past performance information on service contracts with a value of $1M or more. CPARS assesses a contractor's performance and provides a written record on a given contract during a specified period. All CPARS are accomplished using the Naval Sea Logistics Center's Contractor Performance Assessment Reporting System (CPARS) found on the web at http://www.cpars.csd.disa.mil/. This system requires the Contractor to provide a designated representative to receive the CPARS electronically. The Contractor shall submit their representative's name, telephone number, and e-mail address with their proposal. The initial CPARS for this contract will be completed on the anniversary of the contract award.

3.1.2 Phase-Out Transition Plan. The contractor shall submit a plan for the process of closing out the contract. The plan shall show the process the contractor will take to handover any equipment, records, sensitive items, and any other actions. The plan shall include different offices position in staying in compliant with all policies regulations during the closeout of contract. The plan shall show a smooth transition during the end of the contract period. (CDRL A003)

3.2 Policy. The contractor shall be familiar with applicable DoD acquisition and FMS policy, law, regulations, and guidance required to perform efforts as defined in this Performance Work Statement.

3.3 COMSEC Account Manager Identification. All COMSEC Account Manager personnel who attend meetings, answer telephones, correspond by email and work in other situations where the COMSEC Account Manager status is not known or obvious to third parties, the COMSEC Account Manager is required to identify himself or herself as a contractor employee to avoid creating an impression in the minds of members of the public that they are government officials. Any documents or reports produced by the contactor shall be clearly marked as COMSEC Account Manager products or that COMSEC Account Manager participation is appropriately disclosed. COMSEC Account Manager shall wear visible contractor-provided identification either as part of or always attached to their outer clothing while on duty, which clearly identifies the individual as a contractor employee.

3.4 Risk Mitigation Plan: All Contractors operating or managing Communications Security (COMSEC) accounts are required to develop a formal Risk Mitigation Plan. This plan must detail the immediate actions, succession protocols, and accountability measures to be executed if a Primary or Alternate COMSEC Account Manager (CAM) departs their duty station

unexpectedly, ensuring continuous operational security and zero degradation of COMSEC accountability within a 30-day transition window. (CDRL 0003)

3.5 Personnel Management and Training. The contractor shall be responsible for the employment, training, guidance, and supervision of qualified personnel to accomplish the services required under the contract. The contractor shall accomplish the assigned work by employing and utilizing qualified personnel with the appropriate combination of education, training, and experience.

4.0 EVACUATION/DECLARATION OF EMERGENCY

4.1 Evacuations. If the Chief of Mission (COM) orders a mandatory evacuation of some or all personnel, the level of assistance provided to employees of the contractor shall be the same as the level of assistance provided to other U.S. Embassy Mission Essential staff/employees. In the event of a non-mandatory evacuation order, the contractor shall maintain personnel at a location sufficient to meet contractual obligations under this contract until instructed to evacuate by the Contracting Officer, Contracting Officer's Representative, or COM.

4.1.1 In emergencies that pose an immediate risk of death or serious injury to contractor personnel, such as enemy activity or natural disasters, the Embassy Regional Security Officer (RSO) or a representative of the Defense Attache's Office may issue oral instructions. The contractor must notify the CO or COR within 48 hours of any emergency that results in a work stoppage or evacuation.

4.1.2 Medical Evacuation Costs: Should COMSEC Account Manager require medical evacuation from Colombia for whatever reason, all costs will be borne by the COMSEC Account Manager.

4.2 Declaration of Emergency. During a state of emergency, as declared by the National Command Authority or Commander-in-Chief, the COMSEC Account Manager may be required to expand or curtail the level of services listed in the PWS. In accordance with DODI 3020.37, "Continuation of Essential DoD Contractor Services During Crisis", the COMSEC Account Manager is required to already have established an approved Continuity of Operations Plan (COOP) prior to a crisis occurring. The American Embassy will provide specific instructions during the emergency as to which services, as indicated in the COOP, are considered essential and to what level to include hours of operation.

5.0 Regulatory Documents

The following is a list of regulatory documents that shall dictate and guide the performance of a COMSEC Account Manager.

Document Number	Title
NSA/CSS Policy Manual 3-16	Control of Communications Security (COMSEC) Material **dated 23 Jan 2015

CJCSI 6510.06D	Security Directive 1 High Assurance Cryptographic Integration Assessment (HACIA)
CNSSI No. 4001	Controlled Cryptographic Items
Security Doctrine 1	Safeguarding COMSEC Facilities and Materials
CNSSI No. 4003	Reporting and Evaluating COMSEC Incidents
CNSSI No. 4004.1	Destruction and Emergency Protection Procedures for COMSEC and Classified Material
CNSSI No. 4005	Safeguarding COMSEC Facilities and Materials
CNSSI No. 4005 Amendment	Safeguarding COMSEC Facilities and Materials **dated 22 August 2011
CNSSI No. 4006	Controlling Authorities for Traditional COMSEC Keying Material
CNSSI No. 4031	Cryptographic High Value Products
CNSSI No. 4032	Management and Use of SDNS Firefly Keying Material and Equipment
CNSSI No. 4033	Nomenclature for COMSEC
NSA/CSS NAG-14C	Allied **COMSEC** Material Accounting Manual
NSA/CSS NAG-18A	Safeguarding **COMSEC** Material and Facilities

6.0 <u>COMSEC PUBLICATIONS/ Required documents</u>

National Security Agency (NSA) Central Security Service (CSS) Policy Manual 3-16
CJCSI 6510.06D
Security Directive 1
High Assurance Cryptographic Integration Assessment (HACIA)

6.1 CDRL0001 Monthly report shall consist of all activities COMSEC Account Manager participated in during the previous month.
6.2 CDRL0002 TDY report after all travel outside of country, to include slides that are presented at CCIB or other meetings.
6.3 CDRL 0003 Risk Management Plan.
6.4 CDRL 0004 Emergency Action Plan (EAP).
6.5 CDRL 0005 Resumes for COMSEC Account Manager

7: ACRONYMS

AF	Air Force
AFSAC	Air Force Security Assistance and Cooperation Directorate
C4IRS	Command, Control, Communications, Computers, Intelligence, Reconnaissance and Surveillance
CCIB	Command and Control Interoperability Board
CCMD	Combatant Command
CISMOA	Communications and Information Security Memorandum of Agreement
CO	Contracting Officer
COMSEC	Communication Security
COOP	Continuity of Operations Plan
COR	Contracting Officer Representative
COR NSA	Central Office of Record (NSA)
CPARS	Contractor Performance Assessment Reporting System
DFAS	Defense Finance and Accounting Service
DoD	Department of Defense
DODI	Department of Defense Instructions
EDPs	Emergency Destruction Procedures
FD	Foreign Disclosure
FMS	Foreign Military Sales
IA	Information Assurance
IAW	In Accordance With
INFOSEC	Information Security
MOD	Ministry of Defense
LOA	Letter of Offer and Acceptance
MWR	Morale, Welfare, and Recreation
NDA	U.S. National Distribution Authorities
NSA	National Security Agency
OCONUS	Outside Continental United States
OPSEC	Operations Security
OTAR	Over-the-Air-Rekey
OTAT	Over-the Air-Transfer
OTADS	Over-The-Air-File-Distribution
PWS	Performance Work Statement
SCIP	Secure Communications Internet Protocol
SCO	Security Cooperation Office
SME	Subject Matter Expert
STE	Secure Telephone Equipment
SWT	SECTERA Wireline Terminal
TDY	Temporary Duty
TDL	Tactical Data Link
USSOUTHCOM	United States Southern Command
USG	United States Government
US MILGRP	United States Military Group
WAWF	Wide Area Workflow

WeBRoR WeBRoR